TEXAS RULES OF CIVIL PROCEDURE

PART V - RULES OF PRACTICE IN JUSTICE COURTS

SECTION 1. GENERAL RULES

RULE 500. DEFINITIONS

In Parts V and VII of these Rules of Civil Procedure:

(a) "**Answer**" is the written response a defendant must file with the court after the defendant is served with a citation.

(b) "**Cause of action**" is the legal basis, or reason, that a party claims to be entitled to relief from the court.

(c) "**Certified process server**" is a person certified under order of the Supreme Court of Texas to serve civil citations, notices, and other papers issued by Texas courts.

(d) "**Citation**" is the court-prepared document required to be served upon a party to inform the party that the party has been sued.

(e) "**Civil Cases**" are all non-criminal cases filed in a Justice Court, including Small Claims Cases, Eviction Cases, Debt Claim Cases, and Repair and Remedy Suits.

(f) "**Clerk**" is a person designated by the judge as a justice court clerk, or the judge if there is no clerk available.

(g) "**Contest**" means to challenge a statement made by a party claiming inability to pay filing fees, appeal costs, or other costs of court.

(h) "**Co-Party**" is another party on the same side of a lawsuit; for example, if there are two plaintiffs, the two plaintiffs are co-parties. The term is also used if there is more than one defendant in the same lawsuit.

(i) "**Counterclaim**" is a cause of action brought by a party who has been sued against the party suing them, for example, a defendant suing a plaintiff who has sued them.

(j) "**County court**" means the county court, statutory county court, or district court in a particular county with jurisdiction over appeals of civil cases from justice court.

(k) "**Cross-claim**" is a cause of action brought by a party against another party on the same side of a lawsuit. For example, plaintiff sues two defendants, A and B. Defendant A can seek relief against defendant B by means of a cross-claim.

(l) "**Debt Claim Case**" is a claim for the recovery of a debt, brought by an assignee of a claim, a debt collector or collection agency, or a person or entity primarily engaged in the business of lending money at interest. The claim can be for no more than $10,000 in damages, which includes attorney's fees, if any, but does not include statutory interest or court costs.

(m) "**Default Judgment**" is a judgment awarded to a plaintiff when the defendant fails to answer and dispute the plaintiff's claims in the lawsuit.

(n) "**Defendant**" is a person against whom or entity against which the plaintiff files a case. The term includes a plaintiff against whom a counterclaim is filed.

(o) "**Defense**" is a claim by a defendant that could prevent the plaintiff from being awarded a judgment.

(p) "**Discovery**" is the process through which parties obtain information from other parties in order to prepare for trial or enforce a judgment. The term does not refer to any information that a party is entitled to under applicable law.

(q) "**Dismissed without prejudice**" means a case has been dismissed but has not been finally decided. If a case is dismissed without prejudice it may be refiled. If a case is dismissed and the order is not specific with regard to prejudice, it is considered a dismissal without prejudice.

(r) "**Dismissed with prejudice**" means a case has been dismissed AND it has been finally decided. If a case is dismissed with prejudice it may not be refiled.

(s) "**Due diligence**" means that a party or other actor has taken all reasonable and prudent measures necessary to accomplish a duty imposed under the law.

(t) "**Eviction Case**" is a case seeking to recover possession of real property. A suit for rent may be joined with an eviction case if the amount of rent due and unpaid is not more than $10,000.

(u) "**General denial**" is an answer filed by a responding party that doesn't specify the reasons it feels its opponent should not recover, but instead merely states that it generally denies the allegations and demands that they be proven.

(v) "**Judge**" in these rules refers to a justice of the peace.

(w) "**Judgment creditor**" is the party awarded relief in a lawsuit and is legally entitled to enforce the award with the assistance of the court.

(x) "**Judgment debtor**" is the party against whom a court has made a judgment for relief.

(y) "**Judgment**" is an order by the court outlining the relief, if any, a party is entitled to or must provide.

(z) "**Jurisdiction**" refers to the inherent authority of a court to hear a case and to award a judgment.

(aa) "**Motion**" is a request from a party asking the judge to order some requested relief, or to compel a party to do something.

(bb) "**Movant**" means the person or party making a motion to be considered by the court.

(cc) "**Notice**" means a document prepared and delivered by the court to a party announcing that something is required of the party receiving the notice. It is to alert the party to take some action or forfeit some right or privilege, or suffer some consequence for failing to take action.

(dd) "**Parties**" include plaintiffs, defendants, counter-plaintiffs, counter-defendants, co-plaintiffs, co-defendants, third parties, and intervenors.

(ee) "**Personal delivery**" means deliver to the defendant, in person, a true copy of the citation, with the date delivered endorsed on the citation, along with the petition and any documents filed with the petition.

(ff) "**Petition**" means to make a formal written application requesting a court for a specific judicial action. It is the first document filed with the court to begin a lawsuit.

(gg) "**Plaintiff**" is a person who or entity which seeks relief in a civil case in justice court. The term includes defendant who files a counterclaim.

(hh) "**Plea**" means an earnest request, justification, excuse, or pretext.

(ii) "**Pleading**" is a written document filed with a court by a party that expresses a cause of action or defense and outlines the recovery sought, if any.

(jj) "**Plenary Power**" is the ability a court has to exercise its power and authority over a case.

(kk) "**Relief**" is what a party wants in a final judgment from the court, such as the recovery of money or personal property.

(ll) "**Repair and Remedy Case**" is a case brought to seek judicial remedy for the alleged failure of a landlord to remedy or repair a condition that Chapter 92 of the Property Code creates a duty for the landlord to remedy or repair.

(mm) "**Restricted delivery**" means delivery service where delivery must be made only to the named addressee, and delivery will not be allowed without the signature of the addressee so named on the item mailed.

(nn) "**Small Claims Case**" is a claim for money damages, civil penalties, or the recovery of personal property. The claim can be for no more than $10,000 in damages, which includes attorney's fees, if any, but does not include statutory interest or court costs.

(oo) "**Sworn statement**" is a written statement signed in front of someone authorized to take oaths and notarize the party's signature. Filing a false sworn statement could result in criminal prosecution. Instead of being signed in front of someone authorized to take oaths or a notary, the statement may be signed under penalty of perjury.

(pp) "**Third party claim**" is a cause of action brought by a party being sued against another individual or entity, other than the original plaintiff, to have the new party included in the lawsuit.

(qq) "**Trial de novo**" means an appeal where a new trial will be held in which the entire case is presented as if there had been no previous trial.

(rr) "**Venue**" refers to the county and precinct where a lawsuit occurs.

(ss) "**Voir Dire**" means "to see" "to say", and is the part of the jury selection process where the parties, or their attorneys, conduct a brief examination of prospective jurors who were summoned to serve for a trial.

RULE 501. JUSTICE COURT CASES

(a) Small Claims cases in justice court shall be governed by Part V of these rules of civil procedure.

(b) Debt Claim cases in justice court shall be governed by SECTION 8, and also by Part V of these rules of civil procedure. To the extent of any conflict between Part V and SECTION 8, SECTION 8 shall apply.

(c) Repair and Remedy cases in justice court shall be governed by SECTION 9, and also by Part V of these rules of civil procedure. To the extent of any conflict between Part V and SECTION 9, SECTION 9 shall apply.

(d) Eviction cases in justice court shall be governed by SECTION 10, and also by Part V of these rules of civil procedure. To the extent of any conflict between Part V and SECTION 10, SECTION 10 shall apply.

RULE 502. APPLICATION OF RULES IN JUSTICE COURT

Civil cases in the justice courts shall be conducted in accordance with the rules listed in Rule 501 of the Texas Rules of Civil Procedure. Any other rule in the Texas Rules of Civil Procedure shall not govern the justice courts except:

(a) to the extent the judge hearing the case determines that a particular rule must be followed to ensure that the proceedings are fair to all parties; or,
(b) where otherwise specifically provided by law or these rules.

Applicable rules of civil procedure shall be available for examination during the court's business hours.

RULE 503. COMPUTATION OF TIME AND TIMELY FILING

In these rules days mean calendar days. The day of an act, event, or default shall not count for any purpose. If the last day of any specified time period falls on a Saturday, Sunday or legal holiday, the time period is extended until the next day that is not a Saturday, Sunday or legal holiday. If the last day of any specified time period falls on a day during which the court is closed before 5:00 PM, the time period is extended to the court's next business day. Any document required to be filed or served by a given date is considered timely filed or served if deposited in the U.S. mail on or before that date, and received within ten days of the due date. A legible postmark affixed by the United States Postal Service shall be prima facie evidence of the date of mailing.

The judge may, for good cause shown, extend any time period under these rules except those relating to new trial and appeal.

RULE 504. RULES OF EVIDENCE

The Texas Rules of Evidence do not apply to justice courts except to the extent the judge hearing the case determines that a particular rule must be followed to ensure that the proceedings are fair to all parties.

RULE 505. DUTY OF THE JUDGE TO DEVELOP THE CASE

The judge may develop the facts of the case, and for that purpose may question a witness or party and may summon any person or party to appear as a witness as the judge considers necessary to ensure a correct judgment and speedy disposition of the case.

RULE 506. EXCLUSION OF WITNESSES

At the request of a party the court shall order witnesses excluded so that they cannot hear the testimony of other witnesses. Additionally, a court may issue such an order without any request. This rule does not authorize the exclusion of:
(1) a party who is a natural person or the spouse of such natural person;
(2) an officer or employee designated as a representative of a party who is not a natural person; or
(3) a person whose presence is shown by a party to be essential to the presentation of the party's cause.

RULE 506.1. SUBPOENAS

A subpoena may be used by a party or the judge to command a person or entity to attend and give testimony at a hearing or trial. A subpoena may be issued by the clerk of the justice court or an attorney authorized to practice in the State of Texas, as an officer of the court. A person may not be required by subpoena to appear in a county that is more than 150 miles from where the person resides or is served.

Every subpoena must be issued in the name of the "State of Texas" and must:

(a) state the style of the suit and its cause number;
(b) state the court in which the suit is pending;
(c) state the date on which the subpoena is issued;
(d) identify the person to whom the subpoena is directed;
(e) state the time, place, and nature of the action required by the person to whom the subpoena is directed;
(f) identify the party at whose instance the subpoena is issued, and the party's attorney
of record, if any;
(g) state that "Failure by any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of court from which the subpoena is issued and may be punished by fine or confinement, or both"; and
(h) be signed by the person issuing the subpoena.

A subpoena may be served at any place within the State of Texas by any sheriff or constable of the State of Texas, or any person who is not a party and is 18 years of age or older. A subpoena must be served by delivering a copy to the witness and tendering to that person any fees required by law. If the witness is a party and is represented by an attorney of record in the proceeding, the subpoena may be served on the witness's attorney of record.

A person commanded by subpoena to appear and give testimony must remain at the hearing or trial from day to day until discharged by the court or by the party summoning the witness. If a subpoena commanding testimony is directed to a corporation, partnership, association, governmental agency, or other organization, and the matters on

which examination is requested are described with reasonable particularity, the organization must designate one or more persons to testify on its behalf as to matters known or reasonably available to the organization.

A person commanded to attend and give testimony at a hearing or trial may object or move for a protective order before the court at or before the time and place specified for compliance. A party causing a subpoena to issue must take reasonable steps to avoid imposing undue burden or expense on the person served. In ruling on objections or motions for protection, the court must provide a person served with a subpoena an adequate time for compliance, protection from undue burden or expense. The court may impose reasonable conditions on compliance with a subpoena, including compensating the witness for undue hardship.

Failure by any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of the court from which the subpoena is issued or a district court in the county in which the subpoena is served, and may be punished by fine or confinement, or both.

A fine may not be imposed, nor a person served with a subpoena attached, for failure to comply with a subpoena without proof by affidavit of the party requesting the subpoena or the party's attorney of record that all fees due the witness by law were paid or tendered. Proof of service must be made by filing either:

(1) the witness's signed written memorandum attached to the subpoena showing that the witness accepted the subpoena; or

(2) a statement by the person who made the service stating the date, time, and manner of service, and the name of the person served.

RULE 507. PRETRIAL DISCOVERY

Any requests for pretrial discovery must be presented to the court by written motion before being served on the other party. The discovery request shall not be served upon the other party until the judge issues a signed order approving the discovery request. The court shall permit such pretrial discovery that the judge considers reasonable and necessary for preparation for trial, and may completely control the scope and timing of discovery. Failure to comply with the judge's order can result in sanctions, including sanctions that may prove fatal to a party's claim.

RULE 507.1. POST-JUDGMENT DISCOVERY

Post-judgment discovery need not be filed with the court. The party requesting discovery must give the responding party at least 30 days to respond to a post-judgment discovery request. The responding party may file a written objection with the court within 30 days of receiving the request. If an objection is filed, the judge must hold a hearing to determine if the request is valid. If the objection is denied, the judge must

order the party to respond to the request. If the objection is upheld, the judge may reform the request or dismiss it entirely.

SECTION 2. INSTITUTION OF SUIT

RULE 508. PLEADINGS AND MOTIONS

Except for oral motions during trial, or when all parties are present, all pleadings and motions must be written and signed by the party or its attorney, and an exact copy must be sent to all other parties to the suit by the party filing the motion or pleading as provided by Rule 515.

RULE 509. PETITION

(a) *Contents of Petition.* To initiate a suit, a petition must be filed with the court. A petition must contain:
   (1) the name, address, telephone number, and fax number, if any, of the plaintiff;
   (2) the name, address, and telephone number, if known, of the defendant;
   (3) the amount of money, if any, the plaintiff seeks;
   (4) a description and claimed value of any personal property the plaintiff seeks;
   (5) the basis for the plaintiff's claim against the defendant; and
   (6) any email contact information where the plaintiff consents to accept service of the answer and any other motions or pleadings. A party is not required to accept service by email.

(b) *Fees and Statement of Inability to Pay.* On filing the petition, the plaintiff must pay the appropriate filing fee and service fees, if any, with the court. A plaintiff who is unable to pay the fees must file a sworn statement that it is unable to do so.

   (1) *Contents of the Statement of Inability to Pay.* The statement must contain complete information as to the party's identity, nature and amount of governmental entitlement income, nature and amount of employment income, other income, (interest, dividends, et.), spouse's income if available to the party, property owned (other than homestead), cash or checking account, dependents, debts, and monthly expenses.

   The statement must contain the following: "I am unable to pay court costs. I verify that the statements made in this statement are true and correct." The statement shall be sworn before a notary public or other officer authorized to administer oaths or signed under penalty of perjury. If the party is represented by an attorney on a contingent fee basis, due to the party's indigency, the attorney may file a statement to that effect to assist the court in understanding the financial condition of the party.

   (2) *IOLTA Certificate.* If the party is represented by an attorney who is providing free legal services because of the party's indigency, without contingency, and the attorney is

providing services either directly or by referral from a program funded by the Interest on Lawyers Trust Accounts (IOLTA) program, the attorney may file an IOLTA certificate confirming that the IOLTA funded program screened the party for income eligibility under the IOLTA income guidelines. A party's statement of inability to pay accompanied by an attorney's IOLTA certificate may not be contested.

(3) *Contest.* The defendant may file a contest of the statement of inability to pay at any time within 20 days after the day the defendant's answer is due. If contested, the judge must hold a hearing to determine the plaintiff's ability to pay. The court may, regardless of whether the defendant contests the statement, examine the statement and conduct a hearing to determine the plaintiff's ability to pay. If the court finds the plaintiff is able to afford the fees, the plaintiff must pay the fees in the time specified by the court or the case will be dismissed without prejudice.

RULE 510. VENUE

Comprehensive laws regarding where a lawsuit may be brought may be found in Chapter 15, Subchapter E of the Texas Civil Practice and Remedies Code, which is available online at www.***therules.com*** and also is available for examination during the court's business hours.

Generally, a defendant in a small claims case or debt claim case is entitled to be sued in one of the following venues:

(a) In the county and precinct where the defendant resides;
(b) In the county and precinct where the incident, or the majority of incidents, that gave rise to the cause of action occurred;
(c) In the county and precinct where the contract or agreement, if any, that gave rise to the cause of action was to be performed; or
(d) In the county and precinct where the property is located, in a suit to recover personal property.

If the defendant is a non-resident of Texas, or if defendant's residence is unknown, the plaintiff may file the suit in the county and precinct where the plaintiff resides.

If a plaintiff files suit in an improper venue, the defendant may file a Motion to Transfer Venue under Rule 522. If the case is transferred, the plaintiff is responsible for the filing fees in the new court and is not entitled to a refund of any fees already paid.

RULE 522. MOTION TO TRANSFER VENUE

(a) *Motion.* If a defendant wishes to challenge the venue the plaintiff selected, the defendant may file a motion to transfer venue. This motion must be filed no later

than the 20th day after the day the defendant's answer is filed under Rule 516, and must contain a sworn statement that the venue chosen by the plaintiff is improper. The motion must also contain a specific county and precinct of proper venue to which transfer is sought. If the defendant fails to do so, the court must inform the defendant of the defect and allow the defendant 10 days to cure the defect. If the defendant fails to correct the defect, the motion will be denied, and the case will proceed in the county and precinct where it was originally filed.

(b) *Hearing.*

(1) *Procedure.*

(A) *Judge to Set Hearing.* In response to a motion to transfer venue, the judge shall set a hearing at which the motion will be considered.

(B) *Response.* A plaintiff may file a response to a defendant's motion to transfer venue.

(C) *Evidence and Argument.* The parties may present evidence and make legal arguments at the hearing. The defendant presents evidence and argument first. A witness may testify at a hearing, either in person or, with permission of the court, by means of telephone or an electronic communication system. Written documents offered by the parties may also be considered by the judge at the hearing

(2) *Judge's Decision.* The judge must either grant or deny the motion to transfer venue. If the motion is granted, the judge must sign an order designating the court to which the case will be transferred. If the motion is denied, the case will be heard in the court in which the plaintiff initially filed suit.

(3) *Further Consideration of Judge's Ruling.*

(A) *Motions for Rehearing.* Motions for rehearing of the judge's ruling on venue are not permitted.

(B) *Appeal.* No interlocutory appeal of the judge's ruling on venue is permitted.

(4) *Time for Trial of the Case.* No trial shall be held until at least the 15th day after the judge's ruling on the motion to transfer venue.

(c) *Order.* If the motion to transfer venue is granted, the court must issue an order of transfer stating the reason for the transfer and the name of the court to which the transfer is made. When such an order of transfer is made, the judge who issued the order must immediately make out a true and correct transcript of all the entries made on the docket in the cause,

certify the transcript, and send the transcript, with a certified copy of the bill of costs and the original papers in the cause, to the court in the precinct to which the case has been transferred. The court receiving the case must then notify the plaintiff that the case has been received and that the plaintiff has 10 days after receiving the notice to pay the filing fee in the new court, or file a sworn statement of inability to pay, as described in Rule 509. Failure to do so will result in the case being dismissed without prejudice.

RULE 523. FAIR TRIAL VENUE CHANGE

If a party believes they cannot get a fair trial in a specific precinct or before a specific judge, they may file a sworn statement stating such, and specifying if they are requesting a change of location or a change of judge. This statement must be filed no less than seven days before trial, unless the sworn statement shows good cause why it was not so filed. If the party seeks a change in presiding judge, the judge shall exchange benches with another qualified justice of the peace, or if no judge is available to exchange benches, the county judge shall appoint a visiting judge to hear the case. If the party seeks a change in location, the case shall be transferred to any other precinct in the county requested by the defendant. If no specific precinct is requested, it shall be transferred to the nearest justice court in the county. If there is only one justice of the peace precinct in the county, then the judge shall exchange benches with another qualified justice of the peace, or if no judge is available to exchange benches, the county judge shall appoint a visiting judge to hear the case. In cases where exclusive jurisdiction is within a specific precinct, as in Eviction Cases, the only remedy available is a change in presiding judge.

A party may apply for relief under this rule only one time in any given lawsuit.

RULE 524. CHANGE OF VENUE BY CONSENT

The venue shall also be changed to the court of any other justice of the peace of the county, or any other county, upon the written consent of all parties or their attorneys, filed with the court.

RULE 511. ISSUANCE AND FORM OF CITATION

(a) *Issuance.* When a petition is filed with a justice court to initiate a suit, the clerk must promptly issue a citation and deliver the citation as directed by the requesting party. The party filing the petition is responsible for obtaining service on the defendant of the citation and a copy of the petition with any documents filed with the petition. Upon request, separate or additional citations must be issued by the clerk. The clerk must retain a copy of the citation in the court's file.

(c) *Form.* The citation must:

(1) be styled "The State of Texas";

(2) be signed by the clerk under seal of court or by the judge;
(3) contain the name and location of the court;
(4) show the date of filing of the petition;
(5) show the date of issuance of the citation;
(6) show the file number and names of parties;
(7) state the plaintiff's cause of action and relief sought;
(8) be directed to the defendant;
(9) show the name and address of attorney for plaintiff, or if the plaintiff does not have an attorney, the address of plaintiff;
(10) contain the time within which the defendant is required to file a written answer with the court issuing citation;
(11) contain the address of the court; and
(12) must notify defendant that if the defendant fails to file an answer, judgment by default may be rendered for the relief demanded in the petition.

(c) *Notice*. The citation shall include the following notice to the defendant: "*You have been sued. You may employ an attorney to help you in defending against this lawsuit. But you are not required to employ an attorney. You or your attorney must file an answer with the court. Generally, your answer is due by the end of the 14th day after the day you were served with these papers. If the 14th day is a Saturday, Sunday, or legal holiday, your answer is due by the end of the first day following the 14th day that is not a Saturday, Sunday, or legal holiday.* ***Do not ignore these papers****. If you do not file an answer by the due date, a default judgment may be taken against you. For further guidance, consult Rules of Civil Procedure 500-575, which are available online at* ***www.therules.com*** *and also at the court listed on this citation.*" *If a statement of inability to pay has been filed by the plaintiff in this suit, you may have the right to contest that statement.*

(d) **Copies.** The party filing the petition shall provide enough copies to be served on each defendant. If they fail to do so, the clerk may make copies and charge the plaintiff the allowable copying cost.

RULE 512. SERVICE

The plaintiff is responsible for ensuring that the defendant is served with the citation, the petition and all documents filed with the petition. However, the plaintiff, or any other person with an interest in the case, **MAY NOT** directly serve the papers on the defendant. Instead, a plaintiff may have a defendant served with the citation by any of the following methods:

(a) Request the sheriff or constable to serve the defendant with the citation, the petition and all documents filed with the petition via personal delivery. The plaintiff must pay the service fee or provide a sworn statement that they are unable to pay it and why they are unable to.

(b) Request the court, sheriff or constable to serve the defendant with the citation, the petition and all documents filed with the petition via registered mail or certified mail, return receipt requested, restricted delivery requested. The plaintiff must pay a service fee that may not be higher than is necessary to pay the expenses of providing the services.

(c) Employ a certified private process server to serve the defendant with the citation, the petition and all documents filed with the petition via personal delivery, registered mail, or certified mail, return receipt requested, restricted delivery requested.

(d) File a written request with the court to allow any other uninterested party who is at least 18 years of age to serve the defendant with the citation, the petition and all documents filed with the petition via personal delivery, registered mail, or certified mail, return receipt requested, restricted delivery requested. If the court approves the request, the uninterested party may serve the defendant in any of the above listed methods.

If the method utilized is through registered mail or certified mail, return receipt requested, the defendant's signature must be present acknowledging receipt in order for the service to be valid. Additionally, a return of service must be completed as provided by Rule 575.

RULE 513. ALTERNATIVE SERVICE

If the methods under Rule 512 are insufficient to effect service on the defendant, the plaintiff, or the constable, sheriff, or certified process server if utilized, may make a request for alternative service. This request must include a sworn statement detailing the methods attempted under Rule 512. The request shall be that the citation, petition and documents filed with the petition be:

(a) mailed first class mail to the defendant, and also left at the defendant's residence or other place where the defendant can probably be found with any person found there who is at least 16 years of age, or

(b) mailed first class mail to the defendant, and also served by any other method that the movant feels is reasonably likely to provide the defendant with notice of the suit.

The judge shall determine if the method requested is reasonably likely to provide the defendant with notice of the suit, and if so, shall approve the service. If not, the requestor can request a different method.

RULE 514. SERVICE BY PUBLICATION

In the event that service of citation by publication is necessary, the process is governed by Rules 109-117 of the Rules of Civil Procedure.

RULE 515. SERVICE OF PAPERS OTHER THAN CITATION

Every notice required by these rules, and every pleading, plea, motion, or other form of request required to be served under these rules of civil procedure, other than the citation, may be served by a party to the suit, an attorney of record, a sheriff or constable, or by any other person competent to testify and may be served by:

(a) delivering a copy to the party to be served, or the party's duly authorized agent or attorney of record, as the case may be, in person or by agent;

(b) courier receipted delivery or by certified or registered mail, to the party's last known address. Service by certified or registered mail will be complete when the document is properly addressed and deposited in the United States mail, postage prepaid;

(c) fax to the recipient's current fax number. Service by fax after 5:00 p.m. local time of the recipient will be deemed to have been served on the following day;

(d) sending an email message to an email address expressly provided by the receiving party, if the party has consented to email service. Service by email after 5:00 p.m. local time of the recipient will be deemed to have been served on the following day; or,

(e) by such other manner as the court in its discretion may direct.

If service is effectuated by mail, three days will be added to the length of time a party has to respond to the document.

The party or its attorney of record must state in writing on all documents filed a signed statement describing the manner in which the document was served on the other party or parties and the date of service. A certificate by a party or its attorney of record, or the return of the officer, or the sworn statement of any other person showing service of a notice will be proof of service.

However, a party may offer evidence or testimony that the notice or instrument was not received, or, if service was by mail, that it was not received within three days from the date of mailing, and upon so finding, the court may extend the time for taking the action required of such party or grant such other relief as it deems just.

RULE 516. ANSWER FILED

(a) A defendant must file an answer to a lawsuit with the court and must also serve a copy of the answer on the plaintiff as provided by Rule 515. Generally, the defendant's answer is due by the end of the 14th day after the day the defendant was served with the citation and petition. If the 14th day is a Saturday, Sunday, or legal holiday, the defendant's answer is due by the end of the first day following the 14th day that is not a Saturday, Sunday, or legal holiday. Also, if the court closes before 5:00 PM on the day the answer is due under this rule, the answer is due on the next business day.

(b) *When the Defendant is Served by Publication.* A defendant served by publication must file an answer to a lawsuit with the court and must also serve a copy of the answer on the plaintiff as provided by Rule 515. Generally, the defendant's answer is due by the end of the 42nd day after the day the citation was first published. If the 42nd day is a Saturday, Sunday, or legal holiday, the defendant's answer is due by the end of the first day following the 42nd day that is not a Saturday, Sunday, or legal holiday. Also, if the court closes before 5:00 PM on the day the answer is due under this rule, the answer is due on the next business day.

RULE 517. GENERAL DENIAL

A general denial of the plaintiff's cause of action is sufficient to constitute an answer or appearance and does not bar the defendant from raising specific defenses at trial. The defendant's appearance must be noted on the court's docket.

RULE 518. COUNTERCLAIM

A defendant who seeks relief from a plaintiff arising from the same transaction or occurrence that is the subject matter of the plaintiff's suit must file a counterclaim if the relief sought is within the jurisdiction of the justice court. The defendant may file a counterclaim if they seek any other relief from the plaintiff that is within the jurisdiction of the justice court. The counterclaim petition must follow the requirements of Rule 509, including the requirement of a filing fee or a sworn statement of inability to pay the fees to the court where the initial suit is pending. The court need not generate a citation for a counterclaim and no answer to the counterclaim need be filed. The defendant must serve a copy of the counterclaim on the plaintiff and all other parties as provided by Rule 515.

RULE 519. CROSS-CLAIM

A plaintiff seeking relief against a co-plaintiff, or a defendant seeking relief against a co-defendant may file a cross-claim. The filing party must include all information in its petition that is required under Rule 509, and it must pay a filing fee or provide a sworn statement of inability to pay the fees to the court where the initial suit is pending. A citation must be issued and served as provided by Rule 512 on any party that has not yet filed a petition or an answer, as appropriate. A citation is not necessary if the party filed

against has filed a petition or an answer, but the filing party must serve the cross-claim as provided by Rule 515.

RULE 520. THIRD-PARTY CLAIM

A defendant seeking to bring another party into a suit who may be liable for all or part of the plaintiff's claim against the defendant may file a petition as provided in Rule 509, and must pay a filing fee or provide a sworn statement of inability to pay the fees. A citation must be issued and served as provided by Rule 512.

RULE 521. INSUFFICIENT PLEADINGS

Any party may file a motion with the court asking that another party be required to clarify a pleading. The court shall determine if the pleading is sufficient to place all parties on notice of the issues in the lawsuit, and may hold a hearing to make that determination. If it is insufficient, the court shall order the party to amend the pleading, and shall set a date by which the party shall make the needed corrections. If the party fails to make the required corrections, its pleading may be dismissed.

SECTION 3. TRIAL

RULE 525. IF DEFENDANT FAILS TO ANSWER

If the defendant fails to file an answer by the due date listed in Rule 516, the judge must ensure that service was proper, and may hold a hearing for this purpose. If it is determined that proper service did occur, the judge must proceed in the following manner:

(a) If the plaintiff's claim is based on a written instrument executed and signed by both parties, and a copy of this instrument has been filed with the court and served on the defendant, along with a sworn statement from the plaintiff that this is a true and accurate copy of the instrument and the relief sought is owed, and all payments, offsets or credits due to the defendant have been accounted for, the judge shall proceed to render judgment for the plaintiff in the requested amount, without necessity of a hearing. The plaintiff's attorney may also submit affidavits supporting an award of reasonable and necessary attorney's fees, if they are so entitled, and the court may also award those fees.

(b) If the suit is a Debt Claim case that is filed with all required documentation, as provided in Rule 578, the judge shall proceed to render judgment for the plaintiff in the requested amount, without necessity of a hearing. The plaintiff's attorney may also submit affidavits supporting an award of reasonable and necessary attorney's fees, if they are so entitled, and the court may also award those fees.

(c) In situations other than those described in (a) and (b) above, the plaintiff must request, orally or in writing, a default judgment hearing if it seeks the entry of a default judgment against the defendant. If the defendant files a written answer with the court before the default judgment is granted, the default judgment may not be awarded. If the defendant does not answer, the plaintiff must appear at the default judgment hearing and provide evidence of its damages. If the plaintiff proves its damages, the judge shall render judgment for the plaintiff in the amount proven. If the plaintiff is unable to prove its damages, the judge shall render judgment in favor of the defendant. With the permission of the court, a party may appear at a hearing by means of telephone or an electronic communication system.

RULE 526. SUMMARY DISPOSITION

(a) *Motion.* A party may file a motion with the court requesting judgment in its favor without a need for trial. A plaintiff's motion for summary disposition should state that there is no genuine dispute of any material fact in the case, and that it is therefore entitled to judgment as a matter of law. A defendant's motion for summary disposition should state that the plaintiff has no evidence of one or more essential elements of its claim against the defendant.

(b) *Hearing.* If a summary disposition motion is filed, the judge must hold a hearing, unless all parties waive the hearing in writing. Parties may respond to the motion orally at the hearing, unless the court orders them in writing to reduce their responses to writing, which may or may not be sworn, at the discretion of the court.

(c) *Order.* The court may enter judgment after the hearing as to an entire claim, or parts of a claim, as the evidence requires. The court should deny the motion if any material factual dispute exists.

RULE 527. SETTING

After the defendant answers, the case will be set on a pretrial docket or a trial docket at the discretion of the judge. The date, time, and place of this setting must be sent to all parties at their address of record no less than 45 days before the setting date, unless the judge determines that an earlier setting is required in the interest of justice. All subsequent settings must be sent to both parties at their address of record.

RULE 528. CONTINUANCE

The judge, for good cause shown, may continue any setting pending before the court to some other time or day.

RULE 529. JURY TRIAL DEMANDED

Any party is entitled to a trial by jury. A party wishing to request a jury trial must pay the jury fee and submit a written request for a jury no later than the 20th day after the date the defendant's answer was filed. If the jury is not timely requested, the right to a jury is waived. If, after a case is docketed for a jury trial, the party who demanded the jury thereafter withdraws the demand, the case will remain on the jury docket unless all other parties present agree to try the case without a jury. A party withdrawing its jury demand is not entitled to a refund of the jury fee.

RULE 530. IF NO DEMAND FOR JURY

If no party timely demands a jury and pays the jury fee, the judge will try the cause without a jury.

RULE 531. PRETRIAL CONFERENCE

If all parties have appeared in a suit, any party may request, or the court may order a pretrial conference. Appropriate issues for this setting include:

(a) Discovery issues;
(b) The need for amendment or clarification of pleadings;
(c) The admission of facts and documents to streamline the trial process;
(d) Limitation on the number of witnesses at trial;
(e) Identification of facts, if any, which are not in dispute between the parties.
(f) Ordering the parties to mediation or other alternative dispute resolution services;
(g) The possibility of settlement;
(h) Trial setting dates that are amenable to the court and all parties;
(i) Appointment of interpreters, if needed;
(j) Any other issue that the court deems appropriate.

RULE 531a. ALTERNATIVE DISPUTE RESOLUTION

It is the policy of this state to encourage the peaceable resolution of disputes thru alternative dispute resolution, including mediation, and the early settlement of pending litigation through voluntary settlement procedures. It is the responsibility of judges and their court administrators to carry out this policy and develop an alternative dispute resolution system to encourage peaceable resolution in all justice court suits. For that purpose the judge may order any justice court case to mediation or another appropriate and generally accepted alternative dispute resolution process.

RULE 532. TRIAL SETTING

On the day of the trial setting, the judge must call all of the cases set for trial that day. If the plaintiff fails to appear when the cause is called in its order for trial, the judge may postpone or dismiss the suit. If the defendant fails to appear when the cause is called in its order for trial, the judge may postpone the cause, or may proceed to take evidence. If

the plaintiff proves its case, judgment must be awarded for the relief proven. If the plaintiff fails to prove its case, judgment must be rendered in favor of the defendant.

RULE 533. DRAWING JURY AND OATH

If no method of electronic draw has been implemented, the judge must write the names of all the jurors present on separate slips of paper, as nearly alike as may be, and shall place them in a box and mix them well, and shall then draw the names one by one from the box, and write them down as they are drawn, upon several slips of paper, and deliver one slip to each of the parties, or their attorneys.

After the draw, the judge must swear the panel as follows: "You, and each of you, do solemnly swear or affirm that you will give true and correct answers to all questions asked of you concerning your qualifications as a juror, so help you God."

RULE 534. VOIR DIRE

The parties or their attorneys will be allowed to question jurors as to their ability to serve impartially in the given trial but may not ask the jurors how they will rule in the case. The judge will have discretion to allow or disallow specific questions and determine the amount of time each side will have for this process.

RULE 535. CHALLENGE FOR CAUSE

If any party desires to challenge any juror for cause, such challenge will be made during voir dire. The party should explain to the judge why the juror will be prejudiced or biased, and therefore should be excluded from the jury. The judge will evaluate the questions and answers given and either grant or deny the challenge. When a juror has been challenged for cause, and the challenge has been sustained, the juror must be dismissed.

RULE 536. PEREMPTORY CHALLENGE

After challenges for cause are complete, the parties may make their peremptory challenges in the manner prescribed by the judge. Each party will be entitled to three peremptory challenges, which means they may select up to three jurors whom they may dismiss for any reason, or no reason at all, other than membership in a Constitutionally protected class.

RULE 537. THE JURY

After peremptory challenges have been made, the judge will call off the first remaining six names that have not been eliminated by a peremptory challenge or challenge for cause, and these six will constitute the jury to try the case.

RULE 538. IF JURY IS INCOMPLETE

If the jury by challenge for cause or peremptory challenges is left incomplete, the judge will direct the sheriff or constable to summon others to complete the jury; and the same proceedings will be had in selecting and impaneling such jurors as are had in the first instance.

RULE 539. JURY SWORN

When the jury has been selected, they must be sworn by the judge. The form of the oath must be in substance as follows: "***You and each of you do solemnly swear or affirm that in all cases between parties which shall be to you submitted you will a true verdict render, according to the law and the evidence, so help you God.***"

RULE 540. JUDGE MUST NOT CHARGE JURY

The judge must not charge the jury in any civil cause tried in his court before a jury.

RULE 541. JURY VERDICT

When the suit is for the recovery of specific articles, the jury must, if they find for the plaintiff, assess the value of each article separately, according to the proof presented at trial.

SECTION 4. JUDGMENT

RULE 545. JUDGMENT UPON JURY VERDICT

Where the case has been tried by a jury and a verdict has been returned by them, the judge will announce the same in open court and note it in the court's docket, and will proceed to render judgment thereon.

RULE 546. CASE TRIED BY JUDGE

When the case has been tried before the judge without a jury, the judge must announce the decision in open court and note the same in the court's docket and render judgment accordingly.

RULE 547. JUDGMENT

The judgment must be recorded at length in the judge's docket, and must be signed by the judge. The judgment is effective from the date of signature. The judgment must clearly state the determination of the rights of the parties in the subject matter in controversy and the party who must pay the costs, and must direct the issuance of such process as may be necessary to carry the judgment into execution.

RULE 548. COSTS

The successful party in the suit will recover its costs, except in cases where it is otherwise expressly provided.

RULE 549. JUDGMENT FOR SPECIFIC ARTICLES

Where the judgment is for the recovery of specific articles, their value must be separately assessed, and the judgment will be that the plaintiff recover such specific articles, if they can be found, and if not, then their value as assessed with interest at the prevailing post-judgment interest rate.

RULE 550. TO ENFORCE JUDGMENT

The court will cause its judgments to be carried into execution, and where the judgment is for personal property the court may award a special writ for the seizure and delivery of such property to the plaintiff, and may, in addition to the other relief granted in such cases, enforce its judgment by contempt.

RULE 551. ENFORCEMENT OF JUDGMENT

Justice court judgments are enforceable in the same method as in county and district court, except as provided by applicable law.

SECTION 5. NEW TRIAL

RULE 555. SETTING ASIDE DEFAULT JUDGMENTS AND DISMISSALS

A plaintiff whose case is dismissed may file a motion within ten days of that dismissal seeking reinstatement. The plaintiff must serve the defendant with a copy of this motion no later than the next business day using a method approved under Rule 515. The court may reinstate the case on good cause shown.

A defendant against whom a default judgment is granted may file a motion within ten days of that judgment seeking the judgment to be set aside. The defendant must serve the plaintiff with a copy of this motion no later than the next business day using a method approved under Rule 515. The court may set aside the judgment and proceed with a trial setting on good cause shown.

If a court denies either of these motions, the party making the motion is entitled to appeal that decision as provided by SECTION 6, and will receive a trial de novo at county court if they successfully perfect the appeal.

RULE 556. NEW TRIALS

A party may file a motion for a new trial within ten days of the signing of judgment. They must give notice to the other party of this motion no later than the next business

day. The judge may grant a new trial upon a showing that justice was not done in the trial of the cause. A party does not need to file a motion for new trial in order to appeal.

RULE 557. ONLY ONE NEW TRIAL

Only one new trial may be granted to either party.

RULE 558. MOTION DENIED AS A MATTER OF LAW

If the judge has not ruled on a motion to set aside a dismissal or default judgment, or a motion for new trial, the motion is automatically denied at 5:00 PM on the 20th day after the day the judgment was signed.

SECTION 6. APPEAL

RULE 560. APPEAL

(a) *Plaintiff's Appeal.* If the plaintiff wishes to appeal the judgment of the court, the plaintiff or its agent or attorney shall file a bond in the amount of $500 with the judge no later than the 20th day after the judgment is signed or the motion for new trial, if any, is denied. The bond must be supported by such surety or sureties as are approved by the judge, or cash in lieu of surety, must be payable to the appellee, and must be conditioned that the appellant will prosecute its appeal to effect and will pay off and satisfy such costs if judgment or costs be rendered against it on appeal.

(b) *Defendant's Appeal.* If the defendant wishes to appeal the judgment of the court, the defendant or its agent or attorney must file a bond with the judge no later than the 20th day after the judgment is rendered or the motion for new trial, if any, is denied. This bond is calculated by doubling the amount of the judgment rendered in justice court. The bond must be supported by such surety or sureties as are approved by the judge, or cash in lieu of surety, must be payable to the appellee, and must be conditioned that the appellant will prosecute its appeal to effect and will pay off and satisfy the judgment which may be rendered against it on appeal.

(c) *Appeal Perfected.* When such bond has been filed with the court, the appeal will be held to be perfected. The appeal will not be dismissed for defects or irregularities in procedure, either of form or substance, without allowing appellant five days after notice within which to correct or amend same. This notice will be given by the court to which the cause has been appealed.

(d) *Notice Required.* Within five days following the filing of such appeal bond, the party appealing must give notice as provided in Rule 515 of the filing of such bond to all parties to

the suit who have not filed such bond. No judgment may be taken by default against any party in the court to which the cause has been appealed without first showing compliance with this rule.

RULE 561. INABILITY TO PAY APPEAL COSTS

A party that wishes to appeal, but is unable to pay the costs of appeal, or secure adequate sureties, may appeal by filing a sworn statement of this inability no later than the 20th day after the judgment was signed or the motion for new trial, if any, was overruled. This statement must include the contents of section (a) below. The statement may be the same one that accompanied the filing of the petition, if one was filed at that time. Notice of this statement must be given by the court to the other party no later than the next business day.

(a) *Contents of the Statement of Inability to Pay.* The statement must contain complete information as to the party's identity, nature and amount of governmental entitlement income, nature and amount of employment income, other income, (interest, dividends, et.), spouse's income if available to the party, property owned (other than homestead), cash or checking account, dependents, debts, and monthly expenses.

The statement must contain the following: "I am unable to pay court costs. I verify that the statements made in this statement are true and correct." The statement shall be sworn before a notary public or other officer authorized to administer oaths or signed under penalty of perjury. If the party is represented by an attorney on a contingent fee basis, due to the party's indigency, the attorney may file a statement to that effect to assist the court in understanding the financial condition of the party.

(b) *IOLTA Certificate.* If the party is represented by an attorney who is providing free legal services because of the party's indigency, without contingency, and the attorney is providing services either directly or by referral from a program funded by the Interest on Lawyers Trust Accounts (IOLTA) program, the attorney may file an IOLTA certificate confirming that the IOLTA funded program screened the party for income eligibility under the IOLTA income guidelines. A party's statement of inability to pay accompanied by an attorney's IOLTA certificate may not be contested.

(c) *Contest.* The sworn statement is presumed true and will be accepted to allow the appeal unless the opposing party files a contest within five days after receiving notice of the statement. If contested, the judge must hold a hearing to determine the plaintiff's ability to pay. At the hearing, the burden is on the party who filed the statement to prove its inability to pay. The judge should make a written finding as to the inability of the appellant to pay. If the judge rules that the party desiring to appeal is able to pay the costs of appeal, the party desiring to appeal may appeal the judge's ruling to the county court

within five days of the judge's ruling, or may post an appeal bond complying with Rule 560 with the justice court within five days of the judge's ruling.

(d) *Appeal of Ruling.* If the decision is appealed by the appealing party, the judge shall send all papers to the county court. The county court shall set a day for hearing, not later than ten days after the appeal, and shall hear the contest de novo, and if the appeal is granted, shall direct the justice of the peace to transmit to the clerk of the county court, the transcript, records and papers of the case, as provided in these rules. If the county court denies the appeal, the party will have five days to post an appeal bond that satisfies Rule 560 in order to perfect its appeal.

RULE 563. TRANSCRIPT

Whenever an appeal has been perfected from the justice court, the judge who made the order, or the judge's successor, must immediately make out a true and correct copy of all the entries made on the docket in the cause, and certify thereto officially, and immediately send it together with a certified copy of the bill of costs taken, and the original papers in the cause, to the clerk of the county court, or other court having jurisdiction.

RULE 564. NEW MATTER MAY BE PLEADED

No new ground of recovery may be set up by the plaintiff, nor may any set-off or counterclaim be set up by the defendant which was not pleaded in the justice court.

RULE 565. TRIAL DE NOVO

The cause shall be tried de novo in the county court.

SECTION 7. ADMINISTRATIVE RULES FOR JUDGES, COURT PERSONNEL AND SERVERS OF PROCESS

RULE 570. PLENARY POWER

A justice court loses plenary power over a case at any of the following times:

(a) An appeal is perfected;

(b) 20 days have expired since the judgment was signed if no motion for new trial was filed; or

(c) 20 days have expired since the motion for new trial was overruled.

RULE 571. FORMS

A justice court may provide blank forms to enable a party to file documents that comply with these rules. No party may be forced to use the court's forms.

RULE 572. DOCKET

Each justice of the peace must keep a civil docket, which may be maintained electronically, in which judge will enter:

(a) The title of all suits commenced before the court.

(b) The time when the first process was issued against the defendant, when returnable, and the nature of that process.

(c) The time when the parties, or either of them, appeared before the court, either with or without a citation.

(d) A copy of the petition filed by plaintiff, and any documents filed with the petition.

(e) Every adjournment, stating at whose request and to what time.

(f) The time when the trial was had, stating whether the same was by a jury or by the judge.

(g) The verdict of the jury, if any.

(h) The judgment signed by the judge and the time of signing same.

(i) All applications for setting aside judgments or granting new trials and the orders of the judge thereon, with the date thereof.

(j) The time of issuing execution, to whom directed and delivered, and the amount of debt, damages and costs; and, when any execution is returned, the judge must note such return on said docket, with the manner in which it was executed.

(k) All stays and appeals that may be taken, and the time when taken, the amount of the bond and the names of the sureties.

The judge must also keep such other dockets, books and records as may be required by law or these rules, and must keep a fee book in which shall be taxed all costs accruing in every suit commenced before the court.

RULE 573. ISSUANCE OF WRITS

Every writ from the justice courts must be issued by the judge, be in writing and signed by the judge officially. The style thereof must be "The State of Texas." It must, except where otherwise specially provided by law or these rules, be directed to the person or

party upon whom it is to be served, be made returnable to some regular term of court, and note the date of its issuance.

RULE 574. WHO MAY SERVE AND METHOD OF SERVICE

No person who is a party to or interested in the outcome of a suit may serve any process, and, unless otherwise authorized by a written court order, only a sheriff or constable may serve a writ that requires the actual taking possession of a person, property, or thing, or process requiring that an enforcement action be physically enforced by the person delivering the process. No fee may be imposed for issuance of an order authorizing a person to serve process.

RULE 575. DUTY OF OFFICER OR PERSON RECEIVING AND RETURN OF CITATION

(a) The officer or authorized person to whom process is delivered must endorse on the process the date and hour on which he or she received it, and execute and return the same without delay.

(b) The officer or authorized person executing the citation must complete a return of service. The return may, but need not, be endorsed on or attached to the citation.

(c) The return, together with any document to which it is attached, must include the following information:

(1) the cause number and case name;
(2) the court in which the case is filed;
(3) a description of what was served;
(4) the date and time the process was received for service;
(5) the person or entity served;
(6) the address served;
(7) the date of service or attempted service;
(8) the manner of delivery of service or attempted service;
(9) the name of the person who served or attempted service;
(10) if the person named in (9) is a process server certified under Supreme Court Order, his or her identification number and the expiration date of his or her certification; and
(11) any other information required by rule or law.

(d) When the citation was served by registered or certified mail as authorized by Rule 536, the return by the officer or authorized person must also contain the receipt with the addressee's signature.

(e) When the officer or authorized person has not served the citation, the return must show the diligence used by the officer or authorized person to execute the same and

the cause of failure to execute it, and where the defendant is to be found, if ascertainable.

(f) The officer or authorized person who serves or attempts to serve a citation must sign the return. If the return is signed by a person other than a sheriff, constable, or clerk of the court, the return must either be verified or be signed under penalty of perjury. A return signed under penalty of perjury must contain the statement below in substantially the following form:

"My name is _____, my date of birth is _____, and my address is (Street) (City) (State) (Zip Code) (County), and I declare under penalty of perjury that the foregoing is true and correct.
Executed in _____County, State of _____, on the ____day of (Month), (Year)

_____
Declarant"

(g) Where citation is executed by an alternative method as authorized by Rule 513, proof of service must be made in the manner ordered by the court.

(h) The return and any document to which it is attached must be filed with the court and may be filed electronically or by fax, if those methods of filing are available.

(i) No default judgment may be granted in any cause until proof of service as provided by this rule, or as ordered by the court in the event citation is executed by an alternative method under Rule 513, has been on file with the clerk of the court three (3) days, exclusive of the day of filing and the day of judgment.

SECTION 8. DEBT CLAIM CASES

RULE 576. SCOPE

(a) This section applies to:
(1) Any financial institution seeking to collect on an alleged consumer debt;
(2) Any collection agency seeking to collect on an alleged consumer debt;
(3) Any assignee seeking to collect on an alleged consumer debt;
(4) Any original creditor who extended credit on a revolving or open-end account and seeks to collect on that debt; and
(5) Any original creditor who is primarily engaged in the business of lending money at interest and seeks to collect the debt on the money loaned.

(b) This chapter does not apply to:
(1) Any original creditor who is not primarily engaged in the business of lending money at interest and who is also not a financial institution; and

(2) An original creditor or assignee seeking to collect a deficiency balance after the disposition of collateral in a consumer transaction involving a secured debt.

RULE 577. PLAINTIFFS PLEADINGS

(a) The following information must be set forth in the petition of a suit filed under this chapter:

(1) The defendant's name and address as appearing on the original creditor's records;
(2) The name of the original creditor;
(3) The original account number;
(4) The date of origination/issue of the account;
(5) The date and amount of the last payment;
(6) The charge-off date and amount;
(7) If the plaintiff seeks post-charge-off interest, then the petition shall state whether the rate is based on contract default or statute, and the amount of post-charge-off interest claimed;
(8) If the plaintiff is represented by an attorney, then the attorney's name, address, and telephone number; and
(9) Whether the plaintiff is the original creditor.

(b) If the plaintiff is not the original creditor, the petition shall also state:
(1) The date on which the debt was assigned to the plaintiff;
(2) The name of each previous owner of the account and the date on which the debt was assigned to that owner.

(c) If the plaintiff is a third party debt collector, the debt collector must plead that it has complied with Texas Finance Code Section 392.101 requiring a bond. The petition should include the name of the bonded debt collector and the date it filed a copy of the bond with the Texas Secretary of State.

RULE 578 DEFAULT JUDGMENTS

(a) *Default Judgment Without Hearing.* The following documents may be attached to the petition, and must be served on the defendant before a default judgment can be granted without a hearing:

(1) A copy of the contract, promissory note, charge-off statement or an original document evidencing the original debt which must contain a signature of the defendant. This document shall be supported by affidavit from the original creditor.

(2) If a claim is based on credit card debt and no such signed writing evidencing the original debt ever existed, then a copy of the card member agreement in effect at the time the card was charged-off and copies of documents generated when the credit card was actually used must be attached and shall be supported by affidavit from the original creditor.

(b) *Required Documents.* To support a default judgment, these documents must include:

(1) A document signed by the defendant evidencing the debt or the opening of the account; or
(2) a bill or other record reflecting purchases, payments, or other actual use of the credit card or account by the defendant; or
(3) an electronic printout or other documentation from the original creditor establishing the existence of the account and showing purchases, payments, or other actual use of a credit card or account by the defendant.

(c) *Requirements of Affidavit.* Any affidavit from the original creditor must state:

(1) that they were kept in the regular course of business,
(2) that it was the regular course of business for an employee or representative of the creditor with knowledge of the act, event, condition, opinion, or diagnosis, recorded to make the record or to transmit information to be included in such record;
(3) the record was made at or near the time or reasonably soon thereafter; and
(4) the records attached are the original or exact duplicates of the original.

(d) *Default Judgment after Hearing.* If the plaintiff does not file with the court and serve on the defendant the documents required above, and the defendant files a timely answer, the court will proceed with the case as usual. If the plaintiff does not file with the court and serve on the defendant the documents required above, and the defendant fails to file a timely answer, the case will proceed under Rule 525(c). If a defendant who had failed to answer appears at a default judgment hearing, the judge must reset the case or may proceed with trial on the merits, if all parties agree to proceed.

(e) *Post-Answer Default.* If a defendant who has answered fails to appear for trial, the court may proceed to hear evidence and render judgment accordingly.

SECTION 9. PROCEEDINGS TO ENFORCE LANDLORD'S DUTY TO REPAIR OR REMEDY RESIDENTIAL RENTAL PROPERTY

RULE 737.1. APPLICABILITY OF RULE

This rule applies to a suit filed in a justice court by a residential tenant under Chapter 92, Subchapter B of the Texas Property Code to enforce the landlord's duty to repair or

remedy a condition materially affecting the physical health or safety of an ordinary tenant. Rules 500-575 also apply to the extent they are not inconsistent with this rule.

RULE 737.2. CONTENTS OF PETITION; COPIES; FORMS AND AMENDMENTS

(a) *Contents of Petition.* The petition must be in writing and must include the following:

(1) the street address of the residential rental property;

(2) a statement indicating whether the tenant has received in writing the name and business street address of the landlord and landlord's management company;

(3) to the extent known and applicable, the name, business street address, and telephone
number of the landlord and the landlord's management company, on-premises manager, and rent collector serving the residential rental property;

(4) for all notices the tenant gave to the landlord requesting that the condition be repaired or remedied:

(A) the date of the notice;

(B) the name of the person to whom the notice was given or the place where the notice was given;

(C) whether the tenant's lease is in writing and requires written notice;

(D) whether the notice was in writing or oral;

(E) whether any written notice was given by certified mail, return receipt requested, or by registered mail; and

(F) whether the rent was current or had been timely tendered at the time notice was given;

(5) a description of the property condition materially affecting the physical health or safety of an ordinary tenant that the tenant seeks to have repaired or remedied;

(6) a statement of the relief requested by the tenant, including an order to repair or remedy a condition, a reduction in rent, actual damages, civil penalties, attorney's fees, and court costs;

(7) if the petition includes a request to reduce the rent:

(A) the amount of rent paid by the tenant, the amount of rent paid by the

government, if known, the rental period, and when the rent is due; and

(B) the amount of the requested rent reduction and the date it should begin;

(8) a statement that the total relief requested does not exceed $10,000, excluding interest and court costs but including attorney's fees; and

(9) the tenant's name, address, and telephone number.

(b) *Copies.* The tenant must provide the court with copies of the petition and any attachments to the petition for service on the landlord.

(c) *Forms and Amendments.* A petition substantially in the form promulgated by the Supreme Court is sufficient. A suit may not be dismissed for a defect in the petition unless the tenant is given an opportunity to correct the defect and does not promptly correct it.

RULE 737.3. CITATION: ISSUANCE; APPEARANCE DATE

(a) *Issuance.* When the tenant files a written petition with a justice court, the judge must immediately issue citation directed to the landlord, commanding the landlord to appear before such judge at the time and place named in the citation.

(b) *Answer Date.* The answer date on the citation must not be earlier than the seventh day nor later than the fourteenth day after the date of service of the citation. For purposes of this rule, the answer date on the citation is the trial date.

RULE 737.4. SERVICE AND RETURN OF CITATION; ALTERNATIVE SERVICE OF CITATION

(a) *Service and Return of Citation.* The sheriff, constable, or other person authorized by Rule 512 who receives the citation must serve the citation by delivering a copy of it, along with a copy of the petition and any attachments, to the landlord at least six days before the answer date. At least three days before the answer date, the person serving the citation must return the citation, with the action written on the citation, to the justice of the peace who issued the citation. The citation must be issued, served, and returned in like manner as ordinary citations issued from a justice court.

(b) *Alternative Service of Citation.*
(1) If the petition does not include the landlord's name and business street address, or if, after making diligent efforts on at least two occasions, the sheriff, constable, or other, person authorized by Rule 512 is unsuccessful in serving the citation on the landlord under (a), the sheriff, constable, or other person authorized by Rule 512 must serve the citation by delivering a copy of the citation, petition, and any attachments to:

(A) the landlord's management company if the tenant has received written notice

of the name and business street address of the landlord's management company; or

(B) if (b)(1)(A) does not apply and the tenant has not received the landlord's name and business street address in writing, the landlord's authorized agent for service of process, which may be the landlord's management company, on-premise manager, or rent collector serving the residential rental property.

(2) If the sheriff, constable, or other person authorized by Rule 512 is unsuccessful in serving citation under (b)(1) after making diligent efforts on at least two occasions at either the business street address of the landlord's management company, if (b)(1)(A) applies, or at each available business street address of the landlord's authorized agent for service of process, if (b)(1)(B) applies, the sheriff, constable, or other person authorized by Rule 512 must execute and file in the justice court a sworn statement that the sheriff, constable, or other person authorized by Rule 512 made diligent efforts to serve the citation on at least two occasions at all available business street addresses of the landlord and, to the extent applicable, the landlord's management company, on-premises manager, and rent collector serving the residential rental property, providing the times, dates, and places of each attempted service. The judge may then authorize the sheriff, constable, or other person authorized by Rule 512 to serve citation by:

(A) delivering a copy of the citation, petition, and any attachments to someone over the age of sixteen years, at any business street address listed in the petition, or, if nobody answers the door at a business street address, either placing the citation, petition, and any attachments through a door mail chute or slipping them under the front door, and if neither of these latter methods is practical, affixing the citation, petition, and any attachments to the front door or main entry to the business street address;

(B) within 24 hours of complying with (b)(2)(A), sending by first class mail a true copy of the citation, petition, and any attachments addressed to the landlord at the landlord's business street address provided in the petition; and
(C) noting on the return of the citation the date of delivery under (b)(2)(A) and the date of mailing under (b)(2)(B).

The delivery and mailing to the business street address under (b)(2)(A)-(B) must occur at least six days before the answer date. At least one day before the answer date, the citation, with the action written thereon, must be returned to the judge who issued the citation. It is not necessary for the tenant to request the alternative service authorized by this rule.

RULE 737.5. REPRESENTATION OF PARTIES

Parties may represent themselves. A party may also be represented by an authorized agent, but nothing in this rule authorizes a person who is not an attorney licensed to practice law in this state to represent a party before the court if the party is present.

RULE 737.6. DOCKETING AND TRIAL; FAILURE TO APPEAR; CONTINUANCE

(a) *Docketing and Trial.* The case shall be docketed and tried as other cases. The judge may develop the facts of the case in order to ensure justice.

(b) *Failure to Appear.*

(1) If the tenant appears at trial and the landlord has been duly served and fails to appear at trial, the judge may proceed to hear evidence. If the tenant establishes that the tenant is entitled to recover, the judge shall render judgment against the landlord in accordance with the evidence.

(2) If the tenant fails to appear for trial, the judge may dismiss the suit.

(c) *Continuance.* The judge may continue the trial for good cause shown. Continuances should be limited, and the case should be reset for trial on an expedited basis.

RULE 737.7. DISCOVERY

Reasonable discovery may be permitted. Discovery is limited to that considered appropriate and permitted by the judge and must be expedited. In accordance with Rule 215, the judge may impose any appropriate sanction on any party who fails to respond to a court order for discovery.

RULE 737.8. JUDGMENT: AMOUNT; FORM AND CONTENT; ISSUANCE AND SERVICE; FAILURE TO COMPLY

(a) *Amount.* Judgment may be rendered against the landlord for failure to repair or remedy a condition at the residential rental property if the total judgment does not exceed $10,000, excluding interest and court costs but including attorney's fees. Any party who prevails in a suit brought under these rules may recover the party's court costs and reasonable attorney's fees as allowed by law.

(b) *Form and Content.*

(1) The judgment must be in writing, signed, and dated and must include the names of the parties to the proceeding and the street address of the residential rental property where the condition is to be repaired or remedied.

(2) In the judgment, the judge may:

(A) order the landlord to take reasonable action to repair or remedy the condition;

(B) order a reduction in the tenant's rent, from the date of the first repair notice,

in proportion to the reduced rental value resulting from the condition until the condition is repaired or remedied;

(C) award a civil penalty of one month's rent plus $500;

(D) award the tenant's actual damages; and

(E) award court costs and attorney's fees, excluding any attorney's fees for a cause of action for damages relating to a personal injury.

(3) If the judge orders the landlord to repair or remedy a condition, the judgment must include in reasonable detail the actions the landlord must take to repair or remedy the condition and the date when the repair or remedy must be completed.

(4) If the judge orders a reduction in the tenant's rent, the judgment must state:

(A) the amount of the rent the tenant must pay, if any;

(B) the frequency with which the tenant must pay the rent;

(C) the condition justifying the reduction of rent;

(D) the effective date of the order reducing rent;

(E) that the order reducing rent will terminate on the date the condition is repaired or remedied; and

(F) that on the day the condition is repaired or remedied, the landlord must give the tenant written notice, served in accordance with Rule 515, that the condition justifying the reduction of rent has been repaired or remedied and the rent will revert to the rent amount specified in the lease.

(c) *Issuance and Service.* The judge must issue the judgment. The judgment may be served on the landlord in open court or by any means provided in Rule 515 at an address listed in the citation, the address listed on any answer, or such other address the landlord furnishes to the court in writing. Unless the judge serves the landlord in open court or by other means provided in Rule 512 , the sheriff, constable, or other person authorized by Rule 512 who serves the landlord must promptly file a certificate of service in the justice court.

(d) *Failure to Comply.* If the landlord fails to comply with an order to repair or remedy a condition or reduce the tenant's rent, the failure is grounds for citing the landlord for contempt of court under Section 21.002 of the Government Code.

RULE 737.9. COUNTERCLAIMS

Counterclaims and the joinder of suits against third parties are not permitted in suits under these rules. Compulsory counterclaims may be brought in a separate suit. Any potential causes of action, including a compulsory counterclaim, that are not asserted because of this rule are not precluded.

RULE 737.10. POST-JUDGMENT MOTIONS: TIME AND MANNER; DISPOSITION; NUMBER

(a) *Time and Manner.* A party may file a motion for new trial, a motion to amend the judgment, or a motion to set aside a default judgment or a dismissal for want of prosecution. The motion must be in writing and filed within ten days after the date the justice signs the judgment or dismissal order.

(b) *Disposition.*

(1) If the justice grants a motion for new trial or a motion to set aside a default judgment
or a dismissal for want of prosecution, the resulting trial must occur within ten days
after the date the justice signs the order granting the motion.

(2) If the justice grants a motion to amend the judgment, the justice must amend the
judgment within fifteen days after the date the justice signs the original judgment.

(3) If the justice does not rule on a motion for new trial, a motion to amend the judgment, or a motion to set aside a default judgment or a dismissal for want of prosecution with a written, signed order within fifteen days after the justice signs the judgment or dismissal order, the motion is considered overruled by operation of law on expiration of that period.

(c) *Number.* A party may file only one motion for new trial, one motion to amend the judgment, and one motion to set aside a default judgment or a dismissal for want of prosecution.

RULE 737.11. PLENARY POWER

The justice court's plenary power expires when a party perfects an appeal. If a party does not perfect an appeal, the justice court has plenary power to grant a new trial, amend or vacate the judgment, or set aside a default judgment or a dismissal for want of prosecution within fifteen days after the date the judge signs the judgment or dismissal order.

RULE 737.12. APPEAL: TIME AND MANNER; PERFECTION; EFFECT; COSTS; TRIAL ON APPEAL

(a) *Time and Manner.* Either party may appeal the decision of the justice court to a statutory county court or, if there is no statutory county court with jurisdiction, a county court or district court with jurisdiction by filing a written notice of appeal with the justice court within twenty days after the date the judge signs the judgment. If the judgment is amended in any respect, any party has the right to appeal within twenty days after the date the judge signs the new judgment, in the same manner set out in this rule.

(b) *Perfection.* The posting of an appeal bond is not required for an appeal under these rules, and the appeal is considered perfected with the filing of a notice of appeal. Otherwise, the appeal is in the manner provided by law for appeal from a justice court.

(c) *Effect.* The timely filing of a notice of appeal stays the enforcement of any order to repair or remedy a condition or reduce the tenant's rent, as well as any other actions.

(d) *Costs.* The appellant must pay the costs on appeal to a county court in accordance with Rule 143a.

(e) *Trial on Appeal.* On appeal, the parties are entitled to a trial de novo. Either party is entitled to trial by jury on timely request and payment of a fee, if required. An appeal of a judgment of a justice court under these rules takes precedence in the county court and may be held at any time after the eighth day after the date the transcript is filed in the county court.

RULE 737.13. EFFECT OF WRIT OF POSSESSION

If a judgment for the landlord for possession of the residential rental property becomes final, any order to repair or remedy a condition is vacated and unenforceable.

Comment to 2010 change: *The heading of repealed Rule 737, regarding bills of discovery, is deleted. New Rule 737 is promulgated pursuant to Senate Bill 1448 to provide procedures for a tenant's request for relief in a justice court under Section 92.0563(a) of the Property Code. Except when otherwise specifically provided, the terms in Rule 737 are defined consistent with Section 92.001 of the Property Code. All suits must be filed in accordance with the venue provisions of Chapter 15 of the Civil Practice and Remedies Code.*

SECTION 10. EVICTION CASES

RULE 738. COMPUTATION OF TIME FOR EVICTION CASES

All time periods in this section refer to calendar days, including periods of five days or less. The day of an act, event, or default shall not count for any purpose. If a time period ends on a Saturday, Sunday or legal holiday, it shall be extended to the next day that is not a Saturday, Sunday or legal holiday. If the final day of any specified time period falls on a day that the court closed before 5:00 PM, the time period is extended to the court's next business day. A document may be filed by mail, but must be received by the court

on or before the due date. A document may be filed by fax, but must be faxed no later than 5:00 pm on the date that the document is due, and a document filed by fax must also be filed by mail, postmarked on or before the due date, or personally delivered to the court within five days.

RULE 739. PETITION

A petition in an eviction case must be sworn to by the plaintiff, and must contain:

(a) A description of the premises that the plaintiff seeks possession of;
(b) A description of the facts and the grounds for eviction;
(c) A description of when and how notice to vacate was delivered;
(d) The total amount of rent sought by the plaintiff, if any;
(e) Attorneys fees, if applicable, if any.

The petition must be filed in the precinct where the property is located. If it is filed in a precinct other than the precinct where all or part of the property is located, the judge shall dismiss the case. The plaintiff will not be entitled to a refund of the filing fee, but will be refunded any service fees paid if the case is dismissed before service is attempted.

A plaintiff must name as defendants in a petition all tenants obligated under a lease residing at the premises who plaintiff seeks to evict. No judgment or writ of possession shall issue or be executed against a tenant obligated under a lease and residing at the premises who is not named in the petition and not served with citation pursuant to these rules, except that a writ may be executed against occupants not obligated under a lease but claiming under the tenant or tenants.

RULE 740. MAY SUE FOR RENT

A suit for rent may be joined with an eviction case, wherever the suit for rent is within the jurisdiction of the justice court. In such case the court in rendering judgment in the eviction case, may at the same time render judgment for any rent due the landlord by the renter; provided the amount thereof is within the jurisdiction of the justice court.

RULE 741. CITATION

When the plaintiff or his authorized agent shall file his written sworn petition with such justice court, the court shall immediately issue citation directed to the defendant or defendants commanding them to appear before such judge at a time and place named in such citation, such time being not more than fourteen days nor less than seven days from the date of filing of the petition. The citation shall include a copy of the sworn petition and all documents filed by the plaintiff, and shall inform the parties that, upon timely request and payment of a jury fee no later than three days before the date set for trial in the citation, the case shall be heard by a jury, and must contain all warnings provided for in Chapter 24 of the Texas Property Code. Additionally, it should include the following

statement: "For additional assistance, consult Rules of Civil Procedure 500-575 and 738-755. These rules may be viewed at ***www.therules.com*** and are also available at the court listed on this citation."

Note to Rules Committee RE: RULE 742. ***The Task Force was evenly split on whether we should eliminate this rule and thus eliminate Immediate Possession Bonds, or keep it as revised below. No other ruled generated so much discussion and strong opinion among the Task Force, although all members agreed that current Rule 740 of the TRCP is very problematic. Those who wished to eliminate this remedy felt that it is adverse to tenants rights, and is capable of being abused. Those who felt that we should keep it felt that it was an important remedy for landlords to protect their property in certain situations. In the end, we decided to present both our suggestions for revision and suggestions for removal and allow the Supreme Court to decide. Either solution would require minor changes in the Property Code. If this Rule is eliminated, so must Rule 750c and the clause at the end of Rule 749.***

RULE 742. REQUEST FOR IMMEDIATE POSSESSION

(a) *Request for Immediate Possession.* The plaintiff, at the time of filing the petition, may additionally file a sworn statement requesting immediate possession, alleging specific facts that should entitle the plaintiff to possession of the premises during any appeal. If the plaintiff files this statement it must also post a bond, in cash or surety, in an amount approved by the judge. The surety may be the landlord or its agent.

(b) *Calculation of Bond.* The judge shall determine the amount of the bond. This may be done with an ex parte hearing with the landlord, and should cover defendant's damages if a writ of possession is issued, and then later revoked upon appeal. The amount could include moving expenses, additional rent, loss of use, attorney fees, and court costs.

(c) *Notice to Defendant.* The defendant must be served a notice of the plaintiff's Request for Immediate Possession, including a copy of this statement in 12 point **bold** or underlined print: "**A request for immediate possession has been filed in this case. If judgment is rendered against you, you may only have 24 hours to move from this property after judgment. To preserve your right to remain in the property during an appeal, if any, you must post a counterbond in an amount set by the court. Contact the court IMMEDIATELY if you wish to post a counterbond. If this request has been improperly filed, you may be entitled to recover your damages from the plaintiff.**"

(d) *Counterbond.* If the defendant seeks to post a counterbond, the court should set it in an amount that will cover the plaintiff's damages if the defendant maintains possession of the property during appeal. If the defendant posts a counterbond, in cash or in surety approved by the court, the case will proceed in the usual manner for eviction cases.

(e) *Default Judgment.* If the plaintiff is awarded a judgment by default, plaintiff will be awarded a writ of possession at any time after judgment is rendered upon request and payment of applicable fees, unless defendant has posted a counterbond as described in subsection (d).

(f) *Contested Hearing.* If the defendant appears for trial, and plaintiff is awarded judgment for possession, the judge shall proceed to hear evidence and argument from all parties regarding the issue of immediate possession. If it is determined that the plaintiff's interests will not be adequately protected during the normal appeal procedure, the judge may require that a defendant post a bond if the defendant wishes to remain in possession of the premises during appeal, if any. This bond can be a counterbond as described above in subsection (d), or an appeal bond as described by Rule 750. Unless the defendant posts a counterbond or perfects an appeal with a bond as described by Rule 750, the writ of possession shall be issued after the expiration of five days upon request of the plaintiff and payment of the applicable fees.

(g) *Forfeiture of Original Bond.* If the defendant is dispossessed of the property and subsequently is awarded possession at the county court, the defendant will be entitled to recover actual damages resulting from its exclusion, which damages may be awarded from a forfeiture of the plaintiff's original bond. If the defendant posts a counterbond and remains in possession, the county court will make a determination of the plaintiff's damages, if any, which may be awarded from a forfeiture of the defendant's counterbond.

RULE 743. SERVICE OF CITATION

The constable, sheriff, or other person authorized by written court order receiving such citation shall execute the same by delivering a copy of it to the defendant, or by leaving a copy thereof with some person, other than the plaintiff, over the age of sixteen years, at his usual place of abode, at least six days before the day set for trial; and no later than three days before the day assigned for trial he shall return such citation, with his action written thereon, to the court who issued the same.

RULE 743a. SERVICE BY DELIVERY TO PREMISES

If the sworn complaint lists all home and work addresses of the defendant which are known to the person filing the sworn complaint, and if it states that such person knows of no other home or work addresses of the defendant in the county where the premises are located, service of citation may be by delivery to the premises in question as follows:

If the officer receiving such citation is unsuccessful in serving such citation under Rule 743, the officer shall, no later than five days after receiving such citation, execute a sworn statement that the officer has made diligent efforts to serve such citation on at least two occasions at all addresses of the defendant in the county where the premises are located as may be shown on the sworn complaint, stating the times and places of attempted service. Such sworn statement shall be filed by the officer with the judge who shall

promptly consider the sworn statement of the officer. The judge may then authorize service according to the following:

(a) The officer will place the citation, including the petition and all documents filed with the petition, inside the premises by placing it through a door mail chute or by slipping it under the front door; and if neither method is possible or practical, the officer will securely affix the citation to the front door or main entry to the premises.

(b) The officer will that same day or the next day deposit in the mail a true copy of such citation, including the petition and all documents filed with the petition, with a copy of the sworn complaint attached thereto, addressed to defendant at the premises in question and sent by first class mail;

(c) The officer will note on the return of such citation the date of delivery under (a) above and the date of mailing under (b) above; and

(d) Such delivery and mailing to the premises must occur at least six days before the day set for trial; and at least one day before the day assigned for trial he must return such citation with his action written thereon, to the court which issued the same. It shall not be necessary for the aggrieved party or his authorized agent to make request for or motion for alternative service pursuant to this rule.

RULE 744. DOCKETED

The cause will be docketed and tried as other cases. No eviction trial may be held less than six days after service under Rule 743 or 743a has been obtained. If the defendant files an answer but fails to appear for trial, the court will proceed to hear evidence from the plaintiff, and render judgment accordingly. If the defendant fails to appear at trial and fails to file an answer, the allegations of the complaint may be taken as admitted and judgment by default entered accordingly.

RULE 745. DEMANDING JURY

Any party shall have the right of trial by jury, by making a request to the court at least three days before the day set for trial, and by paying a jury fee. Upon such request, a jury shall be summoned as in other cases in justice court.

RULE 746. TRIAL POSTPONED

For good cause shown by either party, the trial may be postponed not exceeding seven days. A continuance may exceed seven days if both parties agree in writing.

RULE 747. ONLY ISSUE

In eviction cases, the only issue shall be the right to actual possession; and the merits of the title shall not be adjudicated.

RULE 748. TRIAL

If no jury is demanded by either party, the judge will try the case. If a jury is demanded by either party, the jury will be empanelled and sworn as in other cases; and after hearing the evidence it will return its verdict in favor of the plaintiff or the defendant as it shall find.

RULE 748a. REPRESENTATION BY AGENTS

In eviction cases for non-payment of rent or holding over beyond the rental term, the parties may represent themselves or be represented by their authorized agents who need not be attorneys. In eviction cases for any other reason, if a party is a corporation, it may be represented by its authorized agent who need not be an attorney. All other parties may either appear in person to represent themselves otherwise they must be represented by their attorney.

RULE 749. JUDGMENT AND WRIT

If the judgment or verdict be in favor of the plaintiff, the judge will give judgment for plaintiff for possession of the premises, costs, attorney's fees, and back rent, if any; and he must award a writ of possession upon demand of the plaintiff and payment of any required fees. If the judgment or verdict be in favor of the defendant, the judge will give judgment for defendant against the plaintiff for costs and attorney's fees, if any. No writ of possession may issue until the expiration of five days from the time the judgment is signed, except as provided by Rule 742.

A writ of possession may not be issued after the 30th day after a judgment for possession is signed, and a writ of possession expires if not executed by the 30th day after the date it is issued. If the 30th day falls on a Saturday, Sunday, or legal holiday, for the purpose of satisfying this rule, it will become the next day that is not a Saturday, Sunday or legal holiday.

RULE 750. MAY APPEAL

In appeals in eviction cases, no motion for new trial may be filed.

Either party may appeal from a final judgment in such case, to the county court of the county in which the judgment is rendered by filing with the judge within five days after the judgment is signed, a bond to be approved by said judge, and payable to the adverse party, conditioned that the appellant will prosecute its appeal with effect, or pay all costs and damages which may be adjudged against it. The judge will set the amount of the bond to include the items enumerated in Rule 753. Within five days following the filing of such bond, the party appealing shall give notice as provided in Rule 515 of the filing of such bond to the adverse party. No judgment shall be taken by default against the adverse

party in the court to which the cause has been appealed without first showing substantial compliance with this rule.

RULE 750a. INABILITY TO PAY APPEAL COSTS IN EVICTION CASES

(a) *Contents of Statement.* If a party wishes to appeal, but is unable to pay the costs of appeal, or secure adequate sureties, it may appeal by filing a sworn statement of its inability to pay the costs of appeal no later than the fifth day after the judgment was rendered. The justice court must make available a form that a person may use to comply with these requirements. Notice of this statement must be given by the court to the other party no later than the next business day. The statement must contain the following information:

(1) the tenant's identity;
(2) the nature and amount of the tenant's employment income;
(3) the income of the tenant's spouse, if applicable and available to the tenant;
(4) the nature and amount of any governmental entitlement income of the tenant;
(5) all other income of the tenant;
(6) the amount of available cash and funds available in savings or checking accounts of the tenant;
(7) real and personal property owned by the tenant, other than household furnishings, clothes, tools of a trade, or personal effects;
(8) the tenant's debts and monthly expenses; and
(9) the number and age of the tenant's dependents and where those dependents reside

(b) *IOLTA Certificate.* If the party is represented by an attorney who is providing free legal services, without contingency, because of the party's indigency and the attorney is providing services either directly or by referral from a program funded by the Interest on Lawyers Trust Accounts (IOLTA) program, the attorney may file an IOLTA certificate confirming that the IOLTA funded program screened the party for income eligibility under the IOLTA income guidelines. A party's affidavit of inability accompanied by an attorney's IOLTA certificate may not be contested.

(c) *Contest.* The sworn statement is presumed to be true and will be accepted to allow the appeal unless the opposing party files a contest within five days after receiving notice of the statement. If the opposing party contests a statement not accompanied by an IOLTA certificate, the judge shall hold a hearing no later than the fifth day after the contest is filed. At the hearing, the burden is on the party who filed the statement to prove its inability to pay. The judge should make a written finding as to the inability of the appellant to pay. If the judge rules that the statement is denied, the party who filed it may appeal that decision by filing, within five days, a written contest with the justice court, which will then forward the matter and related documents to the county court for resolution, or the party may post an appeal bond complying with Rule 750 with the justice court within one day from the date the order denying the pauper's affidavit is signed.

(d) *Appeal of Decision.* If the decision is appealed, the judge shall send all papers to the county court. The county court shall set a day for a hearing, not later than five days after the appeal, and shall hear the contest de novo, and if the appeal is granted, shall direct the justice of the peace to transmit to the clerk of the county court, the transcript, records and papers of the case, as provided in these rules. If the county court denies the appeal, the party will have one day to post an appeal bond that satisfies Rule 750 in order to perfect its appeal.

RULE 750b. PAYMENT OF RENT DURING NONPAYMENT OF RENT APPEALS

(a) *Notice to Pay Rent into Registry.* If a tenant files a pauper's affidavit in an eviction for nonpayment of rent, the justice court shall provide to the tenant a written notice at the time the pauper's affidavit is filed that contains the following information in bold or conspicuous type:

(1) the amount of the initial deposit of rent stated in the judgment that the tenant must pay into the justice court registry;

(2) whether the initial deposit must be paid in cash, cashier's check, or money order, and to whom the cashier's check or money order, if applicable, must be made payable;

(3) the calendar date by which the initial deposit must be paid into the justice court registry, which must be within five days of the date the tenant files the pauper's affidavit;

(4) for a court that closes before 5 p.m. on the date specified by Subdivision (3), the time the court closes; and

(5) a statement that failure to pay the required amount into the justice court registry by the date prescribed by Subdivision (3) may result in the court issuing a writ of possession without hearing.

(b) *Failure to Pay Rent.* If a tenant fails to do comply with the notice in subsection (a), the landlord is entitled, upon request and payment of the applicable fee, to a writ of possession, which will issue immediately and without hearing. The appeal will then be sent up to county court in the usual manner for cases with perfected appeals.

(c) *Payment of Rent During Appeal.* If an eviction case is based on nonpayment of rent, and the tenant appeals by paupers affidavit, the tenant must pay the rent, as it becomes due, into the justice court or the county court registry, as applicable, during the pendency of the appeal. During the appeal process as rent becomes due under the rental agreement, the tenant/appellant shall pay the rent into the county court registry within five days of the due date under the terms of the rental agreement. If a government agency is responsible for all or a portion of the rent under an agreement with the landlord, the tenant shall pay only that portion of the rent determined by the justice court to be paid by the tenant during appeal, subject to either party's right to contest that determination under

Subsection (c).

(d) *Contest of Amount Paid by Tenant.* If an eviction case is based on nonpayment of rent and the tenant's rent during the rental agreement term has been paid wholly or partly by a government agency, either party may contest the portion of the rent that the justice court determines must be paid into the county court registry by the tenant under this section. The contest must be filed on or before the fifth day after the date the justice signs the judgment. If a contest is filed, not later than the fifth day after the date the contest is filed the justice court shall notify the parties and hold a hearing to determine the amount owed by the tenant in accordance with the terms of the rental agreement and applicable laws and regulations. After hearing the evidence, the justice court shall determine the portion of the rent that must be paid by the tenant under this section.

(e) *Objection to Ruling.* If the tenant objects to the justice court's ruling under Subsection (d) on the portion of the rent to be paid by the tenant during appeal, the tenant shall be required to pay only the portion claimed by the tenant to be owed by the tenant until the issue is tried de novo along with the case on the merits in county court. During the pendency of the appeal, either party may file a motion with the county court to reconsider the amount of the rent that must be paid by the tenant into the registry of the court.

(e) *Contests at Same Hearing.* If either party files a contest under Subsection (d) and the tenant files a pauper's affidavit that is contested by the landlord, the justice court shall hold the hearing on both contests at the same time.

(f) *Remedies in County Court.* Landlord/appellee may withdraw any or all rent in the county court registry upon a) sworn motion and hearing, prior to final determination of the case, showing just cause, b) dismissal of the appeal, or c) order of the court upon final hearing. If the tenant/appellant fails to pay the rent into the court registry within the time limits prescribed by these rules, the appellee may file a notice of default in county court. Upon sworn motion by the appellee and a showing of default to the judge, the court shall issue a writ of possession. All hearings and motions under this rule shall be entitled to precedence in the county court.

RULE 750c. PAUPER'S AFFIDAVIT IN CASES WITH IMMEDIATE POSSESSION BONDS

If a tenant seeks to appeal a judgment of possession awarded in an eviction case where plaintiff filed a bond for immediate possession under Rule 742, and possession was granted to plaintiff by default, or awarded to the plaintiff following a contested hearing where the judge ordered the defendant to post a bond if the defendant seeks to appeal, the defendant may still perfect an appeal with a pauper's affidavit.

However, the defendant must post a counterbond as provided by Rule 742 if they wish to remain in possession of the premises during the appeal. If the defendant fails to do so, the court shall, upon request and payment of any applicable fee by the landlord, issue a writ of possession before sending the appeal to the county court

RULE 750c. APPEAL PERFECTED

When an appeal bond has been timely filed in conformity with Rule 750, or a pauper's affidavit approved in conformity with Rule 750a or 750b, the appeal shall be perfected.

RULE 751. FORM OF APPEAL BOND

The appeal bond authorized in the preceding article may be substantially as follows:

"The State of Texas,

"County of _____

"Whereas, upon a writ of forcible entry (or forcible detainer) in favor of A.B., and against C.D., tried before , a justice of the peace of county, a judgment was rendered in favor of the said A.B. on the _____ day of _____, A.D. _____, and against the said C.D., from which the said C.D. has appealed to the county court; now, therefore, the said C.D. and his sureties, covenant that he will prosecute his said appeal with effect and pay all costs and damages which may be adjudged against him, provided the sureties shall not be liable in an amount greater than $_____, said amount being the amount of the bond herein.

"Given under our hands this _____ day of _____, A.D. _____."

RULE 752. TRANSCRIPT

When an appeal has been perfected, the judge must stay all further proceedings on the judgment, and immediately make out a transcript of all the entries made on the docket of the proceedings had in the case; and must immediately file the same, together with the original papers and any money in the court registry, including sums tendered pursuant to Rule 750b(a), with the clerk of the court having jurisdiction of such appeal. The clerk must docket the cause, and the trial will be de novo. The clerk must immediately notify both appellant and the adverse party of the date of receipt of the transcript and the docket number of the cause. Such notice must advise the defendant of the necessity for filing a written answer in the county court when the defendant has pleaded orally in the justice court. The trial, as well as all hearings and motions, will be entitled to precedence in the county court.

RULE 753. DAMAGES ON APPEAL

On the trial of the cause in the county court the appellant or appellee will be permitted to plead, prove and recover his damages, if any, suffered for withholding or defending possession of the premises during the pendency of the appeal. Damages may include but are not limited to loss of rentals during the pendency of the appeal and reasonable attorney fees in the justice and county courts provided, as to attorney fees, that the

requirements of Section 24.006 of the Texas Property Code have been met. Only the party prevailing in the county court will be entitled to recover damages against the adverse party. The prevailing party will also be entitled to recover court costs and to recover against the sureties on the appeal bond in cases where the adverse party has executed such bond.

RULE 754. JUDGMENT BY DEFAULT ON APPEAL

Said cause will be subject to trial at any time after the expiration of eight full days after the date the transcript is filed in the county court. If the defendant has filed a written answer in the justice court, the same shall be taken to constitute his appearance and answer in the county court, and such answer may be amended as in other cases. If the defendant made no answer in writing in the justice court, and if he fails to file a written answer within eight full days after the transcript is filed in the county court, the allegations of the complaint may be taken as admitted and judgment by default may be entered accordingly.

RULE 755. WRIT OF POSSESSION ON APPEAL

The writ of possession, or execution, or both, will be issued by the clerk of the county court according to the judgment rendered, and the same will be executed by the sheriff or constable, as in other cases. The judgment of the county court may not be stayed unless within 10 days from the judgment the appellant files a supersedeas bond in an amount set by the county court pursuant to Texas Property Code 24.007 and Texas Rule of Appellate Procedure 24.

JUSTICE COURT RULES TASK FORCE REPORT

The purpose of this document is to give the Texas Supreme Court and its Advisory Committee (and any other interested party) a look into the logic and reasoning behind the proposed rules submitted by the task force. I have also included some comments and proposed modifications from the June meeting. I welcome any comments/questions, and am very happy to help in any way possible to make the new Justice Court the best tool that it can be, for judges, attorneys and pro-se parties alike.

Bronson Tucker
General Counsel
Texas Justice Court Training Center
Bt16@txstate.edu
(512) 663-6686 (cell)

SMALL CLAIMS COURT RULES

There was some discussion that we were being too detailed and thorough in these rules. The majority of the Task Force felt that clearly delineating the process would help lay judges and litigants alike, and ensure that speedy, inexpensive justice is available to all who come to the Justice Court.

RULE 500 – DEFINITIONS

This rule we want to be as thorough as possible. As mentioned, we hope for "one-stop shopping" for laypeople to be able to understand what's happening with their case. Any additions or clarifications always welcome. Judge Yelenosky mentioned defining "consumer debt".

RULE 501 – JUSTICE COURT CASES

Straightforward, trying to clarify each type of case and that the specific section controls, then the general rules apply where there are no specific rules. Need to give a specific Section number to the basic rules, since Part V also includes Section 8.

RULE 502 – APPLICATION OF RULES IN JUSTICE COURT

Our goal was to make these rules one-stop shopping, while also allowing flexibility for unforeseen circumstances. Strong arguments were made to eliminate the 'except as the judge sees fit' language from this. The Task Force feels strongly that it is important to have some

discretion built into the rule. The SCAC liked language last time of "Civil cases in justice court will be conducted in accordance with Rule V of the Rules of Civil Procedure."

RULE 503 – COMPUTATION OF TIME AND TIMELY FILING

There is currently confusion about how to count days, sometimes weekends and holidays are counted and sometimes they are not. We sought to streamline and clarify this by making all timeframes simply calendar days. We added the provision about 5:00 PM to be fair to litigants when a court closes early on a 'deadline day'.

RULE 504 – RULES OF EVIDENCE

SCAC voted to change to "The Rules of Evidence do not apply to justice court. The judge will review any evidence and determine what will be considered by the judge or jury." There was also discussion of combining 502 and 504.

RULE 505 – DUTY OF THE JUDGE TO DEVELOP THE CASE

Currently in Ch. 28 of the Government Code. Adds 'person' to clarify that a judge can summon a person to be a witness who isn't listed as a party, consistent with common interpretation of the current rule. Also, proposal made to replace the first 'may' with 'shall, if necessary'

RULE 506 – EXCLUSION OF WITNESSES

"The Rule" from the TRE.

RULE 506.1 – SUBPOENAS

From the current TRCP.

RULE 507 – PRETRIAL DISCOVERY

Implemented the concept from the current Small Claims Court, with some fleshing out of details. Court must approve discovery before it is served.

RULE 507.1 – POST-JUDGMENT DISCOVERY

Eliminates the requirement that post-j/m discovery be filed, but sets up a system where the responding party may object to the discovery and receive a hearing to determine if the request is valid. Gives more freedom to the now-judgment creditor without shutting out the judgment debtor from access to the court.

RULE 508 – PLEADINGS AND MOTIONS

Mandates that all pleadings and motions be written and signed, except for oral motions during trial or when all parties are present. The current antiquated system allows for oral pleadings which are listed in the docket, and fail to provide adequate notice.

RULE 509 – PETITION

Again, our stated objective was to provide information about proceeding with a case that makes it clear to pro se litigants what the steps are. This walks through what should be in the petition, how payment (or affidavit of inability) is handled, and how a party may contest an affidavit of inability.

RULE 510 – VENUE

We discussed in-depth whether we should include the "general" venue rules. We included them because they cover 99% of cases, and we direct laypeople to the proper statute for a full description of proper venue, which will be hosted online and will be available at the court.

RULE 522 (WOULD RENUMBER) – MOTION TO TRANSFER VENUE

We made significant changes to the current MTV procedure. The largest is that the defendant can file this motion up to 20 days after the day they answer, instead of being mandatory that they file it concurrent with or prior to their answer. Our reasoning is to allow some leeway to pro se litigants who often trap themselves by answering without realizing they are permanently waiving venue.

RULE 523 (WOULD RENUMBER) – FAIR TRIAL VENUE CHANGE

Pretty significant changes here too, due to the failings of current Rule 528, which is the only method a party has for challenging a judge in our court, because the recusal rules were held not to apply to our court. The main failings of current 528 are that it merely says to transfer to the nearest JP in the county (some counties only have one JP, what if all JPs in county DQd?), and that it possibly offers tenants a permanent defense against eviction, since jurisdiction is only precinct-wide in eviction cases. This rule addresses those by: 1) making the party state if they object to the judge or the location; 2) providing procedures in cases where there is only one judge in a county, or all are disqualified; and 3) only allowing a change in presiding judge and not location in eviction suits.

RULE 524 (WOULD RENUMBER) – CHANGE OF VENUE BY CONSENT

Same as current TRCP.

RULE 511 – ISSUANCE AND FORM OF CITATION

Changes time for answer from "Monday next following expiration of 10 days" to "14th day after served". Also adds more information to the notice and directs the defendant to the location online and at the court of these rules of procedure for further guidance.

RULE 512 – SERVICE

Clarifies and lays out the proper method of service, and informs that a return must be filed. Some have argued against laying out this information, but it is very helpful as this process is intimidating to non-lawyers. Language in (b) may need to change to reflect that the commissioners court has authority under LGC 118.131 to set a fee that the constable can charge for certified mail service.

RULE 513 – ALTERNATIVE SERVICE

Clarifies the current procedure for alternative service. Also allows the constable or process server to make the request for alternative service. This is frequently done, though as written it should be the plaintiff making the motion. However, the process server/officer is the individual with the information regarding the service attempt and can best decide what method will actually effect service.

RULE 514 – SERVICE BY PUBLICATION

Rare enough that we were comfortable using the district court rules and directing parties to the specific rules that apply.

RULE 515 – SERVICE OF PAPERS OTHER THAN CITATION

This is the JP version of Rule 21a. We added some clarifications, and also added email service as valid if, and only if, a party has consented to email service.

RULE 516 – ANSWER FILED

Similar language to the current rule, except we have simplified the answer timeline to 14 days instead of Monday after 10. As outlined in the computation rule above, if the court closes before 5 on the 14th day, the answer is due the next business day.

RULE 517 – GENERAL DENIAL

Bringing elements of Rule 92 into our rules, and also ensuring a simplified process and avoiding trapdoors by specifying that a GD does not bar the defendant from later raising specific defenses.

RULE 518 – COUNTERCLAIM

Addresses a current problem where sometimes a mandatory counterclaim is outside the JP court jurisdiction by making it mandatory only if it is within the court's jurisdiction.

RULE 519 – CROSS-CLAIM

No substantive changes.

RULE 520 – THIRD-PARTY CLAIM

No substantive changes.

RULE 521 – INSUFFICIENT PLEADINGS

Simplified procedure for special exceptions with the general concept remaining unchanged.

RULE 525 – IF DEFENDANT FAILS TO ANSWER

This rule is a major issue in our courts. One issue is that whether a hearing is required currently hinges on whether the damages are liquidated or not. Appellate courts have disagreed as to the definition of liquidated damages, so we instead created a system where the specific filings dictate whether a hearing is necessary. A hearing is not necessary in a suit based on a sworn filing based on a claim on a written instrument, or in Debt Claim Cases where all required documentation under Rule 578 has been filed. Otherwise, a hearing must occur. We added into the rule the caselaw rule that a default j/m may not be rendered if the defendant answers before j/m is granted, and added a provision that parties may appear telephonically or electronically with consent of the court.

We think this rule, as modified, will make it clear when a hearing is necessary, will make parties' rights clearer, and will allow more convenient hearings where appropriate.

RULE 526 – SUMMARY DISPOSITION

There was some debate over the role of summary judgment in these Rules. Ultimately, we decided that the ability to summarily get rid of cases where there is no material factual dispute is too important to judicial efficiency and fairness to lose. However, the current system is fraught with peril for the unfamiliar. We have eliminated the affidavit requirement, and also allow a party to offer oral response, unless the judge orders them to respond in writing. Some judges expressed concern at allowing oral response at the hearing, but at least this way, the party is put on written notice that they must respond in writing, as opposed to showing up at the hearing and being told they can't speak.

RULE 527 – SETTING

Current rule in justice court is the first setting must be at least 45 days out, while small claims court has no minimum timeframe. This rule sets a baseline of 45 days, but allows the judge to set the case earlier if it is in the interest of justice.

RULE 528 – CONTINUANCE

No substantive changes.

RULE 529 – JURY TRIAL DEMANDED

A considerable problem in our courts is the current rule allowing a jury to be demanded as late as the day before trial. This rule changes that to mandate a jury request no later than 20 days after filing an answer. This will allow courts to plan their dockets and will eliminate last minute jury requests which frequently result in continuances, delay, and frustration.

RULE 530 – IF NO DEMAND FOR JURY

No substantive change.

RULE 531 – PRETRIAL CONFERENCE

Sets up parameters for pretrial conferences as a tool for parties and courts. TAA has expressed concern about this being applied in eviction cases. We would support an addition either explicitly eliminating eviction cases from this rule, or stating that a pretrial is only appropriate in eviction cases if it can be held without delaying the timeframes found in the eviction rules.

RULE 531A – ALTERNATIVE DISPUTE RESOLUTION

Makes explicit that a judge can order mediation or other ADR. TAA has expressed concern about this being applied in eviction cases. We would support an addition either explicitly eliminating eviction cases from this rule, or stating that ADR is only appropriate in eviction cases if it can be implemented without delaying the timeframes found in the eviction rules.

RULE 532 – TRIAL SETTING

Specifies what happens on trial day. Some are opposed to the judge being able to postpone the case if the defendant doesn't appear, and feel that it should be automatic that the plaintiff can put on evidence. The majority felt that since the judge could postpone instead of dismiss if the plaintiff failed to appear, that the converse should also be true.

RULE 533 – DRAWING JURY AND OATH

No substantive changes, just addressed the issue of electronic draw, as many counties have implemented one.

RULE 534 – VOIR DIRE

Explained the process in clear language to let laypeople know what to expect at this stage.

RULE 535 – CHALLENGE FOR CAUSE

No substantive change, just rewritten in (hopefully) clearer language for laypeople.

RULE 536 – PEREMPTORY CHALLENGE

Allows the judge to control the method of peremptories instead of mandating antiquated procedures. Clarifying language.

RULE 537 – THE JURY

No substantive changes.

RULE 538 – IF JURY IS INCOMPLETE

No substantive changes, though there was discussion on whether this was still the best method to fill incomplete juries (sending the constable/sheriff to round up citizens)

RULE 539 – JURY SWORN

No substantive changes.

RULE 540 – JUDGE MUST NOT CHARGE JURY

No substantive changes. There was considerable debate on whether this was a good rule to keep. The benefits of explaining the law to the jury was ultimately outweighed by the drawbacks of long, drawn-out charge conference interfering with the speediness objective of our court.

RULE 541 – JURY VERDICT

RULE 545 – JUDGMENT UPON JURY VERDICT

RULE 546 – CASE TRIED BEFORE JUDGE

RULE 547 – JUDGMENT

RULE 548 – COSTS

RULE 549 – JUDGMENT FOR SPECIFIC ARTICLES

No substantive changes. However, if we can't get the Gov't Code modified to exclude costs from the amount in controversy, we should add to Rule 548 language making costs optional. As it exists now, if I sue for $10k in justice court and win, I am now outside the jurisdiction because costs "shall" be awarded, and GC says costs count against amount in controversy, so the j/m of $10,031 is over the limit.

RULE 550 – TO ENFORCE JUDGMENT

Replaced "attachment, fine, and imprisonment" with "contempt", since debtor's prison is not allowed in Texas.

RULE 551 – ENFORCEMENT OF JUDGMENT

Clarifies that the court has the tools available in district and county court at its disposal, ensuring that we haven't written out executions, sequestrations, garnishments, etc.

RULE 555 – SETTING ASIDE DEFAULT JUDGMENTS AND DISMISSALS

Clarifies the reinstatement and setting aside a default judgment procedures, and makes the timeframes consistent at 10 days to file either. Makes explicit that a plaintiff can appeal their dismissal if the judge declines to reinstate their case.

RULE 556 – NEW TRIALS

Extends from 5 to 10 days the period to request a new trial.

RULE 557 – ONLY ONE NEW TRIAL

No changes.

RULE 558 – MOTION DENIED AS A MATTER OF LAW

Extends from 10 to 20 days the deadline where the above motions are auto-denied.

RULE 560 – APPEAL

Several changes: 1) extends time from 10 to 20 days to file an appeal; 2) changes appeal bond for losing plaintiff from "twice justice court costs and estimated county court costs less justice court costs paid" to "$500"; 3) imports the provision that cash bonds are acceptable in lieu of sureties; 4) makes explicit that the county court is responsible for giving the appellant the 5 days to correct any defects, it is currently unclear which court is responsible.

RULE 561 – INABILITY TO PAY APPEAL COSTS

Organized and clarified the information on pauper's affidavits. Extends the time for a hearing on the matter from 5 to 10 days.

RULE 563 – TRANSCRIPT

RULE 564 – NEW MATTER TO BE PLEADED

RULE 565 – TRIAL DE NOVO

No substantive changes.

RULE 570 – PLENARY POWER

Currently is a debate whether our courts have 10 or 30 days of plenary power, this rule clarifies it to 20 days or appeal, whichever comes first.

RULE 571 – FORMS

Gives some guidance on legal advice, clarifying blank forms are allowable, but parties can't be forced to use court-generated forms.

RULE 572 – DOCKET

RULE 573 – ISSUANCE OF WRITS

RULE 574 – WHO MAY SERVE AND METHOD OF SERVICE

RULE 575 – DUTY OF OFFICER OR PERSON RECEIVING AND RETURN OF CITATION

No substantive changes.

DEBT CLAIM CASE RULES

HB 79 directed us to adopt special rules for cases brought by plaintiffs who are assignees, who are primarily engaged in lending money at interest, and who are collection agents. The end result was this set of rules which applies to what we defined as Debt Claim Cases, the vast majority of which are suits to recover credit card debt by an assignee of this debt. Our goal was to reward plaintiffs who have all the necessary proof with an expedient, predictable, inexpensive process, while also protecting defendants from many of the inherent problems in these suits, including an often disturbing lack of proof.

RULE 576 – SCOPE

We tried to define these cases in a way consistent with HB 79 while also ensuring it applied to the cases that in practice need the additional guidelines. Was proposed to remove 'alleged' from (a) (1)-(a) (3). Change "chapter" in (b) to "section". Also change "and" to "or" in (b).

RULE 577 – PLAINTIFFS PLEADINGS

These requirements were selected to help reduce mistaken identity cases, and ensure the defendant understands the subject of the lawsuit. Often they will receive a lawsuit by a company like Unifund saying they owe $6700 and think it's a scam because they have never heard of Unifund. Change "chapter" to "section". Proposal to include either "In addition to the requirements of Rule 509..." or explicitly list all 509 requirements.

RULE 578 – DEFAULT JUDGMENTS

Most appellate courts currently hold that credit card debt is unliquidated. That means that in our courts, there must be a hearing. Plaintiffs in these cases are very interested in getting default judgments without the necessity, time and expense of a hearing. In conjunction with the default j/m rule earlier, this rule provides a framework that allows plaintiffs who have good supporting documents, and not just a computer screen printout of a name and $ amount, to get a default judgment without hearing. If the plaintiff doesn't have those documents, a hearing will be required for default judgment.

Additionally, the Task Force voted unanimously to follow the Martinez standard in lieu of the Simien standard and require an affidavit proving up business records to be from the company that generated the records.

Proposed to fold (b) and (c) into (a) and add sub-parts, since they all relate to 'no-hearing' defaults. Proposed to replace the requirement that the affidavit is from the original creditor with "If the affidavit lacks trustworthiness, the trial judge may deny the request for the default judgment." Proposed to add "as to liability and damages" in (e) after "may proceed to hear evidence". Proposed to replace "affidavit" with "sworn statement".

REPAIR AND REMEDY CASE RULES

We left these rules almost completely alone, as they are very new. We thought the comment at the end might be removed, and modified 737.2 and 737.3 to be on the same timeframe as eviction cases, as they are currently.

EVICTION RULES

There has been some controversy over whether we were supposed to write rules for eviction cases, although HB 79 is very explicit on its face that we were. As mentioned, we are not trying to blow up and rebuild the eviction process from the ground up. Instead, our goals were to patch some holes in the current process and ensure fairness to both sides, while also maintaining the same goal for these cases as in other civil cases in the new justice court – fair,

speedy justice that does not require a lawyer and allows the judge to make rulings that are fair and equitable.

RULE 738 – COMPUTATION OF TIME FOR EVICTION CASES

We wanted to clarify that all days were calendar days, and also address a major problem with the mailbox rule in eviction cases. As it is currently, if a tenant mails the appeal on the day it is due, the landlord can get a writ of possession the next day, then the court receives the appeal several days later and it was technically timely filed. What now? We eliminated that problem by requiring a mail filing in an eviction case to be received by the due date. However, that created a problem for litigants who are far from the court, so we added the ability to file with the court by fax. They must also follow that up with a mailing of the original. The application of this will mainly be for appeals, and we thought it was important to give parties an option. A judge mentioned concerns about fax volume and paper costs, but the numbers of appeals annually don't bear that out.

Proposed to clarify that the first day does not count but the last day does count.

RULE 739 – PETITION

This rule addresses several problems with the current framework: 1) It makes explicit in the rules that it must be filed where the property is located and that the plaintiff won't receive a refund if they file improperly; 2) it makes clear that a writ of possession can't issue against a tenant who isn't named in the petition. Currently some landlords will try to evict John and Jane Doe by filing suit against John Doe "and all occupants". Jane is not an occupant, she is a tenant. So no writ may issue against Jane. Of course, she may leave when a writ is executed against John.

TAA requested a change to (d) from "rent sought" to "rent currently due" and we are on board with that change. They were concerned that, for example, if the petition was filed on Sept 29, and the next month became due on Oct 1, that could create a problem. We put that clause in there because some landlords don't put an amount, then at a default j/m hearing claim large amounts. This way, the defendant is on notice of what is being claimed. Of course, if rent becomes due during the pendency of the court, it is appropriate for the court to award it, and the defendant would have knowledge of the monthly rent.

Proposed to clarify last sentence, putting period after rules, then strike "except that" and add "of possession" after writ. Proposal to include either "In addition to the requirements of Rule 509..." or explicitly list all 509 requirements.

RULE 740 – MAY SUE FOR RENT

No substantive changes.

RULE 741 – CITATION

Another big problem with the current eviction system: the judge is required to list the hearing date in the citation BUT the hearing date window is dependent on the date that the defendant is served, which is of course unknown at the time the citation is generated. So we decided to base the hearing date window on the date of filing. Since it is currently 6-10 days from service, we thought 7-14 days from filing would be roughly equivalent. It is not our intention to modify the actual timeframe these cases occur in, instead to allow a judge to set the trial date in the citation. Some discussion from judges/constables indicates that 10-21 days may be a more realistic window to allow for service, and sometimes alternative service, and the counsel for TAA indicated that cases were generally being heard 3-4 weeks from filing, so that shouldn't prejudice landlords to give a window of 10-21 days instead of the 7-14 in the draft of rules. If this is modified to 10-21 days, so should rule 737 to be consistent.

Another benefit to working from filing instead of service is that some constables will refuse to serve an eviction citation during certain times, for example, around the Christmas holiday season. Under the current system, the landlord has no redress, because the trial window doesn't start until service occurs. Under the new rule, the clock is ticking upon the filing of the petition.

RULE 742 – REQUEST FOR IMMEDIATE POSSESSION

Current Rule 740 is very troublesome. It states that the sheriff or constable shall immediately place the plaintiff in possession of the premises if the defendant doesn't demand a trial or post a counterbond in 6 days from filing of a bond for immediate possession. However, it doesn't provide a mechanism for doing so. Many judges feel the only mechanism would be a writ of possession, which would then make this rule conflict with the Property Code which only allows writs after a trial (6 days after unless an IPB is filed and j/m is by default).

The main benefit of the rule is to allow immediate possession after defaults, the rest is difficult to understand and/or implement. Our proposed replacement keeps that benefit, while also allowing the plaintiff to get a writ 24 hours after judgment if they can show good cause. This is intended for cases where, for example, the tenant is threatening other tenants or the landlord, selling drugs on-premises, damaging the property, etc. It also explicitly lays out the procedure so all parties and judges can understand it.

Several members of our Task Force wanted to just eliminate immediate possession bonds while others felt it was a very important remedy that needed some updating and clarification. Another option would be to simply make it where a writ of possession issues immediately on default j/m if an IPB is filed, and no other impact on the case.
Whatever the SCAC does, we ask that you please not just leave current Rule 740 as-is. It is vague and being implemented in ways that may be overly damaging to tenants' rights in some areas.

RULE 743 – SERVICE OF CITATION

No substantive changes, but note this works with the previous rule to set up a window for service, since the trial date was set when the citation was issued. This rule requires service at least six days before that date. So if the trial date is modified to 10-21 days from filing, the constable will have at least 4 and up to 15 days to serve the citation, depending on when the judge set the trial. Also requires the return to be at least 3 days before the trial date, whereas the current rule allows return the day of trial.

RULE 743A – SERVICE BY DELIVERY TO PREMISES

No substantive changes, other than requiring the return no later than the day before trial instead of the day of trial.

RULE 744 – DOCKETED

Makes explicit that no trial may be held less than six days after service. Proposal has been made to add that no counterclaims may be docketed, which is currently only in caselaw, and not in rules or statute. That would probably be helpful.

RULE 745 – DEMANDING JURY

Another difficulty with the current procedure is that the defendant has 5 days after service to request a jury. However, that is 5 days NOT COUNTING weekends/holidays. With the trial being 6-10 calendar days after service, it is often the case that the defendant can lawfully request a jury the day of the trial, which most courts can't accommodate, resulting in continuances or other problems. We modified to say they must request it at least 3 days before the trial date to allow the court to prepare.

RULE 746 – TRIAL POSTPONED

We extended the allowable continuance from 6 to 7 days, to accommodate many courts who hold evictions exclusively on one day of the week, this allows them to manage their docket in that manner legally. Additionally we eliminated the affidavit requirement, only requiring the party to show good cause.

RULE 747 – ONLY ISSUE

RULE 748 – TRIAL

RULE 748A – REPRESENTATION BY AGENTS

No substantive changes.

RULE 749 – JUDGMENT AND WRIT

Added a requirement that the plaintiff must request a writ of possession within 30 days of judgment and the constable has 30 days to execute it. Currently, many landlords negotiate with tenants and allow them to stay. Then months later, they become disenchanted and want their writ. A new contract has been formed, and it is not proper for it to terminate with the old writ. However, our court has no jurisdiction to do anything under current rules but issue the writ. The tenant would need to get an injunctive order and has no idea how to do that or that their rights are being infringed. This rule would drastically reduce/eliminate this practice.

A proposal has been made to add "without good cause shown" to these timeframes. A concern would be plenary power issues, but we would generally have no objection to this addition.

RULE 750 – MAY APPEAL

RULE 750A – INABILITY TO PAY APPEAL COSTS IN EVICTION CASES

No substantive changes.

RULE 750B – PAYMENT OF RENT DURING NONPAYMENT OF RENT APPEALS

Added the information from the latest legislative session regarding paying rent into the justice court registry when an appeal of a nonpayment of rent eviction is made via paupers affidavit. There is some objection to including this information here, since it is in the Property Code. Our thought was we wanted lay tenants to be able to read this set of rules and know their rights and responsibilities.

RULE 750C – PAUPER'S AFFIDAVIT IN CASES WITH IMMEDIATE POSSESSION BONDS

Ties into Rule 742 requiring a bond to be posted if the defendant wants to stay in possession when a court has ruled that immediate possession is appropriate. If 742 is removed/modified, this must be too.

RULE 750D – APPEAL PERFECTED

Currently also 750c in the draft. Needs renumbering. Nothing substantive.

RULE 751 – FORM OF APPEAL BOND

RULE 752 – TRANSCRIPT

RULE 753 – DAMAGES ON APPEAL

RULE 754 – JUDGMENT BY DEFAULT ON APPEAL

No substantive changes.

RULE 755 – WRIT OF POSSESSION ON APPEAL

Clarified process with information from Property Code.

Andrew E. Lemanski & Associates

Attorney at Law

September 29, 2012

Supreme Court Advisory Committee
c/o Charles L. "Chip" Babcock
Jackson Walker L.L.P.
1401 McKinney, Suite 1900
Houston, Texas 77010

Re: Small Claims Court Rules

Dear Mr. Chairman and Members of the Committee:

Thank you for the opportunity to provide comments on the proposed small claims court rules.

Small damage personal injury claims filed in small claims court should not be the subject of extensive discovery. Expenses can easily create a barrier to accessing courts in these types of cases. Also, they allow young attorneys the opportunity to sharpen their trial skills in a relatively informal and low risk setting. Rule 504 should include language stating that a court has to weigh the actual cost to the parties before applying the Rules of Evidence.

Similarly, Rule 507 should include language stating that a court has to weigh the actual cost to the parties before requiring formal discovery. A rule requiring the requesting party to pay for all discovery (depositions, expert fees, subpoenas, etc.) could also help alleviate this burden.

Rule 526, Summary Disposition, should require that some form of sworn statement be filed in response to a motion. A party should be allowed some notice of what the other side is going to argue at a hearing. Furthermore, because they are not courts of record, litigants are sometimes willing to say far more in JP court than they will swear to under oath. Any concerns about confusion can be handled by allowing for an automatic reset of the motion if a party does not file a sworn response.

Rule 564 should be changed to "New Matter Cannot Be Pleaded on Appeal" or similar language to more closely follow the rule and prevent confusion.

6200 Savoy, Suite 440 ◆ Houston, TX 77036 ◆ Phone: 713/515-2826 ◆ Fax: 713/952-8375

Rule 565 should make it clear the same procedures and relaxed standards should be used in county court in a trial de novo. Otherwise, the purpose of small claims court is obviated and the requirement of a fast, inexpensive trial is not met.

I have attached three sets of documents. Exhibit "A" is an excerpt from the Federal Register regarding the Fair and Accurate Credit Transactions Act of 2003. The "Red Flag Rules" it discusses protect against identity theft and ensure that financial institutions have accurate data. This document is provided to show the Committee just some of the safeguards and protections that banks have in place to protect against someone wrongly being saddled with a debt.

Exhibits "B" and "C" are responses and counterclaims in two debt cases. I have redacted the information that would allow one to identify the plaintiff, defendant, or the defendant's attorney. The case in Exhibit "B" involved a debt of just under $2,500. The case in Exhibit "C" involved a debt of just under $3,500. Because of the vigorous defense, and the counterclaims, both cases settled on terms very favorable to the debtors. The settlements had nothing to do with the merits of either case. Exhibits "B" and "C" are provided to show the Committee how debtors can easily and unfairly turn the tables on creditors by making the cost of recovery so high that creditors are put in the position of either dropping the case or losing a significant amount of money. Cases should be determined on the merits, and not on the basis of legal maneuvering. If a creditor's access to small claims courts is going to be severely limited by the rules, then a debtor's access to filing counterclaims should be similarly limited. The rules should require very specific pleadings and attaching evidence of counterclaims.

Simien v. Unifund CCR Ptnrs, 321 S.W.3d 235 (Tex.App.—Houston[1st Dist.] 2010, no pet.) was not about debt collection cases. It was about how modern society works. Every day, businesses reasonably rely on other businesses' records. This basic fact was recognized by the *Simien* court and then applied in the context of debt collection cases. Bank records are reliable and should be admissible under the Rules of Evidence. Their credibility can be argued all day long to a fact finder. This distinction is being lost under the small claims rules for debt cases, as admissibility and credibility seem to merge into one for the purposes of a default judgment.

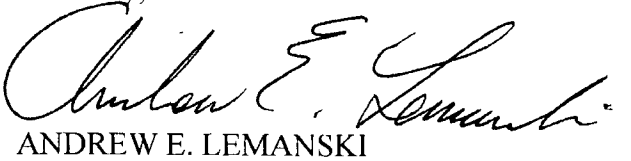
Even the most skilled, brightest and articulate lawyer, on their best day, cannot compete with a judge who had made up their mind. The rules fundamentally alter our court system that has been in place for well over 150 years by turning the judge into an advocate and requiring the judge to determine if evidence is deemed worthy of credit. While this is normal in the context of a bench trial, it should have no place in the context of a default judgment.

Almost without exception, defaults occur because debtors know they owe the debt. There is no point in paying a lawyer to defend against a debt that is owed *unless* the court system is little more than a game.

If the fundamental purpose of a court strays from deciding cases on the merits, and instead focuses on jumping through legally mandated hoops, then our court system becomes little more than a game. The small claims court rules on debt cases are not just about what goes on in small claims courts. They represent a fundamental shift in the role of a judge. No longer is a judge a neutral; someone who enforces the rules and considers arguments from both sides. Now, the judge sits as a policy maker, who decides what is and is not good for private parties, even in the absence of a dispute. That decision should be left in the hands of private parties.

If you have any questions, or require any additional information, please feel free to contact me at (713) 515-2826.

Sincerely,



ANDREW E. LEMANSKI

EXHIBIT A

Federal Register

Friday,
November 9, 2007

Part IV

Department of the Treasury
Office of the Comptroller of the Currency
12 CFR Part 41

Federal Reserve System
12 CFR Part 222

Federal Deposit Insurance Corporation
12 CFR Parts 334 and 364

Department of the Treasury
Office of Thrift Supervision
12 CFR Part 571

National Credit Union Administration
12 CFR Part 717

Federal Trade Commission
16 CFR Part 681

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule

EXHIBIT "A"

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 41

[Docket ID OCC–2007–0017]

RIN 1557–AC87

FEDERAL RESERVE SYSTEM

12 CFR Part 222

[Docket No. R–1255]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Parts 334 and 364

RIN 3064–AD00

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 571

[Docket No. OTS–2007–0019]

RIN 1550–AC04

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 717

FEDERAL TRADE COMMISSION

16 CFR Part 681

RIN 3084–AA94

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003

AGENCIES: Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS); National Credit Union Administration (NCUA); and Federal Trade Commission (FTC or Commission).

ACTION: Joint final rules and guidelines.

SUMMARY: The OCC, Board, FDIC, OTS, NCUA and FTC (the Agencies) are jointly issuing final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act. The rules implementing section 114 require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. In addition, the Agencies are issuing guidelines to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the rules. The rules implementing section 114 also require credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances. Additionally, the Agencies are issuing joint rules under section 315 that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

DATES: The joint final rules and guidelines are effective January 1, 2008. The mandatory compliance date for this rule is November 1, 2008.

FOR FURTHER INFORMATION CONTACT:

OCC: Amy Friend, Assistant Chief Counsel, (202) 874–5200; Deborah Katz, Senior Counsel, or Andra Shuster, Special Counsel, Legislative and Regulatory Activities Division, (202) 874–5090; Paul Utterback, Compliance Specialist, Compliance Department, (202) 874–5461; or Aida Plaza Carter, Director, Bank Information Technology, (202) 874–4740, Office of the Comptroller of the Currency, 250 E Street, SW., Washington, DC 20219.

Board: David A. Stein or Ky Tran-Trong, Counsels, or Amy Burke, Attorney, Division of Consumer and Community Affairs, (202) 452–3667; Kara L. Handzlik, Attorney, Legal Division, (202) 452–3852; or John Gibbons, Supervisory Financial Analyst, Division of Banking Supervision and Regulation, (202) 452–6409, Board of Governors of the Federal Reserve System, 20th and C Streets, NW., Washington, DC 20551.

FDIC: Jeffrey M. Kopchik, Senior Policy Analyst, (202) 898–3872, or David P. Lafleur, Policy Analyst, (202) 898–6569, Division of Supervision and Consumer Protection; Richard M. Schwartz, Counsel, (202) 898–7424, or Richard B. Foley, Counsel, (202) 898–3784, Legal Division, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429.

OTS: Ekita Mitchell, Consumer Regulations Analyst, Compliance and Consumer Protection, (202) 906–6451; Kathleen M. McNulty, Technology Program Manager, Information Technology Risk Management, (202) 906–6322; or Richard Bennett, Senior Compliance Counsel, Regulations and Legislation Division, (202) 906–7409, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552.

NCUA: Regina M. Metz, Staff Attorney, Office of General Counsel, (703) 518–6540, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314–3428.

FTC: Naomi B. Lefkovitz, Attorney, or Pavneet Singh, Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, (202) 326–2252, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington DC 20580.

SUPPLEMENTARY INFORMATION:

I. Introduction

The President signed the FACT Act into law on December 4, 2003.[1] The FACT Act added several new provisions to the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. 1681 *et seq.* Section 114 of the FACT Act, 15 U.S.C. 1681m(e), amends section 615 of the FCRA, and directs the Agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances.[2] Section 315 of the FACT Act, 15 U.S.C. 1681c(h), adds a new section 605(h)(2) to the FCRA requiring the Agencies to issue joint regulations that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy.

On July 18, 2006, the Agencies published a joint notice of proposed rulemaking (NPRM) in the **Federal Register** (71 FR 40786) proposing rules and guidelines to implement section 114 and proposing rules to implement section 315 of the FACT Act. The public comment period closed on September 18, 2006. The Agencies collectively received a total of 129 comments in response to the NPRM, although many commenters sent copies of the same letter to each of the Agencies. The comments included 63 from financial institutions, 12 from financial institution holding companies, 23 from financial institution trade associations, 12 from individuals, nine from other trade associations, five from other business entities, three from consumer

[1] Pub. L. 108–159.

[2] Section 111 of the FACT Act defines "identity theft" as "a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade] Commission may prescribe, by regulation." 15 U.S.C. 1681a(q)(3).

groups,[3] one from a member of Congress, and one from the United States Small Business Administration (SBA).

II. Section 114 of the FACT Act

A. Red Flag Regulations and Guidelines

1. Background

Section 114 of the FACT Act requires the Agencies to jointly issue guidelines for financial institutions and creditors regarding identity theft with respect to their account holders and customers. Section 114 also directs the Agencies to prescribe joint regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines, to identify possible risks to account holders or customers or to the safety and soundness of the institution or "customer."[4]

In developing the guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The guidelines must be updated as often as necessary, and cannot be inconsistent with the policies and procedures issued under section 326 of the USA PATRIOT Act,[5] 31 U.S.C. 5318(l), that require verification of the identity of persons opening new accounts. The Agencies also must consider including reasonable guidelines that would apply when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years. These guidelines would provide that in such circumstances, a financial institution or creditor "shall follow reasonable policies and procedures" for notifying the consumer, "in a manner reasonably designed to reduce the likelihood of identity theft."

2. Overview of Proposal and Comments Received

The Agencies proposed to implement section 114 through regulations requiring each financial institution and creditor to implement a written Program to detect, prevent and mitigate identity theft in connection with the opening of an account or any existing account. The Agencies also proposed guidelines that identified 31 patterns, practices, and specific forms of activity that indicate a possible risk of identity theft. The proposed regulations required each financial institution and creditor to incorporate into its Program relevant indicators of a possible risk of identity theft (Red Flags), including indicators from among those listed in the guidelines. To promote flexibility and responsiveness to the changing nature of identity theft, the proposed rules also stated that covered entities would need to include in their Programs relevant Red Flags from applicable supervisory guidance, their own experiences, and methods that the entity had identified that reflect changes in identity theft risks.

The Agencies invited comment on all aspects of the proposed regulations and guidelines implementing section 114, and specifically requested comment on whether the elements described in section 114 had been properly allocated between the proposed regulations and the proposed guidelines.

Consumer groups maintained that the proposed regulations provided too much discretion to financial institutions and creditors to decide which accounts and Red Flags to include in their Programs and how to respond to those Red Flags. These commenters stated that the flexible and risk-based approach taken in the proposed rulemaking would permit "business as usual."

Some small financial institutions also expressed concern about the flexibility afforded by the proposal. These commenters stated that they preferred to have clearer, more structured guidance describing exactly how to develop and implement a Program and what they would need to do to achieve compliance.

Most commenters, however, including many financial institutions and creditors, asserted that the proposal was overly prescriptive, contained requirements beyond those mandated in the FACT Act, would be costly and burdensome to implement, and would complicate the existing efforts of financial institutions and creditors to detect and prevent identity theft. Some industry commenters asserted that the rulemaking was unnecessary because large businesses, such as banks and telecommunications companies, already are motivated to prevent identity theft and other forms of fraud in order to limit their own financial losses. Financial institution commenters maintained that they are already doing most of what would be required by the proposal as a result of having to comply with the customer identification program (CIP) regulations implementing section 326 of the USA PATRIOT Act[6] and other existing requirements. These commenters suggested that the regulations and guidelines take the form of broad objectives modeled on the objectives set forth in the "Interagency Guidelines Establishing Information Security Standards" (Information Security Standards).[7] A few financial institution commenters asserted that the primary cause of identity theft is the lack of care on the part of the consumer. They stated that consumers should be held responsible for protecting their own identifying information.

The Agencies have modified the proposed rules and guidelines in light of the comments received. An overview of the final rules, guidelines, and supplement, a discussion of the comments, and the specific manner in which the proposed rules and guidelines have been modified, follows.

3. Overview of final rules and guidelines

The Agencies are issuing final rules and guidelines that provide both flexibility and more guidance to financial institutions and creditors. The final rules also require the Program to address accounts where identity theft is most likely to occur. The final rules describe which financial institutions and creditors are required to have a Program, the objectives of the Program, the elements that the Program must contain, and how the Program must be administered.

Under the final rules, only those financial institutions and creditors that offer or maintain "covered accounts" must develop and implement a written Program. A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."

The final regulations provide that the Program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. In addition, the Program must be tailored to the entity's size, complexity and nature of its operations.

---

[3] One of these letters represented the comments of five consumer groups.

[4] Use of the term "customer," here, appears to be a drafting error and likely should read "creditor."

[5] Pub. L. 107–56.

[6] *See, e.g.*, 31 CFR 103.121 (applicable to banks, thrifts and credit unions and certain non-federally regulated banks).

[7] 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D–2 and part 225, app. F (state member banks and holding companies); 12 CFR part 364, app. B (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, App. A (credit unions).

The final regulations list the four basic elements that must be included in the Program of a financial institution or creditor. The Program must contain "reasonable policies and procedures" to:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The regulations also enumerate certain steps that financial institutions and creditors must take to administer the Program. These steps include obtaining approval of the initial written Program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the Program, training staff, and overseeing service provider arrangements.

In order to provide financial institutions and creditors with more flexibility in developing a Program, the Agencies have moved certain detail formerly contained in the proposed regulations to the guidelines located in Appendix J. This detailed guidance should assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the regulations to detect, prevent, and mitigate identity theft. Each financial institution or creditor that is required to implement a Program must consider the guidelines and include in its Program those guidelines that are appropriate. The guidelines provide policies and procedures for use by institutions and creditors, where appropriate, to satisfy the requirements of the final rules, including the four elements listed above. While an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program, the Program must nonetheless contain reasonable policies and procedures to meet the specific requirements of the final rules. The illustrative examples of Red Flags formerly in Appendix J are now listed in a supplement to the guidelines.

4. Section-by-Section Analysis [8]

Section__.90(a) Purpose and Scope

Proposed §__.90(a) described the statutory authority for the proposed regulations, namely, section 114 of the FACT Act. It also defined the scope of this section; each of the Agencies proposed tailoring this paragraph to describe those entities to which this section would apply. The Agencies received no comments on this section, and it is adopted as proposed.

Section__.90(b) Definitions

Proposed §__.90(b) contained definitions of various terms that applied to the proposed rules and guidelines. While §__.90(b) of the final rules continues to describe the definitions applicable to the final rules and guidelines, changes have been made to address the comments, as follows.

Section__.90(b)(1) Account. The Agencies proposed using the term "account" to describe the relationships covered by section 114 that an account holder or customer may have with a financial institution or creditor.[9] The proposed definition of "account" was "a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k)." The definition also gave examples of types of "accounts."

Some commenters stated that the regulations do not need a definition of "account" to give effect to their terms. Some commenters maintained that a new definition for "account" would be confusing as this term is already defined inconsistently in several regulations and in section 615(e) of the FCRA. These commenters recommended that the Agencies use the term "continuing relationship" instead, and define this phrase in a manner consistent with the Agencies' privacy rules [10] implementing Title V of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801.[11] These commenters urged that the definition of "account" not be expanded to include relationships that are not "continuing." They stated that it would be very burdensome to gather and maintain information on non-customers for one-time transactions. Other commenters suggested defining the term "account" in a manner consistent with the CIP rules.

Many commenters stated that defining "account" to cover both consumer and business accounts was too broad, exceeded the scope of the FACT Act, and would make the regulation too burdensome. These commenters recommended limiting the scope of the regulations and guidelines to cover only consumer financial services, specifically accounts established for personal, family and household purposes, because these types of accounts typically are targets of identity theft. They asserted that identity theft has not historically been common in connection with business or commercial accounts.

Consumer groups maintained that the proposed definition of "account" was too narrow. They explained that because the proposed definition was tied to financial products and services that can be offered under the Bank Holding Company Act, it inappropriately excluded certain transactions involving creditors that are not financial institutions that should be covered by the regulations. Some of these commenters recommended that the definition of "account" include any relationship with a financial institution or creditor in which funds could be intercepted or credit could be extended, as well as any other transaction which could obligate an individual or other covered entity, including transactions that do not result in a continuing relationship. Others suggested that there should be no flexibility to exclude any account that is held by an individual or which generates information about individuals that reflects on their financial or credit reputations.

The Agencies have modified the definition of "account" to address these comments. First, the final rules now apply to "covered accounts," a term that the Agencies have added to the definition section to eliminate

[8] The OCC, Board, FDIC, OTS and NCUA are placing the regulations and guidelines implementing section 114 in the part of their regulations that implement the FCRA—12 CFR parts 41, 222, 334, 571, and 717, respectively. In addition, the FDIC cross-references the regulations and guidelines in 12 CFR part 364. For ease of reference, the discussion in this preamble uses the shared numerical suffix of each of these agency's regulations. The FTC also is placing the final regulations and guidelines in the part of its regulations implementing the FCRA, specifically 16 CFR part 681. However, the FTC uses different numerical suffixes that equate to the numerical suffixes discussed in the preamble as follows: preamble suffix .82 = FTC suffix .1, preamble suffix .90 = FTC suffix .2, and preamble suffix .91 = FTC suffix .3. In addition, Appendix J referenced in the preamble is the FTC's Appendix A.

[9] The Agencies acknowledged that section 114 does not use the term "account" and, in other contexts, the FCRA defines the term "account" narrowly to describe certain consumer deposit or asset accounts. See 15 U.S.C. 1681a(r)(4).

[10] See 12 CFR 40 (OCC); 12 CFR 216 (Board); 12 CFR 332 (FDIC); 12 CFR 573 (OTS); 12 CFR 716 (NCUA); and 16 CFR 313 (FTC).

[11] Pub. L. 106–102.

confusion between these rules and other rules that apply to an "account." The Agencies have retained a definition of "account" simply to clarify and provide context for the definition of "covered account."

Section 114 provides broad discretion to the Agencies to prescribe regulations and guidelines to address identity theft. The terminology in section 114 is not confined to "consumer" accounts. While identity theft primarily has been directed at consumers, the Agencies are aware that small businesses also have been targets of identity theft. Over time, identity theft could expand to affect other types of accounts. Thus, the definition of "account" in §__.90(b)(1) of the final rules continues to cover *any* relationship to obtain a product or service that an account holder or customer may have with a financial institution or creditor.[12] Through examples, the definition makes clear that the purchase of property or services involving a deferred payment is considered to be an account.

Although the definition of "account" includes business accounts, the risk-based nature of the final rules allows each financial institution or creditor flexibility to determine which business accounts will be covered by its Program through a risk evaluation process.

The Agencies also recognize that a person may establish a relationship with a creditor, such as an automobile dealer or a telecommunications provider, primarily to obtain a product or service that is not financial in nature. To make clear that an "account" includes relationships with creditors that are not financial institutions, the definition is no longer tied to the provision of "financial" products and services. Accordingly, the Agencies have deleted the reference to the Bank Holding Company Act.

The definition of "account" still includes the words "continuing relationship." The Agencies have determined that, at this time, the burden that would be imposed upon financial institutions and creditors by a requirement to detect, prevent and mitigate identity theft in connection with single, non-continuing transactions by non-customers would outweigh the benefits of such a requirement. The Agencies recognize, however, that identity theft may occur at the time of account opening. Therefore, as detailed below, the obligations of the final rule apply not only to existing accounts, where a relationship already has been established, but also to account openings, when a relationship has not yet been established.

Section__.90(b)(2) Board of Directors. The proposed regulations discussed the role of the board of directors of a financial institution or creditor. For financial institutions and creditors covered by the regulations that do not have boards of directors, the proposed regulations defined "board of directors" to include, in the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency. For other creditors that do not have boards of directors, the proposed regulations defined "board of directors" as a designated employee.

Consumer groups objected to the proposed definition as it applied to creditors that do not have boards of directors. These commenters recommended that for these entities, "board of directors" should be defined as a designated employee at the level of senior management. They asserted that otherwise, institutions that do not have a board of directors would be given an unfair advantage for purposes of the substantive provisions of the rules, because they would be permitted to assign *any* employee to fulfill the role of the "board of directors."

The Agencies agree this important role should be performed by an employee at the level of senior management, rather than any designated employee. Accordingly, the definition of "board of directors" has been revised in §__.90(b)(2) of the final rules so that, in the case of a creditor that does not have a board of directors, the term "board of directors" means "a designated employee at the level of senior management."

Section __.90(b)(3) Covered Account. As mentioned previously, the Agencies have added a new definition of "covered account" in §__.90(b)(3) to describe the type of "account" covered by the final rules. The proposed rules would have provided a financial institution or creditor with broad flexibility to apply its Program to those accounts that it determined were vulnerable to the risk of identity theft, and did not mandate coverage of any particular type of account.

Consumer group commenters urged the Agencies to limit the discretion afforded to financial institutions and creditors by requiring them to cover consumer accounts in their Programs. While seeking to preserve their discretion, many industry commenters requested that the Agencies limit the final rules to consumer accounts, where identity theft is most likely to occur.

The Agencies recognize that consumer accounts are presently the most common target of identity theft and acknowledge that Congress expected the final regulation to address risks of identity theft to consumers.[13] For this reason, the final rules require each Program to cover accounts established primarily for personal, family or household purposes, that involve or are designed to permit multiple payments or transactions, *i.e.*, consumer accounts. As discussed above in connection with the definition of "account," the final rules also require the Programs of financial institutions and creditors to cover any other type of account that the institution or creditor offers or maintains for which there is a reasonably foreseeable risk from identity theft.

Accordingly, the definition of "covered account" is divided into two parts. The first part refers to "an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions." The definition provides examples to illustrate that these types of consumer accounts include, "a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account."[14]

The second part of the definition refers to "any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." This part of the definition reflects the Agencies' belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft, and, therefore, should be considered for coverage by the Program of a financial institution or creditor.

In response to the proposed definition of "account," a trade association representing credit unions suggested that the term "customer" in the definition be revised to refer to

[12] Accordingly, the definition of "account" still applies to fiduciary, agency, custodial, brokerage and investment advisory activities.

[13] *See* S. Rep. No. 108-166 at 13 (Oct. 17, 2003) (accompanying S. 1753).

[14] These examples reflect the fact that the rules are applicable to a variety of financial institutions and creditors. They are not intended to confer any additional powers on covered entities. Nonetheless, some of the Agencies have chosen to limit the examples in their rule texts to those products covered entities subject to their jurisdiction are legally permitted to offer.

"member" to better reflect the ownership structure of some financial institutions or to "consumer" to include all individuals doing business at all types of financial institutions. The definition of "account" in the final rules no longer makes reference to the term "customer"; however, the definition of "covered account" continues to employ this term, to be consistent with section 114 of the FACT Act, which uses the term "customer." Of course, in the case of credit unions, the final rules and guidelines will apply to the accounts of members that are maintained primarily for personal, family, or household purposes, and those that are otherwise subject to a reasonably foreseeable risk of identity theft.

Sections __.90(b)(4) and (b)(5) Credit and Creditor. The proposed rules defined these terms by cross-reference to the relevant sections of the FCRA. There were no comments on the definition of "credit" and § __.90(b)(4) of the final rules adopts the definition as proposed.

Some commenters asked the Agencies to clarify that the term "creditor" does not cover third-party debt collectors who regularly arrange for the extension, renewal, or continuation of credit.

Section 114 applies to financial institutions and creditors. Under the FCRA, the term "creditor" has the same meaning as in section 702 of the Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691a.[15] ECOA defines "creditor" to include a person who arranges for the extension, renewal, or continuation of credit, which in some cases could include third-party debt collectors. 15 U.S.C. 1691a(e). Therefore, the Agencies are not excluding third-party debt collectors from the scope of the final rules, and § __.90(b)(5) of the final rules adopts the definition of "creditor" as proposed.

Section __.90(b)(6) Customer. Section 114 of the FACT Act refers to "account holders" and "customers" of financial institutions and creditors without defining either of these terms. For ease of reference, the Agencies proposed to use the term "customer" to encompass both "customers" and "account holders." "Customer" was defined as a person that has an account with a financial institution or creditor. The proposed definition of "customer" applied to any "person," defined by the FCRA as any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.[16] The proposal explained that the Agencies chose this broad definition because, in addition to individuals, various types of entities (*e.g.*, small businesses) can be victims of identity theft. Under the proposed definition, however, a financial institution or creditor would have had the discretion to determine which type of customer accounts would be covered under its Program, since the proposed regulations were risk-based.[17]

As noted above, most industry commenters maintained that including all persons, not just consumers, within the definition of "customer" would impose a substantial financial burden on financial institutions and creditors, and make compliance with the regulations more burdensome. These commenters stated that business identity theft is rare, and maintained that financial institutions and creditors should be allowed to direct their fraud prevention resources to the areas of highest risk. They also noted that businesses are more sophisticated than consumers, and are in a better position to protect themselves against fraud than consumers, both in terms of prevention and in enforcing their legal rights.

Some financial institution commenters were concerned that the broad definition of "customer" would create opportunities for commercial customers to shift responsibility from themselves to the financial institution for not discovering Red Flags and alerting business customers about embezzlement or other fraudulent transactions by the commercial customer's own employees. These commenters suggested narrowing the definition to cover natural persons and to exclude business customers. Some of these commenters suggested that the definition of "customer" should be consistent with the definition of this term in the Information Security Standards and the Agencies' privacy rules.

Consumer groups commented that the proposed definition of "customer" was too narrow. They recommended that the definition be amended, so that the regulations would not only protect persons who are already customers of a financial institution or creditor, but also persons whose identities are used by an imposter to open an account.

Section __.90(b)(6) of the final rule defines "customer" to mean a person that has a "covered account" with a financial institution or creditor. Under the definition of "covered account," an individual who has a consumer account will always be a "customer." A "customer" may also be a person that has another type of account for which a financial institution or creditor determines there is a reasonably foreseeable risk to its customers or to its own safety and soundness from identity theft.

The Agencies note that the Information Security Standards and the privacy rules implemented various sections of Title V of the GLBA, 15 U.S.C. 6801, which specifically apply only to customers who are consumers. By contrast, section 114 does not define the term "customer." Because the Agencies continue to believe that a business customer can be a target of identity theft, the final rules contain a risk-based process designed to ensure that these types of customers will be covered by the Program of a financial institution or creditor, when the risk of identity theft is reasonably foreseeable.

The definition of "customer" in the final rules continues to cover only customers that already have accounts. The Agencies note, however, that the substantive provisions of the final rules, described later, require the Program of a financial institution or creditor to detect, prevent, and mitigate identity theft in connection with the opening of a covered account as well as any existing covered account. The final rules address persons whose identities are used by an imposter to open an account in these substantive provisions, rather than through the definition of "customer."

Section __.90(b)(7) Financial Institution. The Agencies received no comments on the proposed definition of "financial institution." It is adopted in § __.90(b)(7), as proposed, with a cross-reference to the relevant definition in the FCRA.

Section __.90(b)(8) Identity Theft. The proposal defined "identity theft" by cross-referencing the FTC's rule that defines "identity theft" for purposes of the FCRA.[18]

Most industry commenters objected to the breadth of the proposed definition of "identity theft." They recommended that the definition include only actual fraud committed using identifying information of a consumer, and exclude attempted fraud, identity theft committed against businesses, and any identity fraud involving the creation of a fictitious identity using fictitious data combined with real information from

[15] *See* 15 U.S.C. 1681a(r)(5).

[16] *See* 15 U.S.C. 1681a(b).

[17] Proposed § __.90(d)(1) required this determination to be substantiated by a risk evaluation that takes into consideration which customer accounts of the financial institution or creditor are subject to a risk of identity theft.

[18] 69 FR 63922 (Nov. 3, 2004) (codified at 16 CFR 603.2(a)). Section 111 of the FACT Act added several new definitions to the FCRA, including "identity theft," and authorized the FTC to further define this term. *See* 15 U.S.C. 1681a.

multiple individuals. By contrast, consumer groups supported a broad interpretation of "identity theft," including the incorporation of "attempted fraud" in the definition.

Section __.90(b)(8) of the final rules adopts the definition of "identity theft" as proposed. The Agencies believe that it is important to ensure that all provisions of the FACT Act that address identity theft are interpreted in a consistent manner. Therefore, the final rule continues to define identity theft with reference to the FTC's regulation, which as currently drafted provides that the term "identity theft" means "a fraud committed or attempted using the identifying information of another person without authority." [19] The FTC defines the term "identifying information" to mean "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

(1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

Thus, under the FTC's regulation, the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of "identity theft" because such a fraud involves "using the identifying information of another person without authority." [20]

Section __.90(b)(9) Red Flag. The proposed regulations defined "Red Flag" as a pattern, practice, or specific activity that indicates the possible risk of identity theft. The preamble to the proposed rules explained that indicators of a "possible risk" of identity theft would include precursors to identity theft such as phishing,[21] and security breaches involving the theft of personal information, which often are a means to acquire the information of another person for use in committing identity theft. The preamble explained that the Agencies included such precursors to identity theft as "Red Flags" to better position financial institutions and creditors to stop identity theft at its inception.

Most industry commenters objected to the broad scope of the definition of "Red Flag," particularly the phrase "possible risk of identity theft." These commenters believed that this definition would require financial institutions and creditors to identify all risks and develop procedures to prevent or mitigate them, without regard to the significance of the risk. They asserted that the statute does not support the use of "possible risk" and suggested defining a "Red Flag" as an indicator of significant, substantial, or the probable risk of identity theft. These commenters stated that this would allow a financial institution or creditor to focus compliance in areas where it is most needed.

Most industry commenters also stated that the inclusion of precursors to identity theft in the definition of "Red Flag" would make the regulations even broader and more burdensome. They stated that financial institutions and creditors do not have the ability to detect and respond to precursors, such as phishing, in the same manner as other Red Flags that are more indicative of actual ongoing identity theft.

By contrast, consumer groups supported the inclusion of the phrase "possible risk of identity theft" and the reference to precursors in the proposed definition of "Red Flag." These commenters stated that placing emphasis on detecting precursors to identity theft, instead of waiting for proven cases, is the right approach.

The Agencies have concluded that the phrase "possible risk" in the proposed definition of "Red Flag" is confusing and could unduly burden entities with limited resources. Therefore, the final rules define "Red Flag" in § __.90(b)(9) using language derived directly from section 114, namely, "a pattern, practice, or specific activity that indicates the possible existence of identity theft." [22]

The Agencies continue to believe, however, that financial institutions and creditors should consider precursors to identity theft in order to stop identity theft before it occurs. Therefore, as described below, the Agencies have chosen to address precursors directly, through a substantive provision in section IV of the guidelines titled "Prevention and Mitigation," rather than through the definition of "Red Flag." This provision states that a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft in determining an appropriate response to the Red Flags it detects.

Section __.90(b)(10) Service Provider. The proposed regulations defined "service provider" as a person that provides a service directly to the financial institution or creditor. This definition was based upon the definition of "service provider" in the Information Security Standards.[23]

One commenter agreed with this definition. However, two other commenters stated that the definition was too broad. They suggested narrowing the definition of "service provider" to persons or entities that have access to customer information.

Section __.90(b)(10) of the final rules adopts the definition as proposed. The Agencies have concluded that defining "service provider" to include only persons that have access to customer information would inappropriately narrow the coverage of the final rules. The Agencies have interpreted section 114 broadly to require each financial institution and creditor to detect, prevent, and mitigate identity theft not only in connection with any existing covered account, but also in connection with the opening of an account. A financial institution or creditor is ultimately responsible for complying with the final rules and guidelines even if it outsources an activity to a third-party service provider. Thus, a financial institution or creditor that uses a service provider to open accounts will need to provide for the detection, prevention, and mitigation of identity theft in connection with this activity, even when the service provider has access to the information of a person who is not yet, and may not become, a "customer."

Section __.90(c) Periodic Identification of Covered Accounts

To simplify compliance with the final rules, the Agencies added a new provision in § __.90(c) that requires each financial institution and creditor to periodically determine whether it offers or maintains any covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it

[19] *See* 16 CFR 603.2(a).

[20] *See* 16 CFR 603.2(b).

[21] Electronic messages to customers of financial institutions and creditors directing them to provide personal information in response to a fraudulent e-mail.

[22] 15 U.S.C. 1681m(c)(2)(A).

[23] The Information Security Standards define "service provider" to mean any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through the provision of services directly to the financial institution. 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D–2 and part 225, app. F (state member banks and holding companies); 12 CFR part 364, app. B (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, App. A (credit unions).

offers or maintains covered accounts described in § __.90(b)(3)(ii) (accounts other than consumer accounts), taking into consideration:

- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.

Thus, a financial institution or creditor should consider whether, for example, a reasonably foreseeable risk of identity theft may exist in connection with business accounts it offers or maintains that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the internet or telephone. In addition, those institutions and creditors that offer or maintain business accounts that have been the target of identity theft should factor those experiences with identity theft into their determination.

This provision is modeled on various process-oriented and risk-based regulations issued by the Agencies, such as the Information Security Standards. Compliance with this type of regulation is based upon a regulated entity's own preliminary risk assessment. The risk assessment required here directs a financial institution or creditor to determine, as a threshold matter, whether it will need to have a Program.[24] If a financial institution or creditor determines that it does need a Program, then this risk assessment will enable the financial institution or creditor to identify those accounts the Program must address. This provision also requires a financial institution or creditor that initially determines that it does not need to have a Program to reassess periodically whether it must develop and implement a Program in light of changes in the accounts that it offers or maintains and the various other factors set forth in the provision.

Section __.90(d)(1) Identity Theft Prevention Program Requirement

Proposed § __.90(c) described the primary objectives of a Program. It stated that each financial institution or creditor must implement a written Program that includes reasonable policies and procedures to address the risk of identity theft to its customers and to the safety and soundness of the financial institution or creditor, in the manner described in proposed § __.90(d), which described the development and implementation of a Program. It also stated that the Program must address financial, operational, compliance, reputation, and litigation risks and be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

Some commenters believed that the proposed regulations exceeded the scope of section 114 by covering deposit accounts and by requiring a response to the risk of identity theft, not just the identification of the risk of identity theft. One commenter expressed concern about the application of the Program to existing accounts.

The SBA commented that requiring all small businesses covered by the regulations to create a written Program would be overly burdensome. Several financial institution commenters objected to what they perceived as a proposed requirement that financial institutions and creditors have a written Program solely to address identity theft. They recommended that the final regulations allow a covered entity to simply maintain or expand its existing fraud prevention and information security programs as long as they included the detection, prevention, and mitigation of identity theft. Some of these commenters stated that requiring a written program would merely focus examiner attention on documentation and cause financial institutions to produce needless paperwork.

While commenters generally agreed that the Program should be appropriate to the size and complexity of the financial institution or creditor, and the nature and scope of its activities, many industry commenters objected to the prescriptive nature of this section. They urged the Agencies to provide greater flexibility to financial institutions and creditors by allowing them to implement their own procedures as opposed to those provided in the proposed regulations. Several other commenters suggested permitting financial institutions and creditors to take into account the cost and effectiveness of policies and procedures and the institution's history of fraud when designing its Program.

Several financial institution commenters maintained that the Program required by the proposed rules was not sufficiently flexible. They maintained that a true risk-based approach would permit institutions to prioritize the importance of various controls, address the most important risks first, and accept the good faith judgments of institutions in differentiating among their options for conducting safe, sound, and compliant operations. Some of these commenters urged the Agencies to revise the final rules and guidelines and adopt an approach similar to the Information Security Standards which they characterized as providing institutions with an outline of issues to consider without requiring specific approaches.

Although a few commenters believed that the proposed requirement to update the Program was burdensome and should be eliminated, most commenters agreed that the Program should be designed to address changing risks over time. A number of these commenters, however, objected to the requirement that the Program must be designed to address changing identity theft risks "as they arise," as too burdensome a standard. Instead, they recommended that the final regulations require a financial institution or creditor to reassess periodically whether to adjust the types of accounts covered or Red Flags to be detected based upon any changes in the types and methods of identity theft that an institution or creditor has experienced.

Section __.90(d) of the final rules requires each financial institution or creditor that offers or maintains one or more covered accounts to develop and implement a written Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. To signal that the final rules are flexible, and allow smaller financial institutions and creditors to tailor their Programs to their operations, the final rules state that the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

The guidelines are appended to the final rules to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the regulation. Section I of the guidelines, titled "The Program," makes clear that a covered entity may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program. This will avoid duplication and allow covered entities to benefit from existing policies and procedures.

The Agencies do not agree with those commenters who asserted that the scope of the proposed regulations (and hence the final rules that adopt the identical approach with respect to these issues)

[24] The Agencies anticipate that some financial institutions and creditors, such as various creditors regualted by the FTC that solely engage in business-to-business transactions, will be able to determine that they do not need to develop and implement a Program.

exceed the Agencies" statutory mandate. First, section 114 clearly permits the Agencies to issue regulations and guidelines that address more than the mere identification of the risk of identity theft. Section 114 contains a broad mandate directing the Agencies to issue guidelines "regarding identity theft" and to prescribe regulations requiring covered entities to establish reasonable policies and procedures for implementing the guidelines. Second, two provisions in section 114 indicate that Congress expected the Agencies to issue final regulations and guidelines requiring financial institutions and creditors to detect, prevent, and mitigate identity theft.

The first relevant provision is codified in section 615(e)(1)(C) of the FCRA, where Congress addressed a particular scenario involving card issuers. In that provision, Congress directed the Agencies to prescribe regulations requiring a card issuer to take specific steps to assess the validity of a change of address request when it receives such a request and, within a short period of time, also receives a request for an additional or replacement card. The regulations must prohibit a card issuer from issuing an additional or replacement card under such circumstances, unless it notifies the cardholder or "uses other means of assessing the validity of the change of address in accordance with reasonable policies and procedures established by the card issuer in accordance with the regulations prescribed [by the Agencies] * * *." This provision makes clear that Congress contemplated that the Agencies' regulations would require a financial institution or creditor to have policies and procedures not only to identify Red Flags, but also, to prevent and mitigate identity theft.

The second relevant provision is codified in section 615(e)(2)(B) of the FCRA, and directs the Agencies to consider addressing in the identity theft guidelines transactions that occur with respect to credit or deposit accounts that have been inactive for more than two years. The Agencies must consider whether a creditor or financial institution detecting such activity should "follow reasonable policies that provide for notice to be given to the consumer in a manner reasonably designed to reduce the likelihood of identity theft with respect to such account." This provision signals that the Agencies are authorized to prescribe regulations and guidelines that comprehensively address identity theft—in a manner that goes beyond the mere identification of possible risks.

The Agencies' interpretation of section 114 is also supported by the legislative history that indicates Congress expected the Agencies to issue regulations and guidelines for the purposes of "identifying and preventing identity theft." [25]

Finally, the Agencies' interpretation of section 114 is broad, based on a public policy perspective that regulations and guidelines addressing the identification of the risk of identity theft, without addressing the prevention and mitigation of identity theft, would not be particularly meaningful or effective.

The Agencies also have concluded that the scope of section 114 does not only apply to credit transactions, but also applies, for example, to deposit accounts. Section 114 refers to the risk of identity theft, generally, and not strictly in connection with credit. Because identity theft can and does occur in connection with various types of accounts, including deposit accounts, the final rules address identity theft in a comprehensive manner.

Furthermore, nothing in section 114 indicates that the regulations must only apply to identity theft in connection with account openings. The FTC has defined "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." [26] Such fraud may occur in connection with account openings and with existing accounts. Section 615(e)(3) states that the guidelines that the Agencies prescribe "shall not be inconsistent" with the policies and procedures required under 31 U.S.C. 5318(l), a reference to the CIP rules which require certain financial institutions to verify the identity of customers opening new accounts. However, the Agencies do not read this phrase to prevent them from prescribing rules directed at existing accounts. To interpret the provision in this manner would solely authorize the Agencies to prescribe regulations and guidelines identical to and duplicative of those already issued—making the Agencies' regulatory authority in this area superfluous and meaningless.[27]

The Agencies recognize that requiring a written Program will impose some burden. However, the Agencies believe the benefit of being able to assess a covered entity's compliance with the final rules by evaluating the adequacy and implementation of its written Program outweighs the burdens imposed by this requirement.

Moreover, although the final rules continue to require a written Program, as detailed below, the Agencies have substantially revised the proposal to focus the final rules and guidelines on reasonably foreseeable risks, make the final rules less prescriptive, and provide financial institutions and creditors with more discretion to develop policies and procedures to detect, prevent, and mitigate identity theft.

Proposed §__.90(c) also provided that the Program must address changing identity theft risks as they arise based upon the experience of the financial institution or creditor with identity theft and changes in: Methods of identity theft; methods to detect, prevent, and mitigate identity theft; the types of accounts the financial institution or creditor offers; and its business arrangements, such as mergers and acquisitions, alliances and joint ventures, and service provider arrangements.

The Agencies continue to believe that, to ensure a Program's continuing effectiveness, it must be updated, at least periodically. However, in order to simplify the final rules, the Agencies moved this requirement into the next section, where it is one of the required elements of the Program, as discussed below.

Development and Implementation of Identity Theft Prevention Program

The remaining provisions of the proposed rules were set forth under the above-referenced section heading. Many commenters asserted that the Agencies should simply articulate certain objectives and provide financial institutions and creditors the flexibility and discretion to design policies and procedures to fulfill the objectives of the Program without the level of detail required under this section.

As described earlier, to ensure that financial institutions and creditors are able to design Programs that effectively address identity theft in a manner tailored to their own operations, the Agencies have made significant changes in the proposal by deleting whole provisions or moving them into the guidelines in Appendix J. More specifically, the Agencies abbreviated the proposed requirements formerly located in the provisions titled

[25] *See* S. Rep. No. 108–166 at 13 (Oct 17, 2003) (accompanying S. 1753).

[26] 16 CFR 603.2(a).

[27] The Agencies' conclusion is also supported by case law interpreting similar terminology, albeit in a different context, finding that "inconsistent" means it is impossible to comply with two laws simultaneously, or one law frustrates the purposes and objectives of another. *See, e.g., Davenport v. Farmers Ins. Group*, 378 F.3d 839 (8th Cir. 2004); *Retail Credit Co. v. Dade County, Florida*, 393 F. Supp. 577 (S.D. Fla. 1975); *Alexiou v. Brad Benson Mitsubishi*, 127 F. Supp 2d 557 (D N.J 2000).

"Identification and Evaluation of Red Flags" and "Identity Theft Prevention and Mitigation" and have placed them under a section of the final rules titled "Elements of a Program." The proposed requirements on "Staff Training," "Oversight of Service Provider Arrangements," and "Involvement of Board of Directors and Senior Management" are now in a section of the final rules titled "Administration of the Program." The guidelines in Appendix J elaborate on these requirements. A discussion of the comments received on these sections of the proposed rules, and the corresponding sections of the final rules and guidelines follows.

Section __.90(d)(2)(i) Element I of the Program: Identification of Red Flags

Proposed § __.90(d)(1)(i) required a Program to include policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor, using the risk evaluation described in § __.90(d)(1)(ii). It also required the Red Flags identified to reflect changing identity theft risks to customers and to the financial institution or creditor as they arise.

Proposed § __.90(d)(1)(i) provided that each financial institution and creditor must incorporate into its Program relevant Red Flags from Appendix J. The preamble to the proposed rules acknowledged that some Red Flags that are relevant today may become obsolete as time passes. The preamble stated that the Agencies expected to update Appendix J periodically,[28] but that it may be difficult to do so quickly enough to keep pace with rapidly evolving patterns of identity theft or as quickly as financial institutions and creditors experience new types of identity theft. Therefore, proposed § __.90(d)(1)(i) also provided that each financial institution and creditor must incorporate into its Program relevant Red Flags from applicable supervisory guidance, incidents of identity theft that the financial institution or creditor has experienced, and methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.

Some commenters objected to the proposed requirement that the Program contain policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor. They criticized the phrase "possible risk" as too broad and stated that it was unrealistic to impose upon covered entities a continuing obligation to incorporate into their Programs Red Flags to address virtually any new identity theft incident or trend and potential fraud prevention measure. These commenters stated that this would be a burdensome compliance exercise that would limit flexibility and add costs, which in turn, would take away limited resources from the ultimate objective of combating identity theft.

Many commenters objected to the proposed requirement that the Red Flags identified by a financial institution or creditor reflect changing identity theft risks to customers and to the financial institution or creditor "as they arise." These commenters requested that the final rules permit financial institutions and creditors a reasonable amount of time to adjust the Red Flags included in their Programs.

Some commenters agreed that the enumerated sources of Red Flags were appropriate. A few commenters stated that financial institutions and creditors should not be required to include in their Programs any Red Flags except for those set forth in Appendix J or in supervisory guidance, or that they had experienced. However, most commenters objected to the requirement that, at a minimum, the Program incorporate any relevant Red Flags from Appendix J.

Some financial institution commenters urged deletion of the proposed requirement to include a list of relevant Red Flags in their Program. They stated that a financial institution should be able to assess which Red Flags are appropriate without having to justify to an examiner why it failed to include a specific Red Flag on a list. Other commenters recommended that the list of Red Flags in Appendix J be illustrative only. These commenters recommended that a financial institution or creditor be permitted to include any Red Flags on its list that it concludes are appropriate. They suggested that the Agencies encourage institutions to review the list of Red Flags, and use their own experience and expertise to identify other Red Flags that become apparent as fraudsters adapt and develop new techniques. They maintained that in this manner, institutions and creditors would be able to identify the appropriate Red Flags and not waste limited resources and effort addressing those Red Flags in Appendix J that were obsolete or not appropriate for their activities.

By contrast, consumer groups criticized the flexibility and discretion afforded to financial institutions and creditors in this section of the proposed rules. These commenters urged the Agencies to make certain Red Flags from Appendix J mandatory, such as a fraud alert on a consumer report.

Proposed § __.90(d)(1)(ii) provided that in order to identify which Red Flags are relevant to detecting a possible risk of identity theft to its customers or to its own safety and soundness, the financial institution or creditor must consider:

A. Which of its accounts are subject to a risk of identity theft;

B. The methods it provides to open these accounts;

C. The methods it provides to access these accounts; and

D. Its size, location, and customer base.

While some industry commenters thought the enumerated factors were appropriate, other commenters stated that the factors on the list were not necessarily the ones used by financial institutions to identify risk and were irrelevant to any determination of identity theft or actual fraud. These commenters maintained that this proposed requirement would require financial institutions to develop entirely new programs that may not be as effective or efficient as those designed by anti-fraud experts. Therefore, they recommended that the final rules provide financial institutions and creditors with wide latitude to determine what factors they should consider and how they categorize them. These commenters urged the Agencies to refrain from providing a list of factors that financial institutions and creditors would have to consider because a finite list could limit their ability to adapt to new forms of identity theft.

Some commenters suggested that the risk evaluation include an assessment of other factors such as the likelihood of harm, the cost and operational burden of using a particular Red Flag and the effectiveness of a particular Red Flag for that institution or creditor. Some commenters suggested that the factors refer to the likely risk of identity theft, while others suggested that the factors be modified to refer to the possible risk of identity theft to which each type of account offered by the financial institution or creditor is subject. Other commenters, including a trade association representing small financial institutions, asked the Agencies to provide guidelines on how to conduct a risk assessment.

[28] Section 114 directs the Agencies to update the guidelines as often as necessary. *See* 15 U.S.C. 1681m(e)(1)(a).

The final rules continue to address the identification of relevant Red Flags, but simply state that the first element of a Program must be reasonable policies and procedures to identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains. The final rules also state that a financial institution or creditor must incorporate these Red Flags into its Program.

The final rules do not require policies and procedures for identifying which Red Flags are relevant to detecting a "possible risk" of identity theft. Moreover, as described below, a covered entity's obligation to update its Red Flags is now a separate element of the Program. The section of the proposed rules describing the various factors that a financial institution or creditor must consider to identify relevant Red Flags, and the sources from which a financial institution or creditor must derive its Red Flags, are now in section II of the guidelines titled " Identifying Relevant Red Flags."

The Agencies acknowledge that establishing a finite list of factors that a financial institution or creditor must consider when identifying relevant Red Flags for covered accounts could limit the ability of a financial institution or creditor to respond to new forms of identity theft. Therefore, section II of the guidelines contains a list of factors that a financial institution or creditor "should consider * * * as appropriate" in identifying relevant Red Flags.

The Agencies also modified the list in order to provide more appropriate examples of factors for consideration by a financial institution or creditor determining which Red Flags may be relevant. These factors are:

- The types of covered accounts it offers or maintains;
- The methods it provides to open its covered accounts;
- The methods it provides to access its covered accounts; and
- Its previous experiences with identity theft.

Thus, for example, Red Flags relevant to deposit accounts may differ from those relevant to credit accounts, and those applicable to consumer accounts may differ from those applicable to business accounts. Red Flags appropriate for accounts that may be opened or accessed remotely may differ from those that require face-to-face contact. In addition, a financial institution or creditor should consider identifying as relevant those Red Flags that directly relate to its previous experiences with identity theft.

Section II of the guidelines also gives examples of sources from which financial institutions and creditors should derive relevant Red Flags, rather than requiring that the Program incorporate relevant Red Flags strictly from the four sources listed in the proposed rules. Section II states that a financial institution or creditor should incorporate into its Program relevant Red Flags from sources such as: (1) Incidents of identity theft that the financial institution or creditor has experienced; (2) methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and (3) applicable supervisory guidance.

The Agencies have deleted the reference to the Red Flags in Appendix J as a source. Instead, a separate provision in section II of the guidelines, titled "Categories of Red Flags," states that the Program of a financial institution or creditor "should include" relevant Red Flags from five particular categories "as appropriate." The Agencies have included these categories, which summarize the various types of Red Flags that were previously enumerated in Appendix J, in order to provide additional non-prescriptive guidance regarding the identification of relevant Red Flags.

Section II of the guidelines also notes that "examples" of individual Red Flags from each of the five categories are appended as Supplement A to Appendix J. The examples in Supplement A are a list of Red Flags similar to those found in the proposed rules. The Agencies did not intend for these examples to be a comprehensive list of all types of identity theft that a financial institution or creditor may experience. When identifying Red Flags, financial institutions and creditors must consider the nature of their business and the type of identity theft to which they may be subject. For instance, creditors in the health care field may be at risk of medical identity theft (*i.e.*, identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk.

The Agencies also have decided not to single out any specific Red Flags as mandatory for all financial institutions and creditors. Rather, the final rule continues to follow the risk-based, non-prescriptive approach regarding the identification of Red Flags that was set forth in the proposal. The Agencies recognize that the final rules and guidelines cover a wide variety of financial institutions and creditors that offer and maintain many different products and services, and require the flexibility to be able to adapt to rapidly changing risks of identity theft.

Sections __.90(d)(2)(ii) and (iii) Elements II and III of the Program: Detection of and Response to Red Flags

Proposed § __.90(d)(2) stated that the Program must include reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account. This section then described the policies and procedures that the Program must include, some of which related solely to account openings while others related to existing accounts.

Some financial institution commenters acknowledged that reference to prevention and mitigation of identity theft was generally a good objective, but they urged that the final rules refrain from prescribing how financial institutions must achieve it. Others noted that the CIP rules and the Information Security Standards already required many of the steps in the proposal. They recommended that the final rules recognize this and clarify that compliance with parallel requirements would be sufficient for compliance under these rules.

Section __.90(d)(1) of the final rules requires financial institutions and creditors to develop and implement a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Therefore, the Agencies concluded that it was not necessary to reiterate this requirement in § __.90(d)(2). The Agencies have deleted the prefatory language from proposed § __.90(d)(2) on prevention and mitigation in order to streamline the final rules. The various provisions addressing prevention and mitigation formerly in this section, namely, verification of identity, detection of Red Flags, assessment of the risk of Red Flags, and responses to the risk of identity theft, have been incorporated into the final rules as "Elements of the Program" and into the guidelines elaborating on these provisions. Comments received regarding these provisions and the manner in which they have been integrated into the final rules and guidelines follows.

Detecting Red Flags

Proposed § __.90(d)(2)(i) stated that the Program must include reasonable policies and procedures to obtain identifying information about, and verify the identity of, a person opening an account. This provision was designed to address the risk of identity

theft to a financial institution or creditor that occurs in connection with the opening of new accounts.

The proposed rules stated that any financial institution or creditor would be able to satisfy the proposed requirement in § __.90(d)(2)(i) by using the policies and procedures for identity verification set forth in the CIP rules. The preamble to the proposed rules explained that although the CIP rules exclude a variety of entities from the definition of "customer" and exclude a number of products and relationships from the definition of "account," [29] the Agencies were not proposing any exclusions from either of these terms given the risk-based nature of the regulations.

Most commenters supported this provision. Many of these commenters urged the Agencies to include in the final rules a clear statement acknowledging that financial institutions and creditors complying with the CIP rules would be deemed to be in compliance with this provision's requirements. Some of these commenters encouraged the Agencies to place the exemptions from the CIP rules in these final rules for consistency in implementing both regulatory mandates.

Some commenters, however, believed the requirement to verify the identity of a person opening an account duplicated the requirements in the CIP rules and urged elimination of this redundancy. Other entities not already subject to the CIP rules stated that complying with those rules would be very costly and burdensome. These commenters asked that the Agencies provide them with additional guidance regarding the CIP rules.

Consumer groups were concerned that use of the CIP rules would not adequately address identity theft. They stated that the CIP rules allow accounts to be opened before identity is verified, which is not the proper standard to prevent identity theft.

As described below, the Agencies have moved verification of the identity of persons opening an account into section III of the guidelines where it is described as one of the policies and procedures that a financial institution or creditor should have to detect Red Flags in connection with the opening of a covered account.

Proposed § __.90(d)(2)(ii) stated that the Program must include reasonable policies and procedures to detect the Red Flags identified pursuant to paragraph § __.90(d)(1). The Agencies did not receive any specific comments on this provision.

[29] *See, e.g.*, 31 CFR 103.121(a).

In the final rules, the detection of Red Flags is the second element of the Program. The final rules provide that a Program must contain reasonable policies and procedures to detect the Red Flags that a financial institution or creditor has incorporated into its Program.

Section III of the guidelines provides examples of various means to detect Red Flags. It states that the Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts, such as by obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the CIP rules. Section III also states that the Program's policies and procedures should address the detection of Red Flags in connection with existing covered accounts, such as by authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

Covered entities subject to the CIP rules, the Federal Financial Institution's Examination Council's guidance on authentication,[30] the Information Security Standards, and Bank Secrecy Act (BSA) rules [31] may already be engaged in detecting Red Flags. These entities may wish to integrate the policies and procedures already developed for purposes of complying with these issuances into their Programs. However, such policies and procedures may need to be supplemented. For example, the CIP rules were written to implement section 326 [32] of the USA PATRIOT Act,[33] an Act directed toward facilitating the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Certain types of "accounts," "customers," and products are exempted or treated specially in the CIP rules because they pose a lower risk of money laundering or terrorist financing. Such special treatment may not be appropriate to accomplish the broader objective of detecting, preventing, and mitigating identity theft. Accordingly, the Agencies expect all financial institutions and creditors to evaluate the adequacy of existing policies and procedures and to develop and implement risk-based policies and procedures that detect Red Flags in an effective and comprehensive manner.

[30] "Authentication in an Internet Banking Environment" (October 12, 2005) available at *http://www.ffiec.gov/press/pr101205.htm.*

[31] *See, e.g.* 12 CFR 21.21 (national banks); 12 CFR 208.63 (state member banks); 12 CFR 326.8 (state non-member banks); 12 CFR 563.177 (savings associations); and 12 CFR 748.2 (credit unions)

[32] 31 U.S.C. 5318(l).

[33] Pub. L. 107–56

Responding to Red Flags

Proposed § __.90(d)(2)(iii) stated that to prevent and mitigate identity theft, the Program must include policies and procedures to assess whether the Red Flags the financial institution or creditor detected pursuant to proposed § __.90(d)(2)(ii) evidence a risk of identity theft. It also stated that a financial institution or creditor must have a reasonable basis for concluding that a Red Flag (detected) does not evidence a risk of identity theft.

Financial institution commenters expressed concern that this standard would force an institution to justify to examiners why it did not take measures to respond to a particular Red Flag. Some consumer groups believed it was appropriate to require a financial institution or creditor to have a reasonable basis for concluding that a particular Red Flag detected does not evidence a risk of identity theft. Other consumer groups believed that this was too weak a standard and that mandating the detection of certain Red Flags would be more effective and preventive.

Some commenters mistakenly read the proposed provision as requiring a financial institution or creditor to have a reasonable basis for excluding a Red Flag listed in Appendix J from its Program requiring the mandatory review and analysis of each and every Red Flag. These commenters urged the Agencies to delete this provision.

Proposed § __.90(d)(2)(iv) stated that to prevent and mitigate identity theft, the Program must include policies and procedures that address the risk of identity theft to the customer, the financial institution, or creditor, commensurate with the degree of risk posed. The proposed regulations also provided an illustrative list of measures that a financial institution or creditor could take, including:

- Monitoring an account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a customer's account;
- Reopening an account with a new account number;
- Not opening a new account;
- Closing an existing account;
- Notifying law enforcement and, for those that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

• Implementing any requirements regarding limitations on credit extensions under 15 U.S.C. 1681c–1(h), such as declining to issue an additional credit card when the financial institution or creditor detects a fraud or active duty alert associated with the opening of an account, or an existing account; or

• Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, to correct or update inaccurate or incomplete information.

Some commenters agreed that financial institutions and creditors should be able to use their own judgment to determine which measures to take depending upon the degree of risk that is present. However, consumer groups believed that the final rules should require notification of consumers in every case where a Red Flag that requires a response has been detected.

Other commenters objected to some of the examples given as measures that financial institutions and creditors could take to address the risk of identity theft. For example, one commenter objected to the inclusion, as an example, of the requirements regarding limitations on credit extensions under 15 U.S.C. 1681c–1(h). The commenter stated that this statutory provision is confusing, useless, and should not be referenced in the final rules. Other commenters suggested that the Agencies clarify that the inclusion of this statutory provision in the proposed rules as an example of how to address the risk of identity theft did not make this provision discretionary.

The final rules merge the concepts previously in proposed § __.90(d)(2)(iii) and § __.90(d)(2)(iv) into the third element of the Program: reasonable policies and procedures to respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft.

In order to "respond appropriately," it is implicit that a financial institution or creditor must assess whether the Red Flags detected evidence a risk of identity theft, and must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft. Therefore, the Agencies concluded that it is not necessary to specify any such separate assessment, and, accordingly, deleted the language from the proposal regarding assessing Red Flags and addressing the risk of identity theft.

Most of the examples of measures for preventing and mitigating identity theft previously listed in proposed § __.90(d)(2)(iv) are now located in section IV of the guidelines, titled "Prevention and Mitigation of Identity Theft." Section IV states that the Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In addition, as described earlier, the final rules do not define Red Flags to include indicators of a "possible risk" of identity theft (including "precursors" to identity theft). Instead, section IV states that in determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, and provides examples of such factors.

The Agencies also modified the examples of appropriate responses as follows. First, the Agencies added "not attempting to collect on a covered account or not selling a covered account to a debt collector" as a possible response to Red Flags detected. Second, the Agencies added "determining that no response is warranted under the particular circumstances" to make clear that an appropriate response may be no response, especially, for example, when a financial institution or creditor has a reasonable basis for concluding that the Red Flags detected do not evidence a risk of identity theft.

In addition, the Agencies moved the proposed examples, that referenced responses mandated by statute, to section VII of the guidelines titled "Other Applicable Legal Requirements" to highlight that certain responses are legally required.

The section of the proposal listing examples of measures to address the risk of identity theft included a footnote that discussed the relationship between a consumer's placement of a fraud or active duty alert on his or her consumer report and ECOA, 15 U.S.C. 1691, *et seq.* A few commenters objected to this footnote. Some commenters believed that creditors had a right to deny credit automatically whenever a fraud or active duty alert appears on the consumer report of an applicant. Other commenters believed that the footnote raised complex issues under the ECOA and FCRA that required more thorough consideration, and questioned the need and appropriateness of addressing ECOA in the context of this rulemaking.

Under ECOA, it is unlawful for a creditor to discriminate against any applicant for credit because the applicant has in good faith exercised any right under the Consumer Credit Protection Act (CCPA), 15 U.S.C. 1691(a). A consumer who requests the inclusion of a fraud alert or active duty alert in his or her credit file is exercising a right under the FCRA, which is a part of the CCPA, 15 U.S.C. 1601, *et seq.* When a credit file contains a fraud or active duty alert, section 605A of the FCRA, 15 U.S.C. 1681c–1(h), requires a creditor to take certain steps before extending credit, increasing a credit limit, or issuing an additional card on an existing credit account. For an initial or active duty alert, these steps include utilizing reasonable policies and procedures to form a reasonable belief that the creditor knows the identity of the consumer and, where a consumer has specified a telephone number for identity verification purposes, contacting the consumer at that telephone number or taking reasonable steps to verify the consumer's identity and confirm that the application is not the result of identity theft, 15 U.S.C. 1681c–1(h)(1)(B).

The purpose of the footnote was to remind financial institutions and creditors of their legal responsibilities in circumstances where a consumer has placed a fraud or active duty alert on his or her consumer report. In particular, the Agencies have concerns that in some cases, creditors have adopted policies of automatically denying credit to consumers whenever an initial fraud alert or an active duty alert appears on an applicant's consumer report. The Agencies agree that this rulemaking is not the appropriate vehicle for addressing issues under ECOA. However, the Agencies will continue to evaluate compliance with ECOA through their routine examination or enforcement processes, including issues related to fraud and active duty alerts.

Section __.90(d)(2)(iv) Element IV of the Program: Updating the Program

To ensure that the Program of a financial institution or creditor remains effective over time, the final rules provide a fourth element of the Program: policies and procedures to ensure the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft. As described earlier, this element replaces the requirements formerly in proposed § __.90(c)(2) which stated that the Program must be designed to address changing identity theft risks as they arise, and proposed § __.90(d)(1)(i) which stated that the Red Flags included in a covered entity's Program must reflect changing identity theft risks to customers and to the financial institution or creditor as they arise.

Unlike the proposed provisions, however, this element only requires "periodic" updating. The Agencies concluded that requiring financial institutions and creditors to immediately and continuously update their Programs would be overly burdensome.

Section V of the guidelines elaborates on the obligation to ensure that the Program is periodically updated. It reiterates the factors previously in proposed § __.90(c)(2) that should cause a financial institution or creditor to update its Program, such as its own experiences with identity theft, changes in methods of identity theft, changes in methods to detect, prevent and mitigate identity theft, changes in accounts that it offers or maintains, and changes in its business arrangements.

Section __.90(e) Administration of the Program

The final rules group the remaining provisions of the proposed rules under the heading "Administration of the Program," albeit in a different order than proposed. This section of the final rules describes the steps that financial institutions and creditors must take to administer the Program, including: Obtaining approval of the initial written Program; ensuring oversight of the development, implementation and administration of the Program; training staff; and overseeing service provider arrangements.

A number of commenters criticized each of the proposed provisions regarding administration of the Program, arguing they were not specifically required by section 114. The Agencies believe the mandate in section 114 is broad, and provides the Agencies with an ample basis to issue rules and guidelines containing these provisions because they are critical to ensuring the effectiveness of a Program. Therefore, the Agencies have retained these elements in the final rules and guidelines with some modifications, as follows.

Sections __.90(e)(1) and (2) Involvement of the Board of Directors and Senior Management

Proposed § __.90(d)(5) highlighted the responsibility of the board of directors and senior management to develop, implement, and oversee the Program. Proposed § __.90(d)(5)(i) specifically required the board of directors or an appropriate committee of the board to approve the written Program. Proposed § __.90(d)(5)(ii) required that the board, an appropriate committee of the board, or senior management be charged with overseeing the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation. The proposal also provided that persons charged with overseeing the Program must review reports prepared at least annually by staff regarding compliance by the financial institution or creditor with the regulations.

Proposed § __.90(d)(5)(iii) stated that reports must discuss material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes in the Program.

Some commenters agreed that identity theft is an important issue, and the board, therefore, should be involved in the overall development, approval, and oversight of the Program. These commenters suggested that the final rules make clear that the board need not be responsible for the day-to-day operations of the Program.

Most industry commenters opposed the proposed requirement that the board or board committee approve the Program and receive annual reports about compliance with the Program. These commenters asserted that the statute does not mandate such requirements, and that compliance with these rules did not warrant more board attention than other regulations. They asserted that such requirements would impede the ability of a financial institution or creditor to keep up with the fast-paced changes and developments inherent with instances of fraud and identity theft. They stated that boards of directors should not be required to consider the minutiae of the fraud prevention efforts of a financial institution or creditor and suggested the task be delegated to senior management with expertise in this area. Some commenters suggested the final rules provide a covered entity with the discretion to assign oversight responsibilities in a manner consistent with the institution's own risk evaluation.

One commenter suggested that the final rules permit the board of directors of a holding company to approve and oversee the Program for the entire organization. The commenter explained that this approach would eliminate the need for redundant actions by a multiplicity of boards, and help to insure uniformity of policy throughout large organizations.

Some commenters stated that the preparation of reports for board review would be costly and burdensome. The SBA suggested that the FTC consider a one-page certification option for small low-risk entities to minimize the burden of reports. One commenter opined that it would be sufficient if the Agencies mandated that covered entities continuously review and evaluate the policies and procedures they adopted pursuant to the regulations and modify them as necessary. Consumer groups suggested that the final rules specifically require financial institutions and creditors to adjust their Programs to address deficiencies raised by their annual reports.

Commenters generally took the position that reports to the board, a board committee, or senior management regarding compliance with the final rules should be prepared at most on a yearly basis, or when significant changes have occurred that alter the institution's risk. One commenter recommended a clarification that any reporting to the board of material information relating to the Program could be combined with reporting obligations required under the Information Security Standards.

Section __.90(e)(1) of the final rules continues to require approval of the written Program by the board of directors or an appropriate committee of the board. However, to ensure that this requirement does not hamper the ability of a financial institution or creditor to update its Program in a timely manner, the final rules provide that the board or an appropriate committee must approve only the initial written Program. Thereafter, at the discretion of the covered entity, the board, a committee, or senior management may update the Program.

Bank holding companies and their bank and non-bank subsidiaries will be governed by the principles articulated in connection with the banking agencies" Information Security Standards:

> The Agencies agree that subsidiaries within a holding company can use the security program developed at the holding company level. However, if subsidiary institutions choose to use a security program developed at the holding company level, the board of directors or an appropriate committee at each subsidiary institution must conduct an independent review to ensure that the program is suitable and complies with the requirements prescribed by the subsidiary's primary regulator * * *.
>
> 66 FR 8620 (Feb. 1, 2001) (Preamble to final Information Security Standards.)

The Agencies recognize that boards of directors have many responsibilities and it generally is not feasible for a board to involve itself in the detailed oversight, development, implementation, and administration of the Program. Accordingly, § __.90(e)(2) of the final rules provides discretion to a financial institution or creditor to determine who will be responsible for these aspects of the Program. It states that a financial institution or creditor must involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the Program.

Section VI of the guidelines elaborates on this provision of the final rules. The guidelines note that such oversight should include assigning specific responsibility for the Program's implementation and reviewing reports prepared by staff on compliance by the financial institution or creditor with this section. As suggested by commenters, the guidelines also state that oversight should include approving material changes to the Program as necessary to address changing identity theft risks. Section VI also provides that reports should be prepared at least annually and describes the contents of a report as proposed in § __.90(d)(5)(iii)(B).

These steps are modeled on sections of the Information Security Standards.[34] As noted previously, financial institutions and creditors subject to these Standards may combine elements required under the final rules and guidelines, including reports, with those required by the Standards, as they see fit.

Section __.90(e)(3) Staff Training

Proposed § __.90(d)(3) required each financial institution or creditor to train staff to implement its Program.

Consumer groups believed that this provision should be more detailed and specifically require monitoring, oversight, and auditing of a covered entity's training efforts. By contrast, a number of industry commenters recommended that the Agencies withdraw this provision because they believed it was burdensome. Some of these commenters asserted that the Agencies had not taken into account the limited personnel and resources available to smaller institutions to provide training.

Some financial institution commenters stated that it was not clear why staff training would be specifically required under the final rules, absent a specific statutory requirement. They maintained that financial institutions have sufficient incentives to ensure that appropriate staff is trained. Other commenters suggested that the Agencies clarify that this provision would only require training for relevant staff and would permit training on identity theft that is integrated into overall staff training on similar or overlapping matters such as fraud prevention.

One commenter objected to an example in the preamble to the proposed rules which stated that staff should be trained to detect "anomalous wire transfers in connection with a customer's deposit account." The commenter stated that this example potentially exposed financial institutions to significant and unintended liability, predicting that customers and law enforcement would use the rules to support claims that financial institutions are responsible for authorizing transactions by fraudsters. The commenter asserted that financial institutions do not have systems that can detect these transactions because they fall outside the usual fraud filter parameters.

Section __.90(e)(3) of the final rules provides that a covered entity must train staff, as necessary, to effectively implement the Program. There is no corresponding section of the guidelines.

The Agencies continue to believe proper training will enable staff to address the risk of identity theft. However, this provision requires training of only relevant staff. In addition, staff that has already been trained, for example, as a part of the anti-fraud prevention efforts of the financial institution or creditor, do not need to be re-trained except "as necessary."

The Agencies recognize that some of the examples, such as detecting "anomalous wire transfers in connection with a customer's deposit account" may fall outside the usual fraud filter parameters. However, the Agencies expect that compliance with the final rules will improve the ability of financial institutions and creditors to detect, prevent, and mitigate identity theft.

Section __.90(e)(4) Oversight of Service Provider Arrangements

Proposed § __.90(d)(4) stated that, whenever a financial institution or creditor engaged a service provider to perform an activity on its behalf and the requirements of the Program applied to that activity, the financial institution or creditor would be required to take steps designed to ensure the activity is conducted in compliance with a Program that satisfies the regulations. The preamble to the proposed rules explained that this provision would allow a service provider serving multiple financial institutions and creditors to conduct activities on behalf of these entities in accordance with its own program to prevent identity theft, as long as the program meets the requirements of the regulations. The service provider would not need to apply the particular Program of each individual financial institution or creditor to whom it is providing services.

Several commenters asserted it would be costly and burdensome for financial institutions and creditors to ensure third party compliance with the final rules and therefore, this provision should be eliminated. They urged that financial institutions and creditors be given maximum flexibility to manage service provider relationships.

Some financial institution commenters also suggested that the Agencies withdraw this provision. They stated that the FACT Act does not address this issue and asserted that there already is no doubt that if a financial institution delegates any of its operations to a third party, the institution will remain responsible for related regulatory compliance.

Other commenters stated that it should remain a contractual matter between the parties whether the service provider may implement a program that is different from its financial institution client.

Consumer groups asked the Agencies to ensure that the decision of a financial institution or creditor to outsource would not lead to lower Red Flag standards. These commenters suggested the final rules state that the Program must also meet the requirements that would apply if the activity were performed without the use of a service provider. They also suggested the final rules clarify that, in addition to any responsibility on the service provider imposed by law, regulation, or contract, the financial institution or creditor would be responsible for a failure to comply with the Program.

Most commenters, however, agreed with the proposal and stated that a service provider must have the flexibility to meet the objectives of the rules without having to tailor its services to the Program requirements of each company for which it provides

[34] A board approval requirement is also found in the BSA rules of the Federal banking agencies and the NCUA. *See* 12 CFR 21.21; (OCC); 12 CFR 208.63 (Board); 12 CFR 326.8 (FDIC); 12 CFR 563.177 (OTS); and 12 CFR 748.2 (NCUA). Thus, contrary to the assertion of some commenters, this rule is being treated in a manner similar to other rules.

service. These commenters noted that this proposed approach was the same as that used in the Information Security Standards.

The Agencies believe it is important to retain a provision in the final rules addressing service providers to remind financial institutions and creditors that they continue to remain responsible for compliance with the final rules, even if they outsource operations to a third party. However, the Agencies have simplified the service provider provision in the final rules and moved the remaining parts of proposed §__.90(d)(4) to the guidelines.

Section __.90(e)(4) of the final rules provides that a covered entity must exercise appropriate and effective oversight of service provider arrangements, without further elaboration. This provision provides maximum flexibility to financial institutions and creditors in managing their service provider arrangements, while making clear that a covered entity cannot escape its obligations to comply with the final rules and to include in its Program those guidelines that are appropriate by simply outsourcing an activity.

Section VI(c) of the guidelines provides that, whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Thus, the guidelines make clear that a service provider that provides services to multiple financial institutions and creditors may do so in accordance with its own program to prevent identity theft, as long as the program meets the requirements of the regulations. The guidelines also provide an example of how a covered entity may comply with this provision. The guidelines state that a financial institution or creditor could require the service provider, by contract, to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities and either report the Red Flags to the financial institution or creditor or take appropriate steps to prevent or mitigate identity theft.

Section __.90(f) Consideration of Guidelines in Appendix J

The Agencies have added a provision to the final rules that explains the relationship of the rules to the guidelines. Section __.90(f) states that each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J and include in its Program those guidelines that are appropriate.

Each of the guidelines corresponds to a provision of the final rules. As mentioned earlier, the guidelines were issued to assist financial institutions and creditors in the development and implementation of a Program that satisfies the requirements of the final rules. The guidelines provide policies and procedures that financial institutions and creditors should use, where appropriate, to satisfy the regulatory requirements of the final rules. While an institution or a creditor may determine that a particular guideline is not appropriate for its circumstances, it nonetheless must ensure its Program contains reasonable policies and procedures to fulfill the requirements of the final rules. This approach provides financial institutions and creditors with the flexibility to determine "how best to develop and implement the required policies and procedures." [35]

Supplement A to Appendix J: Examples of Red Flags

Section 114 of the FACT Act states that, in developing the guidelines, the Agencies must identify patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. The Agencies proposed implementing this provision by requiring the Program of a financial institution or creditor to include policies and procedures for the identification and detection of Red Flags in connection with an account opening or an existing account, including from among those listed in Appendix J.

The Agencies compiled the Red Flags enumerated in Appendix J from a variety of sources, such as literature on the topic, information from credit bureaus, financial institutions, creditors, designers of fraud detection software, and the Agencies' own experiences. The preamble to the proposed rules stated that some of the Red Flags, by themselves, may be reliable indicators of identity theft, while others are more reliable when detected in combination with other Red Flags.

The preamble to the proposed rules explained that the Agencies recognized that a wide range of financial institutions and creditors, and a broad variety of accounts would be covered by the regulations. Therefore, the Agencies proposed to afford each financial institution and creditor flexibility to determine which Red Flags were relevant for their purposes to detect identity theft, including from among those listed in Appendix J.

As mentioned previously, consumer groups criticized the discretion in the proposal that permitted financial institutions and creditors to choose Red Flags relevant to detecting the risk of identity theft based upon the list of enumerated factors. These groups urged the Agencies to make certain Red Flags in Appendix J mandatory. In addition, consumer groups suggested a number of additional Red Flags for inclusion in Appendix J.

Some commenters agreed that the list of examples of Red Flags was appropriate because, in their view, it was designed to be flexible. Some industry commenters, including a number of small financial institutions, stated that the Red Flags set forth in Appendix J would assist them in developing and improving their identity theft prevention programs. Other commenters suggested deleting the list of Red Flags or modifying the list in a manner appropriate to the nature of their own operations.

The Agencies have retained the list of examples of Red Flags because section 114 states that the Agencies "shall identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft." The Agencies also retained the list because some commenters indicated that having examples of Red Flags would be helpful to them. However, the examples of Red Flags are now set forth in a separate supplement to the guidelines. The list of examples is similar to that which the Agencies proposed, however, the Red Flags that the Agencies identified as precursors to identity theft have been deleted and are now addressed in section IV of the guidelines. Moreover, in response to a Congressional commenter, the Agencies added, as an example of a Red Flag, an application that gives the appearance of having been destroyed and reassembled.

The introductory language to the supplement clarifies that the enumerated Red Flags are examples. Thus, a financial institution or creditor may tailor the Red Flags it chooses for its Program to its own operations. A financial institution or creditor will not need to justify to an Agency its failure to include in the Program a specific Red Flag from the list of examples. However, a covered entity will have to account for the overall effectiveness of a Program that is appropriate to its size and

[35] *See* H.R. Rep. No. 108-263 at 43 (Sept. 4, 2003) (accompanying H.R. 2622); S. Rep. No. 108-166 at 13 (Oct. 17, 2003) (accompanying S. 1753).

complexity and the nature and scope of its activities.

Inactive Accounts

Section 114 also directs the Agencies to consider whether to include reasonable guidelines for notifying the consumer when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years, in order to reduce the likelihood of identity theft. The preamble to the proposed rules noted that the Agencies believed that the two-year limit was not always an accurate indicator of identity theft given the wide variety of credit and deposit accounts that would be covered by the provision. Therefore, in place of guidelines on inactive accounts, the Agencies proposed incorporating a Red Flag on inactive accounts into Appendix J that was flexible and was designed to take into consideration the type of account, the expected pattern of usage of the account, and any other relevant factors.

Some consumer groups suggested that a new section be added to the guidelines requiring notice to the consumer when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years unless this pattern would be expected for a particular type of account. Other commenters agreed with the Agencies' proposal to simply make activity on an inactive account a Red Flag. They also agreed that the Agencies should not use two years of inactivity as a hard and fast rule, and allow financial institutions and creditors to use their own standards to determine when an account is inactive.

In the final rules, the Agencies continue to list activity on an inactive account as a Red Flag. Given the variety of covered accounts to which the final rules and guidelines will apply, the Agencies concluded that the two-year period suggested in section 114 would not necessarily be a useful indicator of identity theft. Therefore, the Agencies have not included a provision in the guidelines regarding notification when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years.

B. Special Rules for Card Issuers

1. Background

Section 114 also requires the Agencies to prescribe joint regulations generally requiring credit and debit card issuers to assess the validity of change of address notifications. In particular, these regulations must ensure that if the card issuer receives a notice of change of address for an existing account and, within a short period of time (during at least the first 30 days), receives a request for an additional or replacement card for the same account, the issuer must follow reasonable policies and procedures to assess the validity of the change of address through one of three methods. The card issuer may not issue the card unless it: (1) Notifies the cardholder of the request at the cardholder's former address and provides the cardholder with a means to promptly report an incorrect address; (2) notifies the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder; or (3) uses other means of evaluating the validity of the address change in accordance with the reasonable policies and procedures established by the card issuer to comply with the joint regulations described earlier regarding identity theft.

For this reason, the Agencies also proposed special rules that required credit and debit card issuers to assess the validity of change of address notifications by notifying the cardholder or through certain other means. The proposed regulations stated that a financial institution or creditor that is a card issuer may incorporate the requirements of § __.91 into its Program.

As described in the section-by-section analysis that follows, commenters generally requested changes that would make the proposed rules more flexible.

2. Section-by-Section Analysis

Section __.91(a) Scope

The proposed rules stated that this section applies to a person, described in proposed § __.90(a), that issues a debit or credit card. The Agencies did not receive any comments on this section.

In the final rules, for clarity, the Agencies deleted the cross-reference to § __.90(a). Each Agency also revised its scope paragraph to list the entities over which it has jurisdiction that are subject to § __.91. Under the final rules, section __.91 applies to any debit or credit card issuer (card issuer) that is subject to an Agency's jurisdiction.

Section __.91(b) Definitions

The proposed rules included two definitions solely applicable to the special rules for card issuers: "cardholder" and "clear and conspicuous." Section __.91(b) of the final rules also contains these definitions as follows.

Section __.91(b)(1) Cardholder

Under section 114, the Agencies must prescribe regulations requiring a card issuer to follow reasonable policies and procedures to assess the validity of a change of address, before issuing an additional or replacement card. Section 114 provides that a card issuer may satisfy this requirement by notifying "the cardholder." The term "cardholder" is not defined in the FACT Act. The preamble to the proposed rules explained that the legislative record relating to this provision indicates that "issuers of credit cards and debit cards who receive a *consumer* request for an additional or replacement card for an existing account" may assess the validity of the request by notifying "the cardholder." [36] As the preamble noted, the request, presumably, will be valid if the consumer making the request and the cardholder are one and the same "consumer." Therefore, the proposal defined "cardholder" as a consumer who has been issued a credit or debit card. The preamble to the proposed rules also explained that, because "consumer" is defined in the FCRA as an "individual," [37] the proposed regulations applied to any request for an additional or replacement card by an individual, including a card for a business purpose, such as a corporate card.

Some commenters asked the Agencies to clarify that this definition does not apply to holders of stored value cards, such as payroll and gift cards, or to cards used to access a home equity line of credit. Another commenter urged that the final rules exclude credit and debit cards for a business purpose.

The final rules continue to define "cardholder" as a consumer who has been issued a credit or debit card. Both "credit card" and "debit card" are defined in section 603(r) of the FCRA. [38] The definition of "credit card" is defined by cross-reference to section 103 of the Truth in Lending Act, 15 U.S.C. 1601, *et seq.* [39] The definition of "debit card" is any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution for the purposes of transferring money between accounts or obtaining money, property, labor, or services. [40]

Section 603(r) of the FCRA provides that "account" and "electronic fund transfer" have the same meaning as those terms have in the Electronic Funds Transfer Act (EFTA), 15 U.S.C.

[36] *See* 149 Cong. Rec. E2513 (daily ed. December 8, 2003) (statement of Rep. Oxley) (emphasis added).

[37] 15 U.S.C. 1681a(c).

[38] 15 U.S.C. 1681a.

[39] *See* 15 U.S.C. 1681a(r)(2).

[40] 15 U.S.C. 1681a(r)(3).

1693, *et seq.* The EFTA, and Regulation E, 12 CFR part 205, govern electronic fund transfers. In contrast to section 603(r) of the FCRA, neither the EFTA nor Regulation E defines the term "debit card." Instead, coverage under the EFTA and Regulation E depends upon whether electronic fund transfers can be made to or from an "account," meaning a checking, savings, or other consumer asset account established primarily for personal, family or household purposes. The Board recently issued a final rule expanding the definition of "account" under Regulation E to cover payroll card accounts.[41] Therefore, a holder of a payroll card is a "cardholder" for purposes of § __.91(b)(1), provided that the card issuer is a "financial institution" as defined in section 603(t) of the FCRA.

The Board decided not to cover other types of prepaid cards as accounts under Regulation E at the time it issued the payroll card rule. Therefore, the definition of "cardholder" does not include the holder of a gift card or other prepaid card product, unless and until the Board elects to cover such cards as accounts under Regulation E.

The definition of "cardholder" would also include a recipient of a home equity loan if the holder is able to access the proceeds of the loan with a credit or debit card within the meaning of 15 U.S.C. 1681a(r).

Identity theft may occur in connection with a card that a consumer uses for a business purpose and may affect the consumer's personal credit standing. Additionally, the definition of "consumer" under the FCRA is simply an "individual."[42] For this reason, the Agencies continue to believe that the protections of this provision must extend to consumers who hold a card for a personal, household, family or business purpose.

Section __.91(b)(2) Clear and conspicuous

The second proposed definition was for the phrase "clear and conspicuous." Proposed § __.91 included a provision that required any written or electronic notice provided by a card issuer to the consumer pursuant to the regulations to be given in a "clear and conspicuous manner." The proposed regulations defined "clear and conspicuous" based on the definition of this phrase found in the Agencies' privacy rules.

The Agencies received no comments on the phrase "clear and conspicuous," and have adopted the definition as proposed in § __.91(b)(2).

Sections __.91(c) and (d) Address Validation

Proposed § __.91(c) simply restated the statutory requirements described above with some minor stylistic changes. A number of commenters noted that the requirements of this section would be difficult and expensive to implement. They stated that millions of address changes are processed every year, though very few turn out to be fraudulent.

By contrast, consumer groups suggested that the final regulations should require the card issuer to notify the consumer of a request for an address change followed by the request for an additional or replacement card, unless there are special circumstances that prevent doing so in a timely manner.

Many commenters recommended that the final rules provide credit and debit card issuers with greater flexibility to verify address changes. For example, they stated it is not clear that an address change linked with a request for an additional card is a significant indicator of identity theft. Therefore, they recommended the rules (1) specifically permit card issuers to satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card; or (2) verify the address whenever a request for an additional or replacement card is made, whether or not the card issuer receives notification of an address change.

One commenter suggested that the rules should only apply to card issuers that receive direct notification of an address change rather than an address change notification from the U.S. Postal Service. The commenter asserted that there is a higher risk of fraud with a direct request for a change of address.

Consumer groups also recommended that the Agencies set a period longer than the 30-day minimum for card issuers to be on alert after an address change request. These commenters recommended that, because of billing cycles and the time it takes to issue a new card, an issuer should be required to assess the validity of an address change if it receives a request for an additional or replacement card within at least 90 days after the request for the address change.

Some commenters asked the Agencies to clarify what "other means" would be acceptable in assessing the validity of a change in address. One commenter stated that it is not cost effective to contact the customer, therefore, most card issuers would use "other means" of assessing the validity of the change of address in accordance with the policies and procedures the card issuer establishes pursuant to § __.90.

Commenters also asked the Agencies to clarify that the obligation to assess the validity of a request for an address change is not triggered unless the card issuer actually changes the cardholder's address.

Some commenters asked the Agencies to clarify whether electronic notices would be acceptable if the cardholder had previously contracted for electronic communications. Consumer groups recommended electronic notification be permitted only when the consumer consents in accordance with the E-Sign Act.

The Agencies note that the statutory provision being implemented here is quite specific. Congress mandated that the requirements set forth in section 615(e)(1)(C) of the FCRA apply to notifications of changes of address, which would necessarily include both those received directly from consumers and those received from the Postal Service. Congress also statutorily provided various methods to card issuers for assessing the validity of a change of address.[43] Accordingly, the final rules reflect these methods.

Under § __.91(c) of the final rules, a card issuer that receives an address change notification and, within at least 30 days, a request for an additional or replacement card, may not issue an additional or replacement card *until* it has notified the cardholder or has otherwise assessed the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § __.90. The Agencies have concluded that card issuers should be granted additional flexibility. Therefore, § __.91(d) clarifies that a card issuer may satisfy the requirements of § __.91(c) by validating an address, according to the methods set forth in § __.91(c)(1) or (2), when it receives an address change notification, before it receives a request for an additional or replacement card. The rules do not require a card issuer that issues an additional or replacement card to validate an address whenever it receives a request for such a card, because section 114 only requires the validation of an address when the card issuer also has received a notification of a change of address.

[41] *See* 71 FR 51,437 (August 10, 2006).

[42] 15 U.S.C. 1681a(c).

[43] *See* S. Rep. No. 108–166 at 14 (October 17, 2003)(accompanying S. 1753)(stating that a card issuer may rely on authentication procedures that do not involve a separate communication with the cardholder so long as the issuer has reasonably assessed the validity of the address change.)

The Agencies also revised § __.91 to clarify that a card issuer must provide to the cardholder a "reasonable" means of promptly reporting incorrect address changes whenever the card issuer notifies the cardholder of the request for an additional or replacement card.[44]

The Agencies declined to adopt the recommendation that an issuer assess the validity of an address change if it receives a request for an additional or replacement card within "at least 90 days" after an address change notification, as "at least 30 days" may be a reasonable period of time in some cases. However, a card issuer that does not validate an address when it receives an address change notification may find it prudent to validate the address before issuing an additional or replacement card, even when it receives a request for such a card more than 30 days after the notification of address change. In sum, the Agencies expect card issuers to exercise diligence commensurate with their own experiences with identity theft.

The Agencies also confirm that a card issuer is not obligated to assess the validity of a notification of an address change after receiving a request for an additional or replacement card if it previously determined not to change the cardholder's address because the address change request was fraudulent.[45]

Section __.91(e) Form of Notice

In the preamble to the proposed rules, the Agencies noted that Congress had singled out this scenario involving card issuers and placed it in section 114 because it is perceived to be a possible indicator of identity theft. To highlight the important and urgent nature of notice that a consumer receives from a card issuer pursuant to § __.91(c), the Agencies also proposed requiring that any written or electronic notice that a card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder. The preamble to the proposed rules stated that a card issuer could also provide notice orally, in accordance with the policies and procedures the card issuer has established.

A few commenters recommended that this proposed requirement apply only if the issuer notifies the cardholder of the change of address request at the cardholder's former address. These commenters stated that, otherwise, the provision would prohibit other types of notices, such as those in periodic statements. Another commenter stated that this provision was not necessary because card issuers would send such notices separately in any event.

The Agencies are not convinced that such a notice would be provided separately from a card issuer's regular correspondence with the cardholder unless required. Moreover, the Agencies do not agree that this requirement should apply only if a card issuer chooses to notify the cardholder of the change of address request at the cardholder's former address in accordance with § __.91(c)(1). Even where the card issuer and cardholder agree to some other means for notice, this alternative means does not change the important nature of the notice. Therefore, § __.91(c) of the final rules provides that any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous, and provided separately from its regular correspondence with the cardholder.

III. Section 315 of the FACT Act

A. Background

Section 315 of the FACT Act amends section 605 of the FCRA, 15 U.S.C. 1681c, by adding a new subsection (h). Section 605(h)(1) requires that, when providing a consumer report to a person that requests the report (the user), a nationwide consumer reporting agency, as defined in section 603(p) of the FCRA, (CRA) must provide a notice of the existence of a discrepancy if the address provided by the user in its request "substantially differs" from the address the CRA has in the consumer's file.

Section 605(h)(2) requires the Agencies to issue joint regulations that provide guidance regarding reasonable policies and procedures a user of a consumer report should employ when the user receives a notice of address discrepancy. These regulations must describe reasonable policies and procedures for a user of a consumer report to employ to (i) enable it to form a reasonable belief that the user knows the identity of the person for whom it has obtained a consumer report, and (ii) reconcile the address of the consumer with the CRA, if the user establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the CRA.

B. Section-by-Section Analysis

Section __.82(a) Scope

Proposed § __.82(a) noted that the scope of section 315 differs from the scope of section 114 and explained that section 315 applies to "users of consumer reports" and "persons requesting consumer reports" (hereinafter referred to as "users"), as opposed to financial institutions and creditors. Therefore, section 315 does not apply to a financial institution or creditor that does not use consumer reports. The Agencies did not receive any comments on this section and have adopted it as proposed in the final rules.

Section __.82(b) Definition

Proposed § __.82(b) defined "notice of address discrepancy" as "a notice sent to a user of a consumer report by a CRA pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer provided by the user in requesting the consumer report and the address or addresses the CRA has in the consumer's file."[46]

In the preamble to the proposed rules, the Agencies noted that section 605(h)(1) requiring CRAs to provide notices of address discrepancy became effective on December 1, 2004. To the extent CRAs each have developed their own standards for delivery of notices of address discrepancy, the proposal noted that it is important for users to be able to recognize and receive notices of address discrepancy, especially if they are being delivered electronically by CRAs. For example, CRAs may provide consumer reports with some type of a code to indicate an address discrepancy. Users must be prepared to recognize the code as an indication of an address discrepancy.

While some commenters agreed with the proposed definition, a number of commenters suggested that the Agencies clarify that only a "substantial" discrepancy would trigger the requirements in this provision and that obvious errors would not. Some commenters also suggested that the Agencies provide examples of what constitutes a "substantial difference." One commenter stated that users should be able to determine when there is a substantial difference.

[44] *See* S. Rep. No. 108–166 at 14 (October 17, 2003) (accompanying S. 1753) (stating that a means of reporting an incorrect change could be through the mail, by telephone, or electronically.)

[45] This position is consistent with the legislative history of this section. *See* S. Rep. No. 108–166 at 14 (Oct. 17, 2003) (accompanying S. 1753) (stating that it would not be necessary for the card issuer to take these steps "if, despite receiving a request for an address change, the issuer did not actually change the cardholder's address for any reason (e.g., the card issuer had previously determined that the request for an address change was invalid)").

[46] All other terms used in this section have the same meanings as set forth in the FCRA (15 U.S.C. 1681a).

As noted earlier, section 605(h)(1) requires a CRA to send a notice of address discrepancy when it determines that the address provided to the CRA by a user "substantially differs" from the address the CRA has in the consumer's file. The phrase "substantially differs" is not defined in the statute. Instead, the statute allows each CRA to construe this phrase as it chooses and, accordingly, to set the standard it will use to determine when it will send a notice of address discrepancy.

As required by section 605(h)(2), this rulemaking focuses on the obligations of users that receive a notice of address discrepancy from a CRA. The statute does not indicate that the Agencies are to define the phrase "substantially differs" for CRAs or to permit users to define that phrase themselves. Therefore, the final rules adopt the proposed definition of "notice of address discrepancy" without change.

Section __.82(c) Requirement to form a reasonable belief

Proposed § __.82(c) implemented the requirement in section 605(h)(2)(B)(i) that the Agencies prescribe regulations describing reasonable policies and procedures to enable the user to form a reasonable belief that the user knows "the identity of the person to whom the consumer report pertains" when the user receives a notice of address discrepancy. Proposed § __.82(c) stated that a user must develop and implement reasonable policies and procedures for "verifying the identity of the consumer for whom it has obtained a consumer report" whenever it receives a notice of address discrepancy. The proposal stated further that these policies and procedures must be designed to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report, or determine that it cannot do so.

A number of commenters stated that the statutory requirement that a user form a reasonable belief that it knows the identity of the consumer for whom it obtained a consumer report should only apply in situations where the user establishes a continuing relationship with the consumer.

A consumer group suggested that the language in the proposed regulation permitting a user to determine that it cannot form a reasonable belief of the identity of the consumer should be deleted because the statute specifically requires a reasonable belief to be formed. This commenter stated that the purpose of the statute was to reduce the number of new accounts opened using false addresses, and that permitting a user to satisfy its obligations under the regulations by simply determining it cannot form a reasonable belief would allow the user to open an account, effectively rendering the statute meaningless.

The purpose of section 315 is to enhance the accuracy of consumer information, specifically to ensure that the user has obtained the correct consumer report for the consumer about whom it has requested such a report. To implement this concept more clearly, § __.82(c) of the final rules provides that a user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when the user receives a notice of address discrepancy.[47]

The Agencies do not agree with commenters who suggested that the proposed provision should apply only in connection with the establishment of a continuing relationship with a consumer, in other words, when a user is opening a new account. The statutory requirement in section 605(h)(2)(B)(i) that a user form a reasonable belief that it knows the identity of the consumer for whom it obtained a consumer report applies whether or not the user subsequently establishes a continuing relationship with the consumer. This is in contrast to the additional statutory requirement in section 605(h)(2)(B)(ii) that a user reconcile the address of the consumer with the CRA, only when the user establishes a continuing relationship with the consumer.

In addition, a user may receive a notice of address discrepancy with a consumer report, both in connection with the opening of an account and in other circumstances when the user already has a relationship with the consumer, such as when the consumer applies for an increased credit line. The Agencies believe it is important for a user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report in both of these cases. Accordingly, the final rules do not limit this provision solely to the establishment of new accounts.

Proposed § __.82(c) also provided that if a user employs the policies and procedures regarding identification and verification set forth in the CIP rules,[48] it would satisfy the requirement to have policies and procedures to verify the identity of the consumer. This provision took into consideration the fact that many users already may be subject to the CIP rules, and have in place procedures to comply with those rules, at least with respect to the opening of accounts. Thus, a user could rely upon its existing CIP policies and procedures to satisfy this requirement, so long as it applied them in all situations where it receives a notice of address discrepancy. The proposal also stated that any user, such as a landlord or employer, may adopt the CIP rules and apply them in all situations where it receives a notice of address discrepancy to meet this requirement, even if it is not subject to a CIP rule.

The Agencies requested comment on whether the CIP procedures would be sufficient to enable a user that receives a notice of address discrepancy with a consumer report to form a reasonable belief that it knows the identity of the consumer for whom it obtained the report, both in connection with the opening of an account, as well as in other circumstances where a user obtains a consumer report, such as when a user requests a consumer report to determine whether to increase the consumer's credit line, or in the case of a landlord or employer, to determine a consumer's eligibility to rent housing or for employment.

Many commenters supported the use of CIP to satisfy this requirement. Some commenters, however, asked the Agencies to clarify that once a consumer's identity was verified using CIP, it would not be necessary to re-verify that consumer's identity under this provision.

Some commenters found the proposal's preamble language confusing. These commenters did not understand why a user would need to use its CIP policies in every situation where a notice of address discrepancy was received in order to comply with this requirement; they felt that it might be possible to form a reasonable belief without using CIP in some circumstances.

Other commenters noted that the CIP rules, which were issued for different purposes, are not the appropriate standard for investigating a consumer's identity after a notice of address discrepancy because those rules permit verification of an address to occur after an account is opened and do not require contacting the consumer. One commenter stated that it was not clear whether a user relying on the CIP rules to satisfy the obligations under the regulation must comply with some or all of the requirements in the CIP rules,

[47] The Agencies acknowledge that an address discrepancy also may be an indicator of identity theft. To address this problem, the Agencies included address discrepancies as an example of a Red Flag in connection with the Identity Theft Red Flag regulations.

[48] See, *e.g.*, 31 CFR 103.121(b)(2)(i) and (ii).

including those that require policies and procedures to address circumstances when a user cannot form a reasonable belief it knows the identity of the consumer.

The Agencies believe that comparing information provided by a CRA to information the user obtains and uses (or has obtained and used) to verify a consumer's identity pursuant to the requirements set forth in the CIP rules is an appropriate way to satisfy this obligation, particularly in connection with the opening of a new account. However, when a user receives a notice of address discrepancy in connection with an existing account, after already having identified and verified the consumer in accordance with the CIP rules, the Agencies would not expect a user to employ the CIP procedures again. To address this issue and provide users with flexibility, § __.82(c) of the final rule provides examples of reasonable policies and procedures that a user may employ to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. These examples include comparing information provided by the CRA with information the user: (1) Obtains and uses to verify the consumer's identity in accordance with the requirements of the CIP rules; (2) maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or (3) obtains from third-party sources. Another example is to verify the information in the consumer report provided by the CRA with the consumer.

If a user cannot establish a reasonable belief that the consumer report relates to the consumer about whom it has requested the report, the Agencies expect the user will not use that report. While section 605(h)(2)(B)(i) is silent on this point, other laws may be applicable in such a situation. For example, in the case of account openings, a user that is subject to the CIP rules generally will need to document how it has resolved the discrepancy between the address provided by the consumer and the address in the consumer report.[49] If the user cannot establish a reasonable belief that it knows the true identity of the consumer, it will need to implement the policies and procedures for addressing these circumstances as required by the CIP rules, which may involve not opening an account or closing an account.[50] If a user is a "financial institution" or "creditor" as defined by the FCRA, a notice of address discrepancy may be a Red Flag and require an appropriate response to prevent and mitigate identity theft under the user's Identity Theft Prevention Program.

Section __.82(d)(1) Requirement To Furnish Consumer's Address to a Consumer Reporting Agency

Proposed § __.82(d)(1) provided that a user must develop and implement reasonable policies and procedures for furnishing to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the following three conditions are satisfied. The first condition, in proposed § __.82(d)(1)(i), was that the user must be able to form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained. This condition would have ensured the user would furnish a new address for the consumer to the CRA only after the user had formed a reasonable belief that it knew the identity of the consumer, using the policies and procedures set forth in paragraph § __.82(c).

The second condition, in proposed § __.82(d)(1)(ii), was that the user furnish the address to the CRA if it establishes or maintains a continuing relationship with the consumer. Section 315 specifically requires that the user furnish the consumer's address to the CRA if the user *establishes* a continuing relationship with the consumer. Therefore, proposed § __.82(d)(1)(ii) reiterated this requirement. However, because a user also may obtain a notice of address discrepancy in connection with a consumer with whom it already has an existing relationship, the proposal also provided that the user must furnish the consumer's address to the CRA from whom the user has received a notice of address discrepancy when the user maintains a continuing relationship with the consumer.

Finally, the third condition, in proposed § _.82(d)(1)(iii), provided that if the user regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained, the consumer's address must be communicated to the CRA as part of the information the user regularly provides.

A majority of commenters recommended that the requirement to furnish a confirmed address should not apply to existing accounts. These commenters maintained that such a requirement would exceed the scope of the statute. They also noted that users often do not obtain full consumer reports for existing customers—just credit scores. These commenters noted that limited reports often do not contain an address for a customer. Some commenters also felt existing relationships should be excluded because users already would have verified a consumer's address at the time of account opening.

The Agencies have modified this section as follows. The final rules continue to provide that a user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the CRA when three conditions are present. The first condition, in § _.82(d)(1)(i), has been revised to be consistent with the earlier changes in section § _.82(c) that focus more narrowly on accuracy and require that a user form a reasonable belief that a consumer report relates to the consumer about whom it requested the report. The second condition, in § _.82(d)(1)(ii), now applies only to new accounts and states that a confirmed address must be furnished if the user "establishes" a continuing relationship with the consumer. The reference to "or maintains" a continuing relationship has been deleted. The Agencies agree with commenters that section 605(h)(2)(B)(ii) does not require the reporting of a confirmed address to a CRA in connection with existing relationships. The Agencies have concluded that users are more likely than a CRA to have an accurate address for an existing customer and, therefore, should not be required by these rules to take additional steps to confirm the accuracy of the customer's address. Users already have an ongoing duty to correct and update information for their existing customers under section 623 of the FCRA, 15 U.S.C. 1681s–2. Accordingly, under the final rules, the obligation to furnish a confirmed address for the consumer to the CRA is applicable only to new relationships. The third condition, in § _.82(d)(1)(iii), has been adopted in the final rule without substantive change.

Section __.82(d)(2) Requirement To Confirm Consumer's Address

In the preamble to the proposal, the Agencies noted that section 315 requires them to prescribe regulations describing reasonable policies and procedures for a user "to reconcile the address of the consumer" about whom it has obtained a notice of address discrepancy with the CRA "by furnishing *such* address" to the CRA. (Emphasis added.) The

[49] *See, e.g.*, 31 CFR 103.121(b)(3)(i)(D).

[50] *See, e.g.*, 31 CFR 103.121(b)(2)(iii).

Agencies noted that, even when the user is able to form a reasonable belief that it knows the identity of the consumer, there may be many reasons the initial address furnished by the consumer is incorrect. For example, a consumer may have provided the address of a secondary residence or inadvertently reversed a street number. To ensure that the address furnished to the CRA is accurate, the Agencies proposed to interpret the phrase, "such address," as an address the user has reasonably confirmed is accurate. This interpretation would have required a user to take steps to "reconcile" the address it initially received from the consumer when it receives a notice of address discrepancy, rather than simply furnishing the initial address it received from the consumer to the CRA. Proposed § __.82(d)(2) contained the following list of illustrative measures that a user may employ to reasonably confirm the accuracy of the consumer's address:

- Verifying the address with the person to whom the consumer report pertains;
- Reviewing its own records of the address provided to request the consumer report;
- Verifying the address through third-party sources; or
- Using other reasonable means.

The Agencies solicited comment on whether these examples were necessary, or whether different or additional examples should be listed.

A number of commenters stated that requiring a user to confirm the address furnished exceeded the scope of the statute. They asserted that the benefit of improvements in the accuracy of addresses and the prevention of identity theft would not outweigh the additional burden of this requirement. A few commenters noted that complying with the CIP rules should be sufficient to verify the address. Commenters also felt that users should have the flexibility to establish their own validation processes based on risk.

As stated earlier, the Agencies believe the purpose of the statute is to enhance the accuracy of information relating to consumers by requiring the user to furnish an address that the user has reasonably confirmed is accurate.[51] Simply providing the CRA with the initial address supplied to the user by the consumer, and which caused the CRA to send a notice of address discrepancy, would not serve this purpose. The Agencies believe the options for confirmation listed in the regulation provide sufficient flexibility for users to confirm consumers' addresses. For this reason, they have been adopted in the final rule as proposed, with minor technical changes. Section __.82(d)(2)(i) has been revised to conform the language with § __.82(c). Section __.82(d)(2)(ii) has been revised to emphasize the verification of the consumer's address rather than the review of the user's records to determine whether the address given by the consumer is the same.

Section __.82(d)(3) Timing

Section 315 specifies when a user must furnish the consumer's address to the CRA. It states that this information must be furnished for the reporting period in which the user's relationship with the consumer is established. Accordingly, proposed § __.82(d)(3)(i) stated that, with respect to new relationships, the policies and procedures a user develops in accordance with § __.82(d)(1) must provide that a user will furnish the consumer's address that it has reasonably confirmed to the CRA as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

The proposed rule also addressed other situations when a user may receive a notice of address discrepancy. Proposed § __.82(d)(3)(ii) stated that in other circumstances, such as when the user already has an existing relationship with the consumer, the user should furnish this information for the reporting period in which the user has reasonably confirmed the accuracy of the address of the consumer for whom it has obtained a consumer report.

The Agencies also noted that, in order to satisfy the requirements of both § __.82(d)(1) and § __.82(d)(3)(i), a user employing the CIP rules would have to establish a continuing relationship and verify the identity of the consumer during the same reporting period.

The Agencies recognized the timing provision for newly established relationships could be problematic for users hoping to take full advantage of the flexibility in timing for verification of identity afforded by the CIP rules. As required by statute, proposed § __.82(d)(3)(i) stated that the reconciled address must be furnished for the reporting period in which the user establishes a relationship with the consumer. Proposed § __.82(d)(1), which also mirrored the requirement of the statute, required the reconciled address to be furnished to the CRA only when the user both establishes a continuing relationship with the consumer and forms a reasonable belief that it knows the identity of the consumer to whom the consumer report relates. Typically, the CIP rules permit an account to be opened (*i.e.*, relationship to be established) if certain identifying information is provided. Verification to establish the true identity of the customer is required within a reasonable period of time *after* the account has been opened. As explained in the preamble to the proposed rules, to satisfy the requirements of both § __.82(d)(1) and § __.82(d)(3)(i), a user employing the CIP rules would have to verify the identity of the consumer using the identifying information it obtained in accordance with the CIP rules within the same reporting period that the user opens the account and establishes a continuing relationship with the consumer.

The Agencies requested comment on whether the timing for responding to notices of address discrepancy received in connection with newly established relationships and in connection with circumstances other than newly established relationships is appropriate. One commenter objected to the requirement that a user employing the CIP rules would have to both establish a continuing relationship and a reasonable belief that it knows the consumer's identity during the same reporting period. A few commenters noted that the timing for reporting should simply be "reasonable," such as the next reporting cycle.

Because the Agencies have determined that the requirement to furnish a confirmed address will apply only to newly established accounts, the Agencies have revised § __.82(d)(3) to remove the references to the timing for furnishing reports in connection with other accounts, contained in the proposal. The final rules reflect the language in section 605(h)(2)(B)(ii), and state that a user's policies and procedures must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

A timing issue still exists for a user that chooses to compare the information in the consumer report with information that the user obtains and uses to verify the consumer's identity in accordance with the CIP rules for the purpose of forming a reasonable belief that a consumer report relates to the consumer

[51] This requirement is consistent with the legislative history which provides that this section is intended to obligate the user to utilize reasonable policies and procedures to resolve discrepancies. *See* H.R. Rep No. 108-263 at 46 (Sept. 4, 2003) (accompanying H.R. 2622).

about whom it has requested the report. However, the Agencies believe that the benefits of being able to use CIP for this purpose should outweigh any additional burden of having to establish a reasonable belief that a consumer report relates to the consumer about whom it has requested the report within the same reporting period that the user opens the account and establishes a continuing relationship with the consumer.

IV. General Provisions

The OCC, the Board, the FDIC, the OTS, and the NCUA [52] proposed to amend the first sentence in § __.3, which contains the definitions that are applicable throughout this part. This sentence stated that the list of definitions in § __.3 apply throughout the part "unless the context requires otherwise." These agencies proposed to amend this introductory sentence to make clear that the definitions in § __.3 apply "for purposes of this part, unless explicitly stated otherwise." Thus, these definitions apply throughout the part unless defined differently in an individual subpart. There were no comments on this proposal, and the change to § __.3 is adopted as proposed.

OTS proposed nonsubstantive, technical changes to its rule sections on purpose and scope (§ 571.1) and disposal of consumer information (§ 571.83). OTS explained that these changes were necessary in light of the proposed incorporation of the address discrepancy section into subpart I. There were no comments on these proposed changes and they are adopted substantially as proposed. Further, since these changes render the definition of "you" in § 571.3(o) superfluous, OTS is removing that definition.

The OCC's final rules add a purpose section at § 41.1. The final rules are simply restoring the purpose section of part 41 that was inadvertently deleted when "subpart D-Medical Information" was added to this part.

V. Effective Date

The Agencies received a number of comments regarding the effective date of the final regulations and guidelines, although the proposed rulemaking did not address this issue. While consumer groups recommended that the effective date for compliance with the regulations be the minimum time allowed by law, many financial institutions and creditors requested the time for compliance be extended from between 12 to 24 months from issuance of the final rules. These commenters felt they needed time to take an inventory of their existing systems and develop new programs necessary for compliance. Some commenters noted that they likely would use technological solutions to comply with the rules and that it is necessary to schedule such projects well in advance. Commenters also noted that compliance with the final rules may require systemic and operational changes across business lines and could affect relationships with vendors and third party service providers that would require time to change.

Neither section 114 nor section 315 of the FACT Act specifically addresses the effective date of the regulations issued pursuant to these sections. Under the Administrative Procedure Act (APA), 5 U.S.C. 553(d), agencies must generally publish a substantive rule not less than 30 days before its effective date. In addition, under section 302 of the Riegle Community Development and Regulatory Improvement Act of 1994 (CDRIA),[53] rules issued by the Federal banking agencies that impose additional reporting, disclosure, or other new requirements on financial institutions generally will take effect on the first day of a calendar quarter that begins on or after the date on which the regulations are published in the **Federal Register**. Because these final rules are substantive and impose additional requirements on financial institutions, the Agencies have provided for an effective date of [January 1, 2008], consistent with the APA and CDRIA.

At the same time, the Agencies have determined that it is appropriate to provide all covered entities with a delayed compliance date of November 1, 2008, to comply with the requirements of the final rulemaking. Some financial institutions and creditors already employ a variety of measures that satisfy the requirements of the final rulemaking because these are usual and customary business practices to minimize losses due to fraud, or as a result of already complying with other existing regulations and guidance that relate to information security, authentication, identity theft, and response programs. However, the Agencies recognize that these entities may still need time to evaluate their existing programs, and to integrate appropriate elements from them into the Program and into the other policies and procedures required by this final rulemaking. Further, the Agencies recognize that some covered entities have not previously been subject to any related regulations or guidance, and thus may need more time to implement the final rules and guidelines. Therefore, the Agencies are providing covered entities with a transition period to comply with the requirements contained in the final rulemaking.

VI. Regulatory Analysis

A. Paperwork Reduction Act

In accordance with the requirements of the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*, 5 CFR part 1320 Appendix A.1), the Agencies have reviewed the final rulemaking and determined that it contains collections of information subject to the PRA. The Board made this determination under authority delegated to the Board by the Office of Management and Budget (OMB). The information collection requirements in the final rulemaking may be found in 12 CFR 41.82, 41.90, 41.91, 222.82, 222.90, 222.91, 334.82, 334.90, 334.91, 571.82, 571.90, 571.91, 717.82, 717.90; and 717.91; and 16 CFR 681.1, 681.2, and 681.3.

An agency may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid OMB control number. The information collection requirements contained in this joint final rule were submitted by the OCC, FDIC, OTS, NCUA, and FTC to OMB for review and approval under the Paperwork Reduction Act of 1995. OMB assigned the following control numbers to the collections of information: OMB Control Nos. 1557–0237 (OCC), 3064–0152 (FDIC), 1550–0113 (OTS), 3133–0175 (NCUA), and 3084–0137 (FTC). The Board's OMB Control No. is 7100–0308.[54]

Description of the Collection

Section 114: The proposed rules implementing section 114 required each financial institution and creditor to (1) create an Identity Theft Prevention Program (Program); (2) report to the board of directors, a committee thereof or senior management, at least annually, on compliance with the proposed regulations; and (3) train staff to implement the Program.

In addition, the proposed rules required each credit and debit card issuer (card issuer) to establish policies and procedures to (1) assess the validity

[52] The equivalent language for the FTC already exists in 16 CFR 603.1.

[53] Pub. L. 103–325; 12 U.S.C. § 4802(b).

[54] The information collections (ICs) in this rule will be incorporated with the Board's Disclosure Requirements Associated with Regulation V (OMB No. 7100–0308). The burden estimates provided in this rule pertain only to the ICs associated with this final rulemaking. The current OMB inventory for Regulation V is available at: *http://www.reginfo.gov/public/do/PRAMain.*

of a change of address notification before honoring a request for an additional or replacement card received during at least the first 30 days after it receives the notification; and (2) notify the cardholder in writing, electronically, or orally, or use another means of assessing the validity of the change of address.

Section 315: The proposed rules implementing section 315 required each user of consumer reports to (1) develop reasonable policies and procedures it would employ when it receives a notice of address discrepancy from a CRA; and (2) to furnish an address the user reasonably confirmed is accurate to the CRA from which it receives a notice of address discrepancy.

The information collections in the final rulemaking are the same as those in the proposal.

Comments Received

The Agencies sought comment on the burden estimates for the information collections described in the proposal. The Agencies received approximately 129 comments on the proposed rulemaking. Most commenters maintained that proposal would impose additional regulatory burden and asserted that the estimates of the cost of compliance should be considerably higher than the Agencies projected. A few of these commenters specifically addressed PRA burden, however, they did not provide specific estimates of additional burden hours that would result from the proposal. Some of these commenters stated that staff training estimates were significantly underestimated. Other commenters stated that the costs of compliance failed to consider the cost to third-party service providers that the commenters characterized as being required to implement the Program.

Explanation of Burden Estimates Under the Final Rulemaking

The Agencies believe that many of the comments received regarding burden stemmed from commenters' misreading of the requirements of the proposed rulemaking. The final rulemaking clarifies these requirements, including those that relate to the information collections. It also differs from the proposal as described below.

The Agencies continue to believe that most covered entities already employ a variety of measures to detect and address identity theft that are required by section 114 of the final rulemaking because these are usual and customary business practices that they employ to minimize losses due to fraud. In addition, the Agencies believe that many financial institutions and creditors already have implemented some of the requirements of the final rules implementing section 114 as a result of having to comply with other existing regulations and guidance, such as the CIP regulations implementing section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l) that require verification of the identity of persons opening new accounts),[55] the Information Security Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801, and section 216 of the FACT Act, 15 U.S.C. 1681w,[56] and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs.[57] The final rulemaking underscores the ability of a financial institution or creditor to incorporate into its Program its existing processes that control reasonably foreseeable risks to customers or to its own safety and soundness from identity theft, such as those already developed in connection with the covered entity's fraud prevention program. Thus, the burden estimate attributable to the creation of a Program is unchanged.

The final rulemaking also clarifies that only relevant staff need be trained to implement the Program, as necessary—meaning that staff already trained, for example, as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as necessary. Despite this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours.

The Agencies' estimates attribute all burden to covered entities, which are entities directly subject to the requirements of the final rulemaking. A covered entity that outsources activities to a third-party service provider is, in effect, reallocating to that service provider the burden that it would otherwise have carried itself. Under these circumstances, burden is, by contract, shifted from the covered entity to the service provider, but the total amount of burden is not increased. Thus, third-party service provider burden is already included in the burden estimates provided for covered entities.

The Agencies continue to believe that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Further, as commenters requested, the final rulemaking clarifies that card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, before a request for an additional or replacement card. Therefore, the estimates attributable to this portion of the rulemaking are unchanged.

Regarding the final rules implementing section 315, the Agencies recognize that users of consumer reports will need to develop policies and procedures to employ upon receiving a notice of address discrepancy in order to: (1) Ensure that the user has obtained the correct consumer report for the consumer; and (2) confirm the accuracy of the address the user furnishes to the CRA. However, under the final rules, a user only must furnish a confirmed address to a CRA for new relationships. Thus, the required policies and procedures will no longer need to address the furnishing of confirmed addresses for existing relationships, and users will not need to furnish to the CRA in connection with existing relationships an address the user reasonably confirmed is accurate.

The Agencies believe that users of credit reports covered by the final rules,

---

[55] *See, e.g.*, 31 CFR 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 CFR 103.122 (broker-dealers); 31 CFR 103.123 (futures commission merchants).

[56] 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D–2 and part 225, app. F (state member banks and holding companies); 12 CFR part 364, app. B (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, app. A and B, and 12 CFR 717 (credit unions); 16 CFR part 314 (financial institutions that are not regulated by the Board, FDIC, NCUA, OCC and OTS).

[57] *See, e.g.*, 12 CFR part 30, supp. A to app. B (national banks); 12 CFR part 208, supp. A to app. D–2 and part 225, supp. A to app. F (state member banks and holding companies); 12 CFR part 364, supp. A to app. B (state non-member banks); 12 CFR part 570, supp. A to app. B (savings associations); 12 CFR 748, app. A and B (credit unions); Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet (the "IS Booklet") *available at http://www.ffiec.gov/guides.htm*; FFIEC "Authentication in an Internet Banking Environment" *available at http://www.ffiec.gov/pdf/authentication_guidance.pdf*; Board SR 01–11 (Supp) (Apr. 26, 2001) *available at: http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm*, "Guidance on Identity Theft and Pretext Calling," OCC AL 2001–4 (April 30, 2001); "Identity Theft and Pretext Calling," OTS CEO Letter #139 (May 4, 2001); NCUA Letter to Credit Unions 01–CU–09, "Identity Theft and Pretext Calling" (Sept. 2001); OCC 2005–24, "Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents," (July 1, 2005); "Phishing and E-mail Scams," OTS CEO Letter #193 (Mar. 8, 2004); NCUA Letter to Credit Unions 04–CU–12, "Phishing Guidance for Credit Unions" (Sept. 2004).

on a regular basis, already furnish information to CRAs in response to notices of address discrepancy because it is a usual and customary business practice—except in connection with new deposit relationships. For the proposed rulemaking, the Agencies had estimated that there would be no implementation burden associated with furnishing confirmed addresses to CRAs. However, as the result of additional research, the Agencies now believe that some burden should be attributable to this collection, to account for information furnished to CRAs for new deposit relationships. Because this burden is offset by the reduction in burden described above, the estimates for the collections attributable to the final rules implementing section 315 remain unchanged.

The Agencies continue to believe that 25 hours to develop a Program, four hours to prepare an annual report, four hours to develop policies and procedures to assess the validity of changes of address, and four hours to develop policies and procedures to respond to notices of address discrepancy, are reasonable estimates.

The potential respondents are national banks and Federal branches and agencies of foreign banks and certain of their subsidiaries (OCC); state member banks, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations (Board); insured nonmember banks, insured state branches of foreign banks, and certain of their subsidiaries (FDIC); savings associations and certain of their subsidiaries (OTS); Federally-chartered credit unions (NCUA); state-chartered credit unions, non-bank lenders, mortgage brokers, motor vehicle dealers, utility companies, and any other person that regularly participates in a credit decision, including setting the terms of credit (FTC).

Burden Estimates

The Agencies estimate the annual burden per respondent is 41 hours (25 hours to develop a Program, four hours to prepare an annual report, four hours for training, four hours for developing policies and procedures to assess the validity of changes of address, and four hours for developing policies and procedures to respond to notices of address discrepancy). The Agencies attribute total burden to covered entities as follows:

OCC:
Number of respondents: 1,806.
Total estimated annual burden: 74,046.
Board:
Number of respondents: 1,172.
Total Estimated Annual Burden: 48,052.
FDIC:
Number of respondents: 5,260.
Total Estimated Annual Burden: 215,660 hours.
OTS:
Number of respondents: 832.
Total Estimated Annual Burden: 34,112.
NCUA:
Number of respondents: 5,103.
Total Estimated Annual Burden: 209,223.
FTC Estimated Burden:[58]
Section 114:
Estimated Hours Burden:

As discussed above, the final regulations require financial institutions and creditors to conduct a risk assessment periodically to determine whether they have covered accounts, which include, at a minimum, consumer accounts. If the financial institutions and creditors determine that they have covered accounts, the final regulations require them to create a written Identity Theft Prevention Program (Program) and they should report to the board of directors, a committee thereof, or senior management at least annually on compliance with the final regulations. The FCRA defines "creditor" to have the same meaning as in section 702 of the Equal Credit Opportunity Act (ECOA).[59] Under Regulation B, which implements the ECOA, a creditor means a person who regularly participates in a credit decision, including setting the terms of credit. Regulation B defines credit as a transaction in which the party has a right to defer payment of a debt, regardless of whether the credit is for personal or commercial purposes.[60] Given the broad scope of entities covered, it is difficult to determine precisely the number of financial institutions and creditors that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction, and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the proposed regulations implementing section 114 will affect over 3,500 financial institutions[61] and over 11 million creditors[62] subject to the FTC's jurisdiction, for a combined total of approximately 11.1 million affected entities. As detailed below, FTC staff estimates that the average annual information collection burden during the three-year period for which OMB clearance was sought will be 4,466,000 hours (rounded to the nearest thousand). The estimated annual labor cost associated with this burden is $142,925,000 (rounded to the nearest thousand).

For the proposed rule, FTC staff had divided affected entities into two categories: entities that are subject to a high risk of identity theft and entities that are subject to a low risk of identity theft. Based on comments as well as changes in the final rule, FTC staff believes that the affected entities can be categorized in three groups, based on the nature of their businesses: entities subject to a high risk of identity theft, entities subject to a low risk of identity theft, but having consumer accounts that will require them to have a written Program, and entities subject to a low risk of identity theft, but not having consumer accounts.[63]

A. High-Risk Entities

In drafting its PRA analysis for the proposed regulations, FTC staff believed that because motor vehicle dealers" loans typically are financed by financial institutions also subject to those regulations, the dealers were likely to use the latter's programs as a basis to develop their own. Therefore, although subject to a high risk of identity theft, their burden would be less than other high-risk entities. Commenters, however, noted among other concerns that some motor vehicle dealers finance

[58] Due to the varied nature of the entities subject to the jurisdiction of the FTC, this Estimated Burden section reflects only the view of the FTC. The banking regulatory agencies have jointly prepared a separate analysis.

[59] U.S.C. 1681a(r)(5).

[60] Regulation B Equal Credit Opportunity, 12 CFR 202 (as amended effective Apr. 15, 2003).

[61] Under the FCRA, the only financial institutions over which the FTC has jurisdiction are state-chartered credit unions. 15 U.S.C. 1681s. As of December 31, 2005, there were 3,302 state-chartered federally-insured credit unions and 362 state-chartered nonfederally insured credit unions, totaling 3,664 financial institutions. *See www.ncua.gov/news/quick_facts/quick_facts.html and* "Disclosures for Non-Federally Insured Depository Institutions under the Federal Deposit Insurance Corporation Improvement Act (FDICIA)," 70 FR 12823 (Mar. 16, 2005).

[62] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, which totaled 11,076,463 creditors subject to the FTC's jurisdiction.

[63] In general, high-risk entities may provide consumer financial services or other goods or services of value to identity thieves such as telecommunication services or goods that are easily convertible to cash, whereas low-risk entities may do business primarily with other businesses or provide non-financial services or goods that are not easily convertible to cash.

their own loans. Thus, for this burden estimate, FTC staff no longer is considering motor vehicle dealers separately from other high-risk entities.

As noted above, the Agencies continue to believe that many of the high-risk entities, as part of their usual and customary business practices, already take steps to minimize losses due to fraud. The final rulemaking clarifies that only relevant staff need be trained to implement the Program, as necessary meaning, for example, that staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as incrementally needed. Notwithstanding this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours, as is the FTC for high-risk entities in their initial year of implementing the Program, but FTC staff continues to believe that one hour of recurring annual training remains a reasonable estimate.

The FTC staff maintains its estimate of 25 hours for high-risk entities to create and implement a written Program, with an annual recurring burden of 1 hour. As before, FTC staff anticipates that these entities will incorporate policies and procedures that they likely already have in place. The FTC staff continues to believe that preparation of an annual report will take high-risk entities 4 hours initially, with an annual recurring burden of 1 hour.

B. Low-Risk Entities

A few commenters believed that FTC staff had underestimated the amount of time it would take low-risk entities to comply with the proposed regulations. These commenters estimated that the amount of time would range from 6 to 20 hours to create a program and 1 hour each to train employees and draft the annual report. The FTC staff believes these estimates were based on a misunderstanding of the requirements of the proposed regulations, including that the list of 31 Red Flags in the proposed guidelines was intended to be a checklist. The final regulations clarify that the list of Red Flags is illustrative only. Moreover, the emphasis of the written Program, as required under the final regulations, is to identify risks of identity theft. To the extent that entities with consumer accounts determine that they have a minimal risk of identity theft, they would be tasked only with developing a streamlined Program. Therefore, the FTC staff does not believe that it would take such an entity 6 to 20 hours to develop a Program, 1 hour to train employees, and 1 hour to draft an annual report on risks of identity theft which are minimal or non-existent. Nonetheless, FTC staff believes that it may have underestimated the time low-risk entities may need to initially apply the final rule to develop a Program. Thus, FTC staff has increased from 20 minutes to 1 hour its previously stated estimate for this activity.

The final regulations have been revised from the proposed regulations to alleviate the burden of creating a written Program for entities that determine that they do not have any covered accounts. The FTC staff believes that entities subject to a low risk of identity theft, but not having consumer accounts, will likely determine that they do not have covered accounts. Such entities would not be required to develop a written Program, and thus will not incur PRA burden. The FTC staff estimates that approximately 9,191,496 [64] of the 10,813,525 low-risk entities subject to the requirement to create a written Program under the proposed regulations will not have covered accounts under the final rule. Therefore, these 9,191,496 low-risk entities will not be required to develop a written Program, thereby substantially reducing the original burden hours estimate in the NPRM for low-risk entities.

The FTC staff believes that for entities subject to a low risk of identity theft, but having consumer accounts that will require them to have a written Program, it will take such entities 1 hour to review the final regulations and create a streamlined Program, with an annual recurring burden of 5 minutes. The FTC staff believes that training staff to be attentive to any future risks of identity theft will take low-risk entities 10 minutes, with an annual recurring burden of 5 minutes. The FTC staff believes that preparing an annual report will take low-risk entities 10 minutes, with an annual recurring burden of 5 minutes.

Accordingly, FTC staff estimates that the final regulations implementing section 114 affect the following: 266,602 high-risk entities subject to the FTC's jurisdiction at an average annual burden of 13 hours per entity [average annual burden over 3-year clearance period for creation and implementation of Program ((25+1+1)/3) plus average annual burden over 3-year clearance period for staff training ((4+1+1)/3) plus average annual burden over 3-year clearance period for preparing annual report ((4+1+1)/3)], for a total of 3,466,000 hours (rounded to the nearest thousand); and 1,622,029 low-risk entities that have consumer accounts subject to the FTC's jurisdiction at an average annual burden of approximately 37 minutes per entity [average annual burden over 3-year clearance period for creation and implementation of streamlined Program ((60+5+5)/3) plus average annual burden over 3-year clearance period for staff training ((10+5+5)/3) plus average annual burden over 3-year clearance period for preparing annual report ((10+5+5)/3], for a total of 1,000,000 hours (rounded to the nearest thousand).

The proposed regulations implementing Section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request, including notifying the cardholder or using another means of assessing the validity of the change of address. The FTC received no comments on its burden estimates in the NPRM and FTC staff does not believe that the changes made to the final regulation have altered its original burden estimates. Accordingly, FTC staff maintains that it will take 100 credit or debit card issuers 4 hours to develop and implement policies and procedures to assess the validity of a change of address request for a total burden of 400 hours.

Estimated Cost Burden:

The FTC staff derived labor costs by applying appropriate estimated hourly cost figures to the burden hours described above. It is difficult to calculate with precision the labor costs associated with the proposed regulations, as they entail varying compensation levels of management and/or technical staff among companies of different sizes. In the NPRM, FTC staff had estimated that low-risk entities would use administrative support personnel at an hourly cost of $16.00. A few commenters disagreed that low-risk entities would use administrative support personnel, arguing instead that the Program would be implemented at a managerial level, and the labor cost should be at least $32.00 and possibly even $48.00. Therefore, in calculating the cost figures, FTC staff assumes that for all entities, professional technical personnel and/or managerial personnel will create and implement the Program, prepare the annual report, train employees, and assess the validity of a

[64] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, net of the number of creditors subject to the FTC's jurisdiction, an estimated subset of which comprise anticipated low-risk entities not having covered accounts under the final rule.

change of address request, at an hourly rate of $32.00.[65]

Based on the above estimates and assumptions, the total annual labor costs for all categories of covered entities under the final regulations implementing section 114 are $142,925,000 (rounded to the nearest thousand) [(3,466,000 hours + 400 hours + 1,000,000 hours) x $32.00)].

Section 315:

Estimated Hours Burden:

The Commission did not receive any comments relating to its original burden estimates for the information collection requirements under section 315. Although the final regulations were modified such that they no longer require users to furnish a confirmed address to a CRA for existing relationships, FTC staff does not believe that this modification will significantly alter its original burden estimates. Therefore, FTC staff burden estimates remain unchanged under section 315 from the estimates proposed in the NPRM. Accordingly, FTC staff estimates that the average annual information collection burden during the three-year period for which OMB clearance was sought will be 831,000 hours (rounded to the nearest thousand). The FTC staff continues to assume that the policies and procedures for notice of address discrepancy and furnishing the correct address will be set up by administrative support personnel at an hourly rate of $16.[66] Thus, the estimated annual labor cost associated with this burden is $13,296,000 (rounded to the nearest thousand).

The Agencies have a continuing interest in the public's opinions of our collections of information. At any time, comments regarding the burden estimate, or any other aspect of this collection of information, including suggestions for reducing the burden, may be sent to:

OCC: Communications Division, Office of the Comptroller of the Currency, Public Information Room, Mail stop 1–5, Attention: 1557–0237, 250 E Street, SW., Washington, DC 20219. In addition, comments may be sent by fax to 202–874–4448, or by electronic mail to *regs.comments@occ.treas.gov*. You can inspect and photocopy the comments at the OCC's Public Information Room, 250 E Street, SW., Washington, DC 20219. For security reasons, the OCC requires that visitors make an appointment to inspect comments. You may do so by calling 202–874–5043. Upon arrival, visitors will be required to present valid government-issued photo identification and submit to security screening in order to inspect and photocopy comments.

Board: You may submit comments, identified by R–1255, by any of the following methods:

Agency Web site: *http://www.federalreserve.gov*. Follow the instructions for submitting comments on *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm*.

Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.

E-mail: *regs.comments@federalreserve.gov*. Include docket number in the subject line of the message.

Fax: 202–452–3819 or 202–452–3102.

Mail: Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW., Washington, DC 20551.

All public comments are available from the Board's Web site at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, unless modified for technical reasons. Accordingly, your comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper form in Room MP–500 of the Board's Martin Building (20th and C Streets, NW.) between 9 a.m. and 5 p.m. on weekdays.

FDIC: You may submit written comments, which should refer to 3064–AD00, by any of the following methods:

Agency Web site: *http://www.fdic.gov/regulations/laws/federal/propose.html*.

Follow the instructions for submitting comments on the FDIC Web site.

Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.

E-mail: *Comments@FDIC.gov*.

Mail: Robert E. Feldman, Executive Secretary, Attention: Comments, FDIC, 550 17th Street, NW., Washington, DC 20429.

Hand Delivery/Courier: Guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7 a.m. and 5 p.m.

Public Inspection: All comments received will be posted without change to *http://www.fdic.gov/regulations/laws/federal/propose/html* including any personal information provided. Comments may be inspected at the FDIC Public Information Center, Room 100, 801 17th Street, NW., Washington, DC, between 9 a.m. and 4:30 p.m. on business days.

OTS: Information Collection Comments, Chief Counsel's Office, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552; send a facsimile transmission to (202) 906–6518; or send an e-mail to related index on the OTS Internet site at *http://www.ots.treas.gov*. In addition, interested persons may inspect the comments at the Public Reading Room, 1700 G Street, NW., by appointment. To make an appointment, call (202) 906–5922, send an e-mail to *publicinfo@ots.treas.gov*, or send a facsimile transmission to (202) 906–7755.

NCUA: You may submit comments by any of the following methods (Please send comments by one method only):

Federal eRulemaking Portal: *http://www.regulations.gov*.

Follow the instructions for submitting comments.

NCUA Web site: *http://www.ncua.gov/RegulationsOpinionsLaws/proposedregs/proposedregs.html*.

Follow the instructions for submitting comments.

E-mail: Address to *regcomments@ncua.gov*. Include "[Your name] Comments on -," in the e-mail subject line.

Fax: (703) 518–6319. Use the subject line described above for e-mail.

Mail: Address to Mary F. Rupp, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314–3428.

Hand Delivery/Courier: Same as mail address.

Additionally, commenters may send a copy of their comments to the OMB desk officer for the OCC, Board, FDIC, OTS, and NCUA by mail to the Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street, NW., Washington, DC 20503, or by fax to (202) 395–6974.

FTC: Comments should refer to "The Red Flags Rule: Project No. R611019," and may be submitted by any of the following methods. However, if the comment contains any material for which confidential treatment is requested, it must be filed in paper form, and the first page of the document

[65] The cost is derived from a mid-range among the reported 2006 Bureau of Labor Statistics rates for likely positions within the professional technical and managerial categories. See June 2006 Bureau of Labor Statistics National Compensation Survey for occupational wages in the United States at *http://www.bls.gov/ncs/ocs/sp/ncbl0910.pdf* ("June 2006 BLS NCS Survey").

[66] This hourly wage is a conservative inflation-adjusted updating of hourly mean wages ($14.86) shown for administrative support personnel in the June 2006 BLS NCS Survey.

must be clearly labeled "Confidential." [67]

E-mail: Comments filed in electronic form should be submitted by clicking on the following Web link: *https://secure.commentworks.com/ftc-redflags* and following the instructions on the Web-based form. To ensure that the Commission considers an electronic comment, you must file it on the Web-based form at *https://secure.commentworks.com/ftc-redflags*.

Federal eRulemaking Portal: If this notice appears at *http://www.regulations.gov*, you may also file an electronic comment through that Web site. The Commission will consider all comments that regulations.gov forwards to it.

Mail or Hand Delivery: A comment filed in paper form should include "The Red Flags Rule, Project No. R611019," both in the text and on the envelope and should be mailed or delivered, with two complete copies, to the following address: Federal Trade Commission/Office of the Secretary, Room H–135 (Annex M), 600 Pennsylvania Avenue, NW., Washington, DC 20580. Because paper mail in the Washington area and at the Commission is subject to delay, please consider submitting your comments in electronic form, as prescribed above. The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should additionally be submitted to: Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission. Comments should be submitted via facsimile to (202) 395–6974 because U.S. Postal Mail is subject to lengthy delays due to heightened security precautions.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC Web site, to the extent practicable, at *http://www.ftc.gov/os/publiccomments.htm*. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm*.

Members of the public also can request additional information or a copy of the collection from:

OCC: Mary Gottlieb, OCC Clearance Officer, (202) 874–5090, Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, 250 E Street, SW., Washington, DC 20219.

Board: Michelle Shore, Clearance Officer, Division of Research and Statistics (202) 452–3829.

FDIC: Steven F. Hanft, Clearance Officer, Legal Division, (202–898–3907).

OTS: Ira L. Mills, OTS Clearance Officer, Litigation Division, Chief Counsel's Office, at *Ira.Mills@ots.treas.gov*, (202) 906–6531, or facsimile number (202) 906–6518.

NCUA: Regina M. Metz, Staff Attorney, Office of General Counsel, (703) 518–6540.

FTC: See **FOR FURTHER INFORMATION CONTACT** above.

B. Regulatory Flexibility Act

OCC: Under section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), the OCC must either publish a Final Regulatory Flexibility Analysis (FRFA) for a final rule or certify, along with a statement providing the factual basis for such certification, the rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration has defined "small entities" for banking purposes as a bank or savings institution with assets of $165 million or less. *See* 13 CFR 121.201.

Based on its analysis and for the reasons stated below, the OCC certifies that this final rulemaking will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 114

The proposed regulations implementing section 114 required the development and establishment of a written identity theft prevention program to detect, prevent, and mitigate identity theft. The proposed regulations also required card issuers to assess the validity of a notice of address change under certain circumstances.

In connection with the proposed rulemaking, the OCC concluded that the proposed regulations implementing section 114, if adopted as proposed, would not impose undue costs on national banks and would not have a substantial economic impact on a substantial number of small national banks. The OCC noted that national banks already employ a variety of measures that satisfy the requirements of the rulemaking because (1) such measures are a good business practice and generally are a part of a bank's efforts to reduce losses due to fraud, and (2) national banks already comply with other regulations and guidance that relate to information security, authentication, identity theft, and response programs. For example, national banks are already subject to CIP rules requiring them to verify the identity of a person opening a new account [68] and already have various systems in place to detect certain patterns, practices and specific activities that indicate the possible existence of identity theft in connection with the opening of new accounts. Similarly, national banks complying with the "Interagency Guidelines Establishing Information Security Standards" [69] and guidance recently issued by the FFIEC titled "Authentication in an Internet Banking Environment" [70] already have policies and procedures in place to detect attempted and actual intrusions into customer information systems and to detect patterns, practices and specific activities that indicate the possible existence of identity theft in connection with existing accounts. Banks complying with the OCC's "Guidance on Identity Theft and Pretext Calling" [71] already have policies and procedures to verify the validity of change of address requests on existing accounts.

Nonetheless, the OCC specifically requested comment and specific data on the size of the incremental burden creating an identity theft prevention program would have on small national banks, given banks" current practices and compliance with existing requirements. The OCC also requested comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Commenters confirmed that the proposed regulations implementing section 114 of the FACT Act are consistent with banks" usual and customary business practices used to minimize losses due to fraud in connection with new and existing

[67] Commission Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. See Commission Rule 4.9(c), 16 CFR 4.9(c).

[68] 31 CFR 103.121; 12 CFR 21.21 (national banks).

[69] 12 CFR part 30, app. B (national banks).

[70] OCC Bulletin 2005–35 (Oct. 12, 2005).

[71] OCC AL 2001–4 (April 30, 2001).

accounts. They also confirmed that banks have implemented measures to address many of the proposed requirements as a result of having to comply with existing regulations and guidance. However, commenters also asserted that the Agencies had underestimated the incremental burden imposed by the proposed rules. They highlighted aspects of the proposal that they maintained would have required banks to alter their current practices and implement duplicative policies and procedures.

Only a few commenters provided estimates of additional burden that would result from the proposed rules. Many of these comments stemmed from a misreading of the requirements of the proposed rules. Further, many commenters confused the Agencies' PRA estimates with the Agencies' overall conclusions regarding regulatory burden.[72]

The OCC believes that the final rules substantially address the concerns of the commenters as follows:

- The final rules allow a covered entity to tailor its Program to its size, complexity and nature of its operations. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.
- The final rules list the four elements that must be a part of a Program, and the steps that a covered entity must take to administer the Program. The rules provide covered entities with greater discretion to determine how to implement these mandates.
- Additional requirements previously in the proposed rules are now in guidelines that are located in Appendix J. The guidelines describe various policies and procedures that a financial institution or creditor must consider and include in its Program, where appropriate, to satisfy the requirements of the final rules. The preamble to the rules explains that an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program as long as its Program contains reasonable policies and procedures to meet the specific requirements of the final rules.
- The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program.
- The final rules clarify that a Program (including the Red Flags determined to be relevant) may be periodically, rather than continually, updated to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
- The rules focus on consumer accounts, and require a Program to include only other accounts "for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft."
- The definition of "Red Flags" no longer includes reference to the "possible risk" of identity theft and no longer incorporates precursors to identity theft.
- The final rules clarify that the Red Flags in Supplement A are examples rather than a mandatory checklist.
- Supplement A includes a Red Flag for activity on an inactive account in place of a separate guideline.
- The final rules clarify that the Board of Directors or a committee thereof must approve only the initial written Program. The rules provide a covered entity with the discretion to determine whether the Board or management will approve changes to the Program and the extent of Board involvement in oversight of the Program.
- The final rules clarify that only relevant staff must be trained to implement the Program, as necessary.
- Card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers' existing procedures.
- Covered entities need not comply with the final rules until November 1, 2008.

The Agencies did consider whether it would be appropriate to extend different treatment or exempt small covered entities from the requirements of this section of the final rulemaking. The Agencies note that identity theft can occur in small entities as well as large ones. The Agencies do not believe that an exemption for small entities is appropriate given the flexibility built into the final rules and guidelines and the importance of the statutory goals and mandate of section 114.

As a result of the changes and clarifications noted above, this section of the final rule is far more flexible and less burdensome than that in the proposed rules while still fulfilling the statutory mandates enumerated in section 114. Moreover, the OCC has concluded that the incremental cost of these final rules and guidelines will not impose undue costs and will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 315

The proposed regulations implementing section 315 required a user of consumer reports to have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. The proposed rules also required the user to furnish to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the user: (1) Is able to form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained; (2) establishes *or* maintains a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained.

In connection with the proposed rulemaking the OCC noted that the FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. The OCC stated that with respect to new accounts, a national bank already is required by the CIP rules to ensure that it knows the identity of a person opening a new account and to keep a record describing the resolution of any substantive discrepancy discovered during the verification process. The OCC also stated that as a matter of good business practice, most national banks currently have policies and procedures in place to respond to notices of address discrepancy when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the bank has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy.

The OCC specifically requested comment on whether the proposed requirements differ from small banks' current practices and whether the proposed requirements on users of consumer reports to have policies and procedures to respond to the receipt of an address discrepancy could be altered

[72] The PRA focuses more narrowly on the time, effort, and financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency. *See* 44 U.S.C. 3501 *et seq.*

to minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Many suggestions received in response to this solicitation for comment would have required a statutory change. However, many commenters noted that section 315 does not require the reporting of a confirmed address to a CRA for a notice of address discrepancy received for an existing account. These commenters stated that the level of regulatory burden imposed by this requirement would be significant and would force users to reconcile and verify addresses millions of times a year in connection with routine account maintenance. Commenters maintained that this would result in enormous costs that provide relatively little benefit to consumers. The final rules address these comments and accordingly, under the rules implementing section 315, a user is not obligated to furnish a confirmed address for the consumer to the CRA in connection with existing accounts.

Although, a bank will likely have to modify its existing procedures to add a new procedure for promptly reporting to CRAs the reconciled address for new deposit accounts, the OCC has concluded that the final rules implementing section 315 will not impose undue costs on national banks and will have not have a significant economic impact on a substantial number of small entities. Finally, as mentioned earlier, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

Board: The Board prepared an initial regulatory flexibility analysis as required by the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 *et seq.*) in connection with the July 18, 2006 proposed rule. The Board received one comment on its regulatory flexibility analysis.

Under Section 605(b) of the RFA, 5 U.S.C. 605(b), the regulatory flexibility analysis otherwise required under Section 604 of the RFA is not required if an agency certifies, along with a statement providing the factual basis for such certification, that the rule will not have a significant economic impact on a substantial number of small entities. Based on its analysis and for the reasons stated below, the Board certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

1. *Statement of the need for, and objectives of, the final rule.*

The FACT Act amends the FCRA and was enacted, in part, for the purpose of helping to reduce identity theft. Section 114 of the FACT Act amends section 615 of the FCRA and directs the Board, together with the other Agencies, to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances. Section 315 of the FACT Act adds section 605(h)(2) to the FCRA and requires the Agencies to issue joint regulations that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy. The Board received no comments on the reasons for the proposed rule. The Board is adopting the final rule to implement sections 114 and 315 of the FACT Act. The **SUPPLEMENTARY INFORMATION** above contains information on the objectives of the final rule.

2. *Summary of issues raised by comments in response to the initial regulatory flexibility analysis.*

In accordance with Section 3(a) of the RFA, the Board conducted an initial regulatory flexibility analysis in connection with the proposed rule. One commenter, the Mortgage Bankers Association (MBA), responded to the initial regulatory flexibility analysis and stated that contrary to the Agencies' belief, the proposed rule would have a significant economic impact on a substantial number of affected small entities. The MBA stated that commercial and multifamily mortgage lenders should not be subject to the proposed rule because it would constitute useless regulatory burden. Three commenters (Independent Community Bankers of America, The Financial Services Roundtable and BITS, and KeyCorp) believed that the Board and the other Agencies had underestimated the costs of compliance. The issues raised by these commenters did not apply uniquely to small entities and are described in the Paperwork Reduction Act section above.

Some small financial institutions expressed concern about the flexibility granted by the proposal. As stated in the Overview of Proposal and Comments Received, these commenters preferred to have more structured guidance that describes how to develop and implement a Program and what they would need to do to achieve compliance. In addition, one commenter expressed concern that smaller institutions would be particularly burdened by the proposal's requirement that the Program be designed to address changing identity risks "as they arise."

3. *Description and estimate of small entities affected by the final rule.*

The final rule applies to all banks that are members of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and Agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*). The Board's rule will apply to the following institutions (numbers approximate): State member banks (881), operating subsidiaries that are not functionally regulated with in the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (877), U.S. branches and agencies of foreign banks (219), commercial lending companies owned or controlled by foreign banks (3), and Edge and agreement corporations (64), for a total of approximately 2,044 institutions. The Board estimates that more than 1,448 of these institutions could be considered small entities with assets of $165 million or less.

4. *Recordkeeping, reporting, and other compliance requirements.*

Section 114 requires the Board to prescribe regulations that require financial institutions and creditors to establish reasonable policies and procedures to implement guidelines established by the Board and other federal agencies that address identity theft with respect to account holders and customers. This would be implemented by requiring a covered financial institution or creditor to create an Identity Theft Prevention Program that detects, prevents and mitigates the risk of identity theft applicable to its accounts.

Section 114 also requires the Board to adopt regulations applicable to credit and debit card issuers to implement policies and procedures to assess the validity of change of address requests. The final rule implements this by requiring credit and debit card issuers to establish reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the issuer receives a request for an additional or replacement card for the same account.

Section 315 requires the Board to prescribe regulations that provide guidance regarding the reasonable policies and procedures that a user of

consumers' reports should employ to verify the identity of a consumer when a consumer reporting agency provides a notice of address discrepancy with the consumer reporting agency in certain circumstances. The final rule requires users of consumer reports to develop and implement reasonable policies and procedures for verifying the identity of a consumer for whom it has obtained a consumer report and for whom it receives a notice of address discrepancy and to reconcile an address discrepancy with the appropriate consumer reporting agency in certain circumstances.

5. *Steps taken to minimize the economic impact on small entities.*

The Board and the other Agencies have attempted to minimize the economic impact on small entities by providing more flexibility in developing a Program and moving certain detail contained in the proposed regulations to the guidelines. In addition, to allow small entities and creditors to tailor their Programs to their operations, the final rules provide that the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. The Board has also eliminated the requirement for institutions to update their Program in response to changing identity theft risks "as they arise." The final rule instead requires "periodic" updating.

FDIC: The FDIC prepared an initial regulatory flexibility analysis as required by the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 et seq.) in connection with the July 18, 2006 proposed rule. Under Section 605(b) of the RFA, 5 U.S.C. 605(b), the regulatory flexibility analysis otherwise required under Section 604 of the RFA is not required if an agency certifies, along with a statement providing the factual basis for such certification, that the rule will not have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include banks with less than $165 in assets). Based on its analysis and for the reasons stated below, the FDIC certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

Under the final rule implementing FACT Act Section 114, financial institutions and creditors must have a written program that includes controls to address the identity theft risks they have identified. Credit and debit card issuers must also have additional policies and procedures to assess the validity of change of address requests.

The final rule would apply to all FDIC-insured state nonmember banks, approximately 3,260 of which are small entities. The rule is drafted in a flexible manner that allows institutions to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.

The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program. The FDIC believes that many institutions have already implemented a significant portion of the detection and mitigation efforts required by the rule.

With respect to the portion of the rule covering card issuers, those entities may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers' existing procedures.

Under the final rule implementing FACT Act Section 315, a user of consumer reports (which constitutes most, if not all, FDIC-insured state nonmember banks) must have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. Although, a bank will likely have to modify its existing procedures to add a new procedure for promptly reporting to consumer reporting agencies the reconciled address for new deposit accounts, the FDIC has concluded that the final rules implementing section 315—which only obligates a user to furnish a confirmed address for the consumer to the consumer reporting agency in connection with new, and not existing, accounts—will not impose undue costs on banks and will not have a significant economic impact on a substantial number of small entities.

Moreover, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

OTS: Under section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), OTS must either publish a Final Regulatory Flexibility Analysis (FRFA) for a final rule or certify, along with a statement providing the factual basis for such certification, the rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration has defined "small entities" to include savings associations with total assets of $165 million or less. 13 CFR 121.201.

The rule will implement section 114 and 315 of the FACT Act and will apply to all savings associations (and federal savings associations operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act), 424 of which have assets of less than or equal to $165 million. Based on its analysis and for the reasons stated below, OTS certifies that this final rulemaking will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 114

The proposed regulations implementing section 114 required the development and establishment of a written identity theft prevention program to detect, prevent, and mitigate identity theft. The proposed regulations also required card issuers to assess the validity of a notice of address change under certain circumstances.

In connection with the proposed rulemaking, OTS concluded that the proposed regulations implementing section 114, if adopted as proposed, would not impose undue costs on savings associations and would not have a substantial economic impact on a substantial number of small savings associations. OTS noted that savings associations already employ a variety of measures that satisfy the requirements of the rulemaking because (1) such measures are a good business practice and generally are a part of a thrift's efforts to reduce losses due to fraud, and (2) savings associations already comply with other regulations and guidance that relate to information security, authentication, identity theft, and response programs. For example, savings associations are already subject to CIP rules requiring them to verify the identity of a person opening a new account [73] and already have various systems in place to detect certain patterns, practices and specific activities that indicate the possible existence of identity theft in connection with the opening of new accounts. Similarly, savings associations complying with the "Interagency Guidelines Establishing

[73] 31 CFR 103.121; 12 CFR 563.177 (savings associations).

Information Security Standards"[74] and guidance recently issued by the FFIEC titled "Authentication in an Internet Banking Environment"[75] already have policies and procedures in place to detect attempted and actual intrusions into customer information systems and to detect patterns, practices and specific activities that indicate the possible existence of identity theft in connection with existing accounts. Savings associations complying with OTS's guidance on "Identity Theft and Pretext Calling"[76] already have policies and procedures to verify the validity of change of address requests on existing accounts.

Nonetheless, OTS specifically requested comment and specific data on the size of the incremental burden creating an identity theft prevention program would have on small saving associations, given their current practices and compliance with existing requirements. OTS also requested comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Commenters confirmed that the proposed regulations implementing section 114 of the FACT Act are consistent with savings associations' usual and customary business practices used to minimize losses due to fraud in connection with new and existing accounts. They also confirmed that savings associations have implemented measures to address many of the proposed requirements as a result of having to comply with existing regulations and guidance. However, commenters also asserted that the Agencies had underestimated the incremental burden imposed by the proposed rules. They highlighted aspects of the proposal that they maintained would have required savings associations to alter their current practices and implement duplicative policies and procedures.

Only a few commenters provided estimates of additional burden that would result from the proposed rules. Many of these comments stemmed from a misreading of the requirements of the proposed rules. Further, many commenters confused the Agencies' PRA estimates with the Agencies' overall conclusions regarding regulatory burden.[77]

[74] 12 CFR part 570, app. B (savings associations).

[75] OTS CEO Letter 228 (Oct. 12, 2005).

[76] OTS CEO Letter 139 (May 4, 2001).

[77] The PRA focuses more narrowly on the time, effort, and financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency. *See* 44 U.S.C. 3501 *et seq.*

OTS believes that the final rules substantially address the concerns of the commenters as follows:

- The final rules allow a covered entity to tailor its Program to its size, complexity and nature of its operations. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.
- The final rules list the four elements that must be a part of a Program, and the steps that a covered entity must take to administer the Program. The rules provide covered entities with greater discretion to determine how to implement these mandates.
- Additional requirements previously in the proposed rules are now in guidelines that are located in Appendix J. The guidelines describe various policies and procedures that a financial institution or creditor must consider and include in its Program, where appropriate, to satisfy the requirements of the final rules. The preamble to the rules explains that an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program as long as its Program contains reasonable policies and procedures to meet the specific requirements of the final rules.
- The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program.
- The final rules clarify that a Program (including the Red Flags determined to be relevant) may be periodically, rather than continually, updated to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
- The rules focus on consumer accounts, and require a Program to include only other accounts "for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft."
- The definition of "Red Flags" no longer includes reference to the "possible risk" of identity theft and no longer incorporates precursors to identity theft.
- The final rules clarify that the Red Flags in Supplement A are examples rather than a mandatory checklist.
- Supplement A includes a Red Flag for activity on an inactive account in place of a separate guideline.
- The final rules clarify that the Board of Directors or a committee thereof must approve only the initial written Program. The rules provide a covered entity with the discretion to determine whether the Board or management will approve changes to the Program and the extent of Board involvement in oversight of the Program.
- The final rules clarify that only relevant staff must be trained to implement the Program, as necessary.
- Card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers' existing procedures.
- Covered entities need not comply with the final rules until November 1, 2008.

The Agencies did consider whether it would be appropriate to extend different treatment or exempt small covered entities from the requirements of this section of the final rulemaking. The Agencies note that identity theft can occur in small entities as well as large ones. The Agencies do not believe that an exemption for small entities is appropriate given the flexibility built into the final rules and guidelines and the importance of the statutory goals and mandate of section 114.

As a result of the changes and clarifications noted above, this section of the final rule is far more flexible and less burdensome than that in the proposed rules while still fulfilling the statutory mandates enumerated in section 114. Moreover, OTS has concluded that the incremental cost of these final rules and guidelines will not impose undue costs and will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 315

The proposed regulations implementing section 315 required a user of consumer reports to have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. The proposed rules also required the user to furnish to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the user: (1) Is able to form a reasonable belief that it knows the identity of the consumer

for whom the consumer report was obtained; (2) establishes *or* maintains a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained.

In connection with the proposed rulemaking OTS noted that the FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. OTS stated that with respect to new accounts, a savings association already is required by the CIP rules to ensure that it knows the identity of a person opening a new account and to keep a record describing the resolution of any substantive discrepancy discovered during the verification process. OTS also stated that as a matter of good business practice, most savings associations currently have policies and procedures in place to respond to notices of address discrepancy when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the association has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy.

OTS specifically requested comment on whether the proposed requirements differ from small savings associations' current practices and whether the proposed requirements on users of consumer reports to have policies and procedures to respond to the receipt of an address discrepancy could be altered to minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Many suggestions received in response to this solicitation for comment would have required a statutory change. However, many commenters noted that section 315 does not require the reporting of a confirmed address to a CRA for a notice of address discrepancy received for an existing account. These commenters stated that the level of regulatory burden imposed by this requirement would be significant and would force users to reconcile and verify addresses millions of times a year in connection with routine account maintenance. Commenters maintained that this would result in enormous costs that provide relatively little benefit to consumers. The final rules address these comments and, accordingly, under the rules implementing section 315, a user is not obligated to furnish a confirmed address for the consumer to the CRA in connection with existing accounts.

Although, a savings association will likely have to modify its existing procedures to add a new procedure for promptly reporting to CRAs the reconciled address for new deposit accounts, OTS has concluded that the final rules implementing section 315 will not impose undue costs on savings associations and will have not have a significant economic impact on a substantial number of small entities. Finally, as mentioned earlier, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

FTC: The Regulatory Flexibility Act ("RFA"), 5 U.S.C. 601–612, requires that the Commission provide an Initial Regulatory Flexibility Analysis ("IRFA") with a proposed rule and a Final Regulatory Flexibility Analysis ("FRFA"), if any, with the final rule, unless the Commission certifies that the rule will not have a significant economic impact on a substantial number of small entities. *See* 5 U.S.C. 603–605.

The Commission hereby certifies that the final regulations will not have a significant economic impact on a substantial number of small business entities. The Commission recognizes that the final regulations will affect a substantial number of small businesses. We do not expect, however, that the final regulations will have a significant economic impact on these small entities.

The Commission continues to believe that a precise estimate of the number of small entities that fall under the final regulations is not currently feasible. Based on changes made to the final regulations in response to comments received, however, and the Commission's own experience and knowledge of industry practices, the Commission also continues to believe that the cost and burden to small business entities of complying with the final regulations are minimal. Accordingly, this document serves as notice to the Small Business Administration of the agency's certification of no effect. Nonetheless, the Commission has decided to publish a FRFA with these final regulations. Therefore, the Commission has prepared the following analysis:

1. Need for and Objectives of the Rule

The FTC is charged with enforcing the requirements of sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) (15 U.S.C. §§ 1681m(e) and 1681c(h)(2)), which require the FTC to establish guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft, and regulations requiring each financial institution and creditor to establish policies and procedures for implementing the guidelines. In addition, section 114 requires credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. Section 315 requires the FTC to develop policies and procedures that a user of consumer reports must employ when such a user receives a notice of address discrepancy from a consumer reporting agency described in section 603(p) of the FCRA. In this action, the FTC promulgates final rules that would implement these requirements of the FACT Act.

2. Significant Issues Received by Public Comment

The Commission received a number of comments on the effect of the proposed regulations. Some of the comments addressed the effect of the proposed regulations on businesses generally, and did not identify small businesses as a particular category. The FTC staff, therefore, has included all comments in this FRFA that raised potentially significant compliance issues for small businesses, regardless of whether the commenter identified small businesses as being an affected category.

In drafting its PRA analysis for the proposed regulations, FTC staff believed that because motor vehicle dealers' loans typically are financed by financial institutions also subject to those regulations, the dealers were likely to use the latter's programs as a basis to develop their own. Therefore, although subject to a high risk of identity theft, their burden would be less than other high-risk entities. Commenters, however, noted among other concerns that some motor vehicle dealers finance their own loans. Thus, FTC staff no longer is considering motor vehicle dealers separately from other high-risk entities.

As noted in the PRA analysis, the Agencies continue to believe that many of the high-risk entities, as part of their usual and customary business practices, already take steps to minimize losses due to fraud. The final rulemaking clarifies that only relevant staff need be trained to implement the Program, as necessary—meaning, for example, that staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as incrementally needed. Notwithstanding this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours, as is the FTC for high-risk entities in their initial year of

implementing the Program, but FTC staff continues to believe that one hour of recurring annual training remains a reasonable estimate.

A few commenters believed that FTC staff had underestimated the amount of time it would take low-risk entities to comply with the proposed regulations. These commenters estimated that the amount of time would range from 6 to 20 hours to create a program and 1 hour each to train employees and draft the annual report. The FTC staff believes these estimates were based on a misunderstanding of the requirements of the proposed regulations, including that the list of 31 Red Flags in the proposed guidelines was intended to be a checklist. The final regulations clarify that the list of Red Flags is illustrative only. Moreover, the emphasis of the written Program, as required under the final regulations, is to identify risks of identity theft. To the extent that entities with consumer accounts determine that they have a minimal risk of identity theft, they would be tasked only with developing a streamlined Program. Therefore, FTC staff does not believe that it would take such an entity 6 to 20 hours to develop a Program, 1 hour to train employees, and 1 hour to draft an annual report on risks of identity theft which are minimal or non-existent. Nonetheless, FTC staff believes that it may have underestimated the time low-risk entities may need to initially apply the final rule to develop a Program. Thus, FTC staff has increased from 20 minutes to 1 hour its previously stated estimate for this activity.

In addition, the final regulations have been revised from the proposed regulations to alleviate the burden of creating a written Program for entities that determine that they do not have any covered accounts. The FTC staff believes that entities subject to a low risk of identity theft, but not having consumer accounts, will likely determine that they do not have covered accounts. Such entities would not be required to develop a written Program. The FTC staff estimates that approximately 9,191,496 [78] of the 10,813,525 low-risk entities subject to the requirement to create a written Program under the proposed regulations will not have covered accounts under the final rule. Therefore, although these 9,191,496 low-risk entities will have to conduct a periodic risk assessment to determine if they covered accounts, they will not be required to develop a written Program, thereby substantially reducing the original burden estimate in the NPRM for low-risk entities.

The FTC received additional comments on its IRFA requesting that the FTC delay implementation of the final rules for small businesses by a minimum of six months, consider creating a certification form for low-risk entities, and develop a small business compliance guide. The Agencies have set a mandatory compliance deadline of November 1, 2008, thereby providing all entities with well over six months in which to implement the final regulations. The FTC staff will be developing a small business compliance guide prior to the mandatory compliance deadline of November 1, 2008. The FTC staff will consider whether to include any model forms in such guide.

The FTC did not receive any comments on its IRFA for the proposed regulations implementing section 114 requiring credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request, including notifying the cardholder or using another means of assessing the validity of the change of address. The FTC staff does not believe that the changes made to the final regulation have altered its original burden estimates.

The FTC did not receive any comments on its IRFA relating to the proposed regulations under section 315.

3. Small Entities to Which the Final Rule Will Apply

The final regulations apply to a wide variety of business categories under the Small Business Size Standards. Generally, the final regulations would apply to financial institutions, creditors, and users of consumer reports. In particular, entities under FTC's jurisdiction covered by section 114 include State-chartered credit unions, non-bank lenders, mortgage brokers, automobile dealers, utility companies, telecommunications companies, and any other person that regularly participates in a credit decision, including setting the terms of credit. The section 315 requirements apply to State-chartered credit unions, non-bank lenders, insurers, landlords, employers, mortgage brokers, automobile dealers, collection agencies, and any other person who requests a consumer report from a consumer reporting agency described in section 603(p) of the FCRA.

Given the coverage of the final rules, a very large number of small entities across almost every industry could be subject to the final rules. For the majority of these entities, a small business is defined by the Small Business Administration as one whose average annual receipts do not exceed $6.5 million or who have fewer than 500 employees.[79]

Section 114: As discussed in the PRA section of this Notice, given the broad scope of section 114's requirements, it is difficult to determine with precision the number of financial institutions and creditors that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the final regulations implementing section 114 will affect over 3500 financial institutions and over 11 million creditors [80] subject to the FTC's jurisdiction, for a combined total of approximately 11.1 million affected entities. Of this total, the FTC staff expects that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors).

One commenter acknowledged that the FTC's estimates as to the number of small entities that will be affected were accurate, but did not provide precise numbers.

The final regulations implementing section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. Indeed, the final regulations require credit and debit card issuers to notify the cardholder or to use another means of assessing the validity of the change of address. FTC staff believes that there may be as many as 3,764 credit or debit card issuers that fall under the jurisdiction of the FTC and that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial

[78] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, net of the number of creditors subject to the FTC's jurisdiction, an estimated subset of which comprise anticipated low-risk entities not having covered accounts under the final rule.

[79] These numbers represent the size standards for most retail and service industries ($6.5 million total receipts) and manufacturing industries (500 employees). A list of the SBA's size standards for all industries can be found at *http://www.sba.gov/size/summary-whatis.html.*

[80] This estimate is derived from census data of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers and businesses. 2003 County Business Patterns, U.S. Census Bureau *(http://censtats.census.gov/cgi- bin/cbpnaic/cbpsel.pl);* and 2002 Economic Census, Bureau *(http://www.census.gov/econ/census02/).*

institutions and $6.5 million in sales for many creditors).

The Commission did not receive any comments to the IRFA on the latter credit or debit card issuers that would allow it to determine the precise number of small entities that will be affected.

Section 315: As discussed in the PRA section of this Notice, given the broad scope of section 315's requirements, it is difficult to determine with precision the number of users of consumer reports that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the final regulations implementing section 315 will affect approximately 1.6 million users of consumer reports subject to the FTC's jurisdiction [81] and that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors).

The Commission did not receive any comments to the IRFA on the proposed regulations under Section 315 that would allow it to determine the precise number of small entities that will be affected.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The final requirements will involve some increased costs for affected parties. Most of these costs will be incurred by those required to conduct periodic risk assessments, and draft identity theft Programs and annual reports. There will also be costs associated with training, and for credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. In addition, there will be costs related to developing reasonable policies and procedures that a user of consumer reports must employ when a user receives a notice of address discrepancy from a consumer reporting agency, and for furnishing an address that the user has reasonably confirmed is accurate. The Commission does not expect, however, that the increased costs associated with the final regulations will be significant as explained below.

Section 114: The FTC staff estimates that there may be as many as 90% of the businesses affected by the proposed rules under section 114 that are subject to a high risk of identity theft that qualify as small businesses. It is likely that many such entities already engage in various activities to minimize losses due to fraud as part of their usual and customary business practices. Accordingly, the impact of the proposed requirements would be merely incremental and not significant. In particular, the rule will direct many of these entities to consolidate their existing policies and procedures into a written Program and may require some additional staff training.

The FTC expects that well over 90% of the businesses affected by the proposed rules under section 114 that are subject to a low risk of identity theft qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors). The final requirements are drafted in a flexible manner that limits the burden on a substantial majority of low-risk entities to conducting periodic risk assessments for covered accounts, and allows the remaining minority of low-risk entities to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. As a result, the FTC staff expects that the burden on these low-risk entities will be minimal (*i.e.*, not significant). The final regulations would require low-risk entities that have covered accounts that have no existing identity theft procedures to state in writing their low-risk of identity theft, train staff to be attentive to future risks of identity theft, and, if appropriate, prepare an annual report. The FTC staff believes that, for the affected low-risk entities, such activities will be not be complex or resource-intensive tasks.

The final regulations implementing section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. It is likely that most of the entities have automated the process of notifying the cardholder or using other means to assess the validity of the change of address such that implementation will pose no further burden. For those that do not, the FTC staff expects that a small number of such entities (100) will need to develop policies and procedures to assess the validity of a change of address request. The impacts on such entities should not be significant, however.

In calculating the costs, FTC staff assumes that for all entities, professional technical personnel and/or managerial personnel will conduct the periodic risk assessment, create and implement the Program, prepare the annual report, train employees, and assess the validity of a change of address request.

Section 315: The final regulations implementing section 315 provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a user receives a notice of address discrepancy from a consumer reporting agency. The final regulations also require a user of consumer reports to furnish an address that the user has reasonably confirmed is accurate to the consumer reporting agency from which it receives a notice of address discrepancy, but only to the extent that such user regularly and in the ordinary course of business furnishes information to such consumer reporting agency. The FTC staff believes that the impacts on users of consumer reports that are small businesses will not be significant. As discussed in the PRA section of the NPRM, the FTC staff believes that it will not take users of consumer reports under FTC jurisdiction a significant amount of time to develop policies and procedures that they will employ when they receive a notice of address discrepancy. FTC staff believes that only 10,000 of such users of consumer reports furnish information to consumer reporting agencies as part of their usual and customary business practices and that approximately 20% of these entities qualify as small businesses. Therefore, the staff estimates that 2,000 small businesses will be affected by this portion of the final regulation that requires furnishing the correct address. As discussed in the PRA section of this NPRM, FTC staff estimates that it will not take such users of consumer reports a significant amount of time to develop the policies and procedures for furnishing the correct address to the consumer reporting agencies pursuant to the final regulations for implementing section 315. The FTC staff estimates that the costs associated with these impacts will not be significant.

In calculating these costs, FTC staff assumes that the policies and procedures for notice of address discrepancy and furnishing the correct address will be set up by administrative support personnel.

[81] This estimate is derived from census data of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers and businesses. 2003 County Business Patterns, U.S. Census Bureau (*http://censtats.census.gov/cgi-bin/cbpnaic/cbpsel.pl*); and 2002 Economic Census, Bureau (*http://www.census.gov/econ/census02/*).

5. Steps Taken To Minimize Significant Economic Impact of the Rule on Small Entities

The Commission considered whether any significant alternatives, consistent with the purposes of the FACT Act, could further minimize the final regulations' impact on small entities. The FTC asked for comment on this issue. The final requirements are drafted in a flexible manner that limits the burden on a substantial majority of low-risk entities to conducting periodic risk assessments for covered accounts and allows the remaining minority of low-risk entities to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. In addition, a commenter requested that the FTC delay implementation of the final rules for small businesses by a minimum of six months, produce a shortened Red Flags list, consider creating a certification form for low-risk entities, and develop a small business compliance guide. The Agencies have set a mandatory compliance deadline of November 1, 2008, thereby providing all entities with well over six months in which to implement the final regulations. As discussed in the PRA analysis *infra*, the Agencies have clarified that the Red Flags Supplement is illustrative only, and is not intended to be used as a checklist. Therefore, the Agencies did not consider it necessary to alter the Red Flags listed. The FTC staff will be developing a small business compliance guide prior to the mandatory compliance deadline of November 1, 2008. The FTC staff will consider whether to include any model forms in such guide.

C. OCC and OTS Executive Order 12866 Determination

The OCC and the OTS each have independently determined that the final rule is not a "significant regulatory action" as defined in Executive Order 12866 because the annual effect on the economy is less than $100 million. Accordingly, a regulatory assessment is not required.

D. OCC and OTS Executive Order 13132 Determination

The OCC and the OTS each has determined that these final rules do not have any federalism implications for purposes of Executive Order 13132.

E. NCUA Executive Order 13132 Determination

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on State and local interests. In adherence to fundamental federalism principles, the NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5) voluntarily complies with the Executive Order. These final rules apply only to federally chartered credit unions and would not have substantial direct effects on the States, on the connection between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. The NCUA has determined that these final rules do not constitute a policy that has federalism implications for purposes of the Executive Order.

F. OCC and OTS Unfunded Mandates Reform Act of 1995 Determination

Section 202 of the Unfunded Mandates Reform Act of 1995, Public Law 104–4 (Unfunded Mandates Act) requests that an agency prepare a budgetary impact statement before promulgating a rule that includes a federal mandate that may result in expenditure by State, local, and tribal governments, in the aggregate, or by the private section, of $100 million or more in any one year. If a budgetary impact statement is required, section 205, of the Unfunded Mandates Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule.

The OCC and OTS each has determined that this rule will not result in expenditures by State, local, and tribal governments, or by the private sector, of $100 million or more. National banks and savings associations already employ a variety of measures that satisfy the requirements of the final rulemaking because, as described earlier, these are usual and customary business practices to minimize losses due to fraud, or because, as described earlier, they already comply with other existing regulations and guidance that relate to information security, authentication, identity theft, and response programs. Accordingly, neither the OCC not the OTS has prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

G. NCUA: The Treasury and General Government Appropriations Act, 1999—Assessment of Federal Regulations and Policies on Families

The NCUA has determined that these final rules will not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105–277, 112 Stat. 2681 (1998).

H. NCUA: Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) Determination

A SBREFA (Pub. L. 104–121) reporting requirement is triggered in instances where NCUA issues a final rule as defined by section 551 of the Administrative Procedure Act, 5 U.S.C. 551. NCUA has determined this final rule is not a major rule for purposes of SBREFA and the Office of Management and Budget (OMB) has concurred.

I. Plain Language

Section 722 of the Gramm-Leach-Bliley Act (12 U.S.C. 4809) requires the Federal banking agencies and the NCUA to use "plain language" in all proposed and final rules published in the **Federal Register**. The Agencies received no comments on how to make the rules easier to understand, and believe the final rules are presented in a clear and straightforward manner.

List of Subjects

12 CFR Part 41

Banks, banking, Consumer protection, National Banks, Reporting and recordkeeping requirements.

12 CFR Part 222

Banks, banking, Holding companies, state member banks.

12 CFR Part 334

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and soundness.

12 CFR Part 364

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 571

Consumer protection, Credit, Fair Credit Reporting Act, Privacy, Reporting and recordkeeping requirements, Savings associations.

12 CFR Part 717

Consumer protection, Credit unions, Fair credit reporting, Privacy, Reporting and recordkeeping requirements.

16 CFR Part 681

Fair Credit Reporting Act, Consumer reports, Consumer report users, Consumer reporting agencies, Credit, Creditors, Information furnishers, Identity theft, Trade practices.

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Office of the Comptroller of the Currency amends Part 41 of title 12, chapter I, of the Code of Federal Regulations as follows:

PART 41—FAIR CREDIT REPORTING

■ 1. The authority citation for part 41 continues to read as follows:

Authority: 12 U.S.C. 1 *et seq.*, 24 (Seventh), 93a, 481, 484, and 1818; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–3, 1681t, 1681w, Sec. 214, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Section 41.1 is added to read as follows:

§ 41.1 Purpose.

(a) *Purpose.* The purpose of this part is to establish standards for national banks regarding consumer report information. In addition, the purpose of this part is to specify the extent to which national banks may obtain, use, or share certain information. This part also contains a number of measures national banks must take to combat consumer fraud and related crimes, including identity theft.

(b) [Reserved]

■ 3. Amend § 41.3 by revising the introductory text to read as follows:

§ 41.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 4. Revise the heading for Subpart I to read as follows:

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

■ 5. Add § 41.82 to read as follows:

§ 41.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a national bank, Federal branch or agency of a foreign bank, or any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 6. Add Subpart J to part 41 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.

Subpart J—Identity Theft Red Flags

§ 41.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to a financial institution or creditor that is a national bank, Federal branch or agency of a foreign bank, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section and Appendix J, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell

phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 41.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a national bank, Federal branch or agency of a foreign bank, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 41.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendices D–I [Reserved]

■ 7. Add and reserve appendices D through I to part 41.

■ 8. Add Appendix J to part 41 to read as follows:

Appendix J to Part 41—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 41.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 41.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the

formulation and maintenance of a Program that satisfies the requirements of § 41.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 41.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 41.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 41.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Board of Governors of the Federal Reserve System

12 CFR Chapter II.

Authority and Issuance

■ For the reasons set forth in the joint preamble, part 222 of title 12, chapter II, of the Code of Federal Regulations is amended as follows:

PART 222—FAIR CREDIT REPORTING (REGULATION V)

■ 1. The authority citation for part 222 continues to read as follows:

Authority: 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–2, 1681s–3, 1681t, and 1681w; Secs. 3 and 214, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Section 222.3 is amended by revising the introductory text to read as follows:

§ 222.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. The heading for Subpart I is revised to read as follows:

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

■ 4. A new § 222.82 is added to read as follows:

§ 222.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a member bank of the Federal Reserve System (other than a national bank) and its respective operating subsidiaries, a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), commercial

lending company owned or controlled by a foreign bank, and an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 5. A new Subpart J is added to part 222 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.

Subpart J—Identity Theft Red Flags

§ 222.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to financial institutions and creditors that are member banks of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*).

(b) *Definitions.* For purposes of this section and Appendix J, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate

identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 222.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 222.90(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 222.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendices D–I [Reserved]

■ 6. Appendices D through I to part 222 are added and reserved.

■ 7. A new Appendix J is added to part 222 to read as follows:

Appendix J to Part 222—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 222.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 222.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 222.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules

implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 222.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 222.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 222.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Federal Deposit Insurance Corporation is amending 12 CFR parts 334 and 364 of title 12, Chapter III, of the Code of Federal Regulations as follows:

PART 334—FAIR CREDIT REPORTING

■ 1. The authority citation for part 334 is revised to read as follows:

Authority: 12 U.S.C. 1818, 1819 (Tenth) and 1831p–1; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–3, 1681t, 1681w, 6801 and 6805, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 334.3 by revising the introductory text to read as follows:

§ 334.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. Revise the heading for Subpart I as shown below.

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

■ 4. Add § 334.82 to read as follows:

§ 334.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency and that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 5. Add Subpart J to part 334 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.

Subpart J—Identity Theft Red Flags

§ 334.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) *Definitions.* For purposes of this section and Appendix J, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program*—(1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 334.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a

change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 334.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendices D–I [Reserved]

■ 6. Add and reserve appendices D through I to part 334.

■ 7. Add Appendix J to part 334 to read as follows:

Appendix J to Part 334—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 334.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 334.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 334.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. *Detecting Red Flags.*

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l)(31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. *Preventing and Mitigating Identity Theft.*

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. *Updating the Program.*

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 334.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the

financial institution or creditor with § 334.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

■ 8. The authority citation for part 364 is revised to read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth), 1831p–1; 15 U.S.C. 1681b, 1681s, 1681w, 6801(b), 6805(b)(1).

■ 9. Add the following sentence at the end of § 364.101(b):

§ 364.101 Standards for safety and soundness.

* * * * *

(b) * * * The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in §§ 334.90, 334.91, and Appendix J of part 334.

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Chapter V

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Office of Thrift Supervision is amending part 571 of title 12, chapter V, of the Code of Federal Regulations as follows:

PART 571—FAIR CREDIT REPORTING

■ 1. Revise the authority citation for part 571 to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, and 1881–1884; 15 U.S.C. 1681b, 1681c, 1681m, 1681s, 1681s–1, 1681t and 1681w; 15 U.S.C. 6801 and 6805; Sec. 214 Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 571.1 by revising paragraph (b)(9) and adding a new paragraph (b)(10) to read as follows:

§ 571.1 Purpose and Scope.

* * * * *

(b) *scope.*

* * * * *

(9)(i) The scope of § 571.82 of Subpart I of this part is stated in § 571.82(a) of this part.

(ii) The scope of § 571.83 of Subpart I of this part is stated in § 571.83(a) of this part.

(10)(i) The scope of § 571.90 of Subpart J of this part is stated in § 571.90(a) of this part.

(ii) The scope of § 571.91 of Subpart J of this part is stated in § 571.91(a) of this part.

■ 3. Amend § 571.3 by:

■ a. Removing paragraph (o); and

■ b. Revising the introductory text to read as follows:

§ 571.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 4. Revise the heading for Subpart I as shown below.

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

■ 5. Add § 571.82 to read as follows:

§ 571.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 6. Amend § 571.83 by:

■ a. Redesignating paragraphs (a) and (b) as paragraphs (b) and (c), respectively.

■ b. Adding a new paragraph (a) to read as follows:

§ 571.83 Disposal of consumer information.

(a) *Scope.* This section applies to savings associations whose deposits are

insured by the Federal Deposit Insurance Corporation and federal savings association operating subsidiaries in accordance with § 559.3(h)(1) of this chapter (defined as "you").

* * * * *

■ 7. Add Subpart J to part 571 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.

571.90 Duties regarding the detection, prevention, and mitigation of identity theft.

571.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

§ 571.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to a financial institution or creditor that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section and Appendix J, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 571.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a

change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 571.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendices D–I [Reserved]

■ 8. Add and reserve appendices D through I to part 571.

■ 9. Add Appendix J to part 571 to read as follows:

Appendix J to Part 571—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 571.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 571.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 571.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 571.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated

employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 571.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 571.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or

transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

National Credit Union Administration

12 CFR Chapter VII

Authority and Issuance

■ For the reasons discussed in the joint preamble, the National Credit Union Administration is amending part 717 of title 12, chapter VII, of the Code of Federal Regulations as follows:

PART 717—FAIR CREDIT REPORTING

■ 1. The authority citation for part 717 is revised to read as follows:

Authority: 12 U.S.C. 1751 *et seq.*; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–1, 1681t, 1681w, 6801 and 6805, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 717.3 by revising the introductory text to read as follows:

§ 717.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. Revise the heading for Subpart I as shown below.

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

■ 4. Add § 717.82 to read as follows:

§ 717.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is federal credit union.

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief*—(1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other member account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address*—(1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 5. Add Subpart J to part 717 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.

Subpart J—Identity Theft Red Flags

§ 717.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to a financial institution or creditor that is a federal credit union.

(b) *Definitions.* For purposes of this section and Appendix J, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a federal credit union to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A share or deposit account.

(2) The term *board of directors* refers to a federal credit union's board of directors.

(3) *Covered account* means:

(i) An account that a federal credit union offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, checking account, or share account; and

(ii) Any other account that the federal credit union offers or maintains for which there is a reasonably foreseeable risk to members or to the safety and soundness of the federal credit union from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(6) *Customer* means a member that has a covered account with a federal credit union.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the federal credit union.

(c) *Periodic Identification of Covered Accounts.* Each federal credit union must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a federal credit union must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each federal credit union that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the federal credit union and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the federal credit union offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the federal credit union;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to members and to the safety and soundness of the federal credit union from identity theft.

(e) *Administration of the Program.* Each federal credit union that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each federal credit union that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 717.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a federal credit union.

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a member who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a member's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 717.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendices D–I [Reserved]

■ 6. Add and reserve appendices D through I to part 717.

■ 7. Add Appendix J to part 717 to read as follows:

Appendix J to Part 717—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 717.90 of this part requires each federal credit union that offers or maintains one or more covered accounts, as defined in § 717.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist federal credit unions in the formulation and maintenance of a Program that satisfies the requirements of § 717.90 of this part.

I. The Program

In designing its Program, a federal credit union may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to members or to the safety and soundness of the federal credit union from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A federal credit union should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Federal credit unions should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the federal credit union has experienced;

(2) Methods of identity theft that the federal credit union has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the federal credit union.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating members, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the federal credit union has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a federal credit union should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a member's account records held by the federal credit union or a third party, or notice that a member has provided information related to a covered account held by the federal credit union to someone fraudulently claiming to represent the federal credit union or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the member;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Federal credit unions should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to members or to the safety and soundness of the federal credit union from identity theft, based on factors such as:

(a) The experiences of the federal credit union with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the federal credit union offers or maintains; and

(e) Changes in the business arrangements of the federal credit union, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the federal credit union with § 717.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the federal credit union responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the federal credit union with § 717.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the federal credit union in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a federal credit union engages a service provider to perform an activity in connection with one or more covered accounts the federal credit union should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a federal credit union could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the federal credit union, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Federal credit unions should be mindful of other related legal requirements that may be applicable, such as:

(a) Filing a Suspicious Activity Report under 31 U.S.C. 5318(g) and 12 CFR 748.1(c);

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the federal credit union detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each federal credit union may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings From a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 717.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or member presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the federal credit union, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the federal credit union. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the federal credit union. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the federal credit union. For example:

a. The address on an application is fictitious, a mail drop, or prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other members.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other members.

16. The person opening the covered account or the member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the federal credit union.

18. For federal credit unions that use challenge questions, the person opening the covered account or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The member fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account.

24. The federal credit union is notified that the member is not receiving paper account statements.

25. The federal credit union is notified of unauthorized charges or transactions in connection with a member's covered account.

Notice From Members, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Federal Credit Union

26. The federal credit union is notified by a member, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

FEDERAL TRADE COMMISSION

16 CFR Part 681

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

PART 681—IDENTITY THEFT RULES

Sec.

Authority: Pub. L. 108–159, sec. 114 and sec. 315; 15 U.S.C. 1681m(e) and 15 U.S.C. 1681c(h).

§ 681.1 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1) (users).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance

with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) *Definitions.* For purposes of this section, and Appendix A, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate.

§ 681.3 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 681.2(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 681.2 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags

that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Dated: October 5, 2007.

John C. Dugan,

Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System, October 29, 2007.

Jennifer J. Johnson,

Secretary of the Board.

Dated at Washington, DC, this 16th day of October, 2007.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

Dated: October 24, 2007.

By the Office of Thrift Supervision.

John M. Reich,

Director.

By order of the National Credit Union Administration Board, October 15, 2007.

Mary Rupp,

Secretary of the Board.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 07–5453 Filed 11–8–07; 8:45 am]

BILLING CODE 4810–33–P; 6210–01–P; 6714–01–P; 6720–01–P; 7535–01–P; 6750–01–P

EXHIBIT B

CAUSE NO. [redacted]

[redacted]	§	IN THE JUSTICE COURT
	§	
v.	§	PRECINCT 1, PLACE 2
	§	
[redacted]	§	HARRIS COUNTY, TEXAS

ANSWER - SET OFF & COUNTER-CLAIM

To the Honorable Court:

COMES NOW, defendant and counter-plaintiff herein referred to as "Defendant" and files this, Answer and Counter-Claim in the above-styled and numbered cause of action against plaintiff and counter-defendant herein referred to as "Plaintiff" and shows the Court the following:

General Denial

1. Subject to such stipulations as many hereafter be made, Defendant asserts a general denial to the allegations of Plaintiff contained under Rule 92, Texas Rules of Civil Procedure, and asks for a trial of the issues before a jury. Defendant generally denies each and every allegation in the Defendant's Counter-Claim, and demands strict proof of all such allegations.

Facts

2. Defendant incorporates the facts herein in this answer as if fully copied and set forth at length to the paragraphs mentioned below and contends that one if not all of the following occurred:

a. Plaintiff has no evidence to offer by which it can deny the allegations contained in the Defendant's Answer in this case.
b. Plaintiff has no witness to offer who can deny the allegations contained in Defendant's Answer filed in this case.
c. Plaintiff has no evidence to offer by which it can prove any of the allegations contained in the Plaintiff's Original Petition filed in this case.
d. Plaintiff has no witness to offer who can prove any of the allegations contained in the Plaintiff's Operative Petition filed in this case.
e. Plaintiff is a "debt collector" as defined by Tex. Fin. Code § 392.001(6).
f. Plaintiff's designated agent, does not have personal knowledge of the matters set forth and proper verification attached to Plaintiff's Operative Petition did occur.
g. Plaintiff's claim against Defendant includes illegal penalties disguised as liquidated damage items for various charges including, "late charges", "over-limit charges", and/or "miscellaneous charges", designed to increase the credit card interest rate.

EXHIBIT "B"

h. Prior to filing suit, the Plaintiff obtained the services of its attorney of record herein to act as its agent in Plaintiff's collection efforts against the Defendant.

i. Plaintiff's attorney is a "debt collector" as defined by 15 U.S.C.§1692a(6) and Tex. Fin. Code §392.001(6).

j. Plaintiff's attorney is a "third-party debt collector" as defined by Tex. Fin. Code §392.001(7).

k. Plaintiff's attorney is an "independent debt collector" as per Tex. Fin. Code §392.306.

l. Plaintiff's attorney filed this collection case for Plaintiff.

m. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g(a) Notice.

n. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g(a) Notice.

o. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g validation.

p. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g name and address of the original creditor.

q. The Debt Collector for Plaintiff told the Defendant that the legal collection process would continue until the Defendant entered into a repayment agreement or Plaintiff obtained a judgment.

r. The Debt Collector for Plaintiff told the Defendant that the judgment could result in a lien placed against his home.

s. Plaintiff's designated agent, did not review any documents either before, or at the time, he or she signed the statement attached to Plaintiff's Operative Petition.

t. Plaintiff employed a debt collector for Plaintiff.

u. The Debt Collector for Plaintiff spoke to Defendant on the telephone.

v. The Debt Collector for Plaintiff told the Defendant that the judgment could result in a lien placed against his car.

w. The Debt Collector for Plaintiff told the Defendant that the judgment could result in a wage garnishment.

x. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g validation.

y. Plaintiff did not send defendant 15 U.S.C. § 1692g name and address of the original creditor.

z. The Debt Collector for Plaintiff told the Defendant that Plaintiff could satisfy a judgment from any asset Defendant has.

aa. In violation of Tex. Fin. Code 392.301(a)(8), the Plaintiff threatened to take an action prohibited by law.

bb. In violation of Tex. Fin. Code 392.301(a)(8), the Plaintiff misrepresented the character of a consumer debt.

cc. Defendant's home is not an asset available to Plaintiff to satisfy a potential judgment in this case.

dd. Defendant's car is not an asset available to Plaintiff to satisfy a potential judgment in this case.

ee. The Debt Collector for Plaintiff made misrepresentations to the Defendant.

ff. Wage garnishment is not available to Plaintiff regarding its claim against Defendant.

gg. In violation of 15 U.S.C. § 1692d, the Plaintiff engaged in conduct the natural consequence of which was to harass, oppress, or abuse a person in connection with the collection of a debt.

hh. In violation of 15 U.S.C. § 1692e, U.S.C. § 1692e(2)(A) and (B), U.S.C § 1692e(4), U.S.C. § 1692e(5) and U.S.C. § 1692e(10) and the "least sophisticated consumer standard," the Plaintiff used objectively false representations and/or false, deceptive, or misleading representations or means in connection with the collection of a consumer debt.

ii. Plaintiff failed to conduct an investigation of any dispute asserted by the Defendant.

jj. Plaintiff failed to admit, deny, or otherwise act on any dispute asserted by the Defendant.

kk. Plaintiff failed to furnish Defendant with any consumer forms for giving a Tex. Fin. Code § 392.202 notice.

ll. Plaintiff failed to furnish Defendant with any assistance in preparing a Tex. Fin. Code § 392.202 Notice.

mm. Plaintiff has no written agreement with the Defendant.

nn. Plaintiff has no agreement bearing the Defendant's signature.

oo. Plaintiff maintains an employment file on the Debt Collector who telephoned the Defendant.

pp. Plaintiff's attorney is engaged directly or indirectly in consumer debt collection (any action, conduct or practice in collecting debts alleged to be created by an individual primarily for personal, family, or household purposes).

qq. Plaintiff's attorney has regularly collected or attempted to collect, directly or indirectly, consumer debts owed or due or asserted to be owed or due another.

rr. Plaintiff's attorney was required to obtain a debt collector's bond and file a copy thereof with the Texas Secretary of State.

ss. The Plaintiff was required to obtain a debt collector's bond and file a copy thereof with the Texas Secretary of State.

tt. The Defendant notified Plaintiff's attorney and/or the Plaintiff that the Debt was disputed by the Defendant.

uu. After the Defendant notified Plaintiff's attorney and/or the Plaintiff that the Debt was disputed by the defendant, the Plaintiff and/or Plaintiff's attorney continued to report the Debt to consumer credit reporting bureaus.

vv. The Plaintiff and/or its attorney(ies) never reported to any consumer credit reporting bureau that the Debt was being disputed by the Defendant.

ww. The Plaintiff's claim against Defendant is barred by limitations.

xx. Plaintiff never sent the Defendant any validation for the amount due on the Debt.

yy. Plaintiff never satisfied any 15 U.S.C. § 1692g(b) request made by the Defendant.

zz. Plaintiff failed to supervise, its agents, debt collectors, attorney and assigns..."

Unconscionable Acts

2. In so doing, plaintiff acted with knowledge, actual or constructive, of the facts, and with the intent to induce Plaintiff to act on the false representation/concealment of material facts. Defendant was without knowledge of the facts, and had no means of obtaining knowledge of the facts to Defendant's detriment and damage.

Additional Answer

A. For further answer, if such be necessary, Defendant further alleges that Plaintiff's claims are barred by the applicable statutes of limitation.

B. For further answer, if such be necessary, Defendant further alleges that Plaintiff's claims are barred by the statute of frauds.

C. For further answer, if such be necessary, Defendant specially denies each and every item in Plaintiff's account, which is the basis of Plaintiff's action, and demands strict proof of all items in the account.

D. For further answer, if such be necessary, Defendant would show that all of Plaintiff's allegations alleging a contract are barred by lack of consideration or failure of consideration and that the consideration has failed in whole or in part.

E. For further answer, if such be necessary, Defendant would show that all conditions precedent for Plaintiffs to maintain this action or recover herein have not been performed and /or have not occurred.

F. Defendant pleads hearsay and the parole evidence rule in bar to all claims predicated on any alleged agreement, intention or representation of, by or between the parties not specifically in a written contract signed by the Defendant.

G. Defendant pleads that the Plaintiff is not entitled to recover in the capacity in which it sues.

H. Defendant pleads that a contract sued upon, to the extent any contract exists, is usurious.

I. Defendant is excused form performance because of Plaintiff's breach(s) of contract.

J. The contract is one of adhesion and takes advantage to a grossly unfair degree in violation of the Texas Deceptive Trade Practices Act 17.50 et. seq. and needs to be reformed or cancelled.

K. The provisions requiring the payment of fees and/or permitting the retention of fees are invalid and void. These provisions are a penalty designed to punish rather than an attempt to estimate damages. The amounts specified in the agreement are not reasonable compensation for the harm caused by the breach. Further, the amounts stated was not, at the time of contracting, a reasonable estimate of the damages that would result from a breach. The fees are not limited to reasonable administrative costs of carrying the account. Said fees are not utilized to ensure performance of the account or reimburse Plaintiff for expenses on the account. The Plaintiff knew or should have known that the fees are excessive and bore no reasonable relationship to the costs incurred or damages sustained.

L. Equitable Estoppel, Fraud, and Promissory Estoppel as the Plaintiff made false and misleading representations and promises that it knew or should have foreseen would have been relied upon by the Defendant. Defendant relied upon the false and misleading representations and promises and by so doing was harmed.

M. Notice was not given as alleged. With respect to the alleged agreement, including changes and modifications of the alleged agreement. Even had notice had been given as alleged the Plaintiff failed to demand a proper amount that was owed and due.

N. Defendant denies that agreement that Plaintiff contends is applicable is genuine.

O. Plaintiff has dirty hands via bad faith collection practices both prior to and during this lawsuit that would preclude the recovery of an equitable Relief including but not limited to it's claim for unjust enrichment.

P. Mutual Mistake of Fact as to the terms of the alleged agreement.

Q. Reformation of the Agreement.

R. Cancellation or Recession of the Contract.

S. Contract is Illusory given the Plaintiff's unilateral rights to change same.

T. Plaintiff is conduct precludes it from recovering on the basis of its claims in this action. On all times relevant herein, Plaintiff made false representations to and concealed material facts from Defendant. In so doing, Plaintiff acted with knowledge, actual or constructive, of the facts, and with the intent that Defendant act on the false representation/concealment of material facts. Defendant was without knowledge of the facts, and had no means of obtaining knowledge of the facts. To Defendant's detriment, she relied on Plaintiff's false representation/concealment of material facts when she entered into the transaction(s) made the basis of this suit to her detriment and damage.

Acts and Omissions

3. Acts and omissions may include and are not limited to one if not all of the following:

1) Unlawful Due Date Manipulation.
2) Illegal Late Fees.
3) Illegal Over Limit Fees.
4) Hidden Fee.
5) Illegal Interest Rates.
6) Illegal Collection tactics.
7) Illegal Insurance Charges.
8) Increasing Fees without requisite notice.
9) Breach of its own agreement with cardholders, including but not limited notice and modification.
10) Only one payment missed and interest is increased exponentially, regardless of prior payment history.
11) Misrepresenting that a debtor will never have credit with Defendant again and then sending another card although the prior account was charged off.
12) Manipulating the minimum payment, by lowering said payment such that people will be paying interest on a higher balance.
13) Manipulating the public through advertising and sales techniques to obtain credit card accounts.
14) Baiting cardholders with 0% APR or the like. However, given the fine print of the offer to actually obtain said rate is not likely.
15) Utilizing vast data basis to manipulate the public through actuary tables.
16) Plaintiff has employed a systematic collection process that is designed to trick and/or trap the debtor into a procedural or technical default. Plaintiff forwards its' discovery, especially admissions, in a stealth manner attached to a petition.
17) Plaintiff has intentionally and/or recklessly failed to be certain that the cardholder is provided a copy of the agreement.
18) The contract contains hidden clauses and is not conspicuous.
19) Plaintiff has intentionally included provisions such as universal default to profit.
20) Plaintiff has raised interest rates and fees astronomically.

21) Plaintiff should not be allowed to change the rate for items that have already been purchased or cash already advanced.
22) The late fees are not a reasonable assessment of the risk for collection.
23) Plaintiff sets due dates on weekends and holidays to increase potential for a late payment to occur.
24) Plaintiff fails to timely post checks that result in an increase in fees.
25) Plaintiff would hold payments to trigger late fees and over limit fees
26) Failing to properly report to credit agencies.
27) Arbitrarily and capriciously approving or declining charges to create fee revenues.
28) Failing to work with the cardholder prior to suit and making it impossible to discuss and/or work out a dispute.
29) Failing to provide the requisite back up documentation for a debt when it is disputed or at all.
30) Failing to disclose how long the minimum monthly payment will take for a person to pay off a bill.
31) Recklessly disregarding the veracity of testimony with respect to the execution of affidavits pertaining to litigation and/or the debtor's file.
32) Arbitrarily and capriciously determining when to charge off an account.
33) Brining suits for specific performance although Plaintiff has elected to cease performance and has sued on breach.
34) Bringing suits for benefit of the bargain damages although Plaintiff has ceased performance.
35) Plaintiff has sought increased damages from predatory and excessive collections practices.
37) Plaintiff has failed to establish the requisite elements of contract formation have occurred.
38) Plaintiff has filed evidence and alleged trustworthy and inaccurate documents with, at best, a reckless disregard for their authenticity and veracity.
39) Plaintiff had not even provided the background data to ascertain even Plaintiff accurately followed it's own formula to calculate the amount due.
41) The evidence provided if any, are individual transactions that are published to the community without any method to avoid nondisclosure to disinterested parties in invasion of Defendant's privacy rights.
43) Making affidavits in bad faith as summary judgment proof in contravention of 166a(h) as summary judgment proof.
44) Making business records affidavits in bad faith as trial proof.
45) Not including the entire agreement with its proof, i.e. the card carrier, attached letter or accompanying letter or other relevant information that makes up the agreement required to complete it..
47) Unilateral right to amend the alleged agreements makes it illusory.
48) Charging the account and not sending the billing statement.

Acts of Agent Imputed to Principal

4. Whenever it is alleged in this petition that Plaintiff did any act or thing or failed to do any act or thing, it is meant that the officers, agents, successors, predecessors or employees of defendant respectively performed, participated in, or failed to perform the acts or things alleged while in the course or scope of employment or agency relationship

with said Plaintiff. The acts and/or omissions set forth herein taken singularly or in combination, constitute a producing and/or proximate cause of damages sustained by Defendant as a proximate cause of said acts and omissions.

Alleged Agreement Cancelled-Reformed

5. Defendant requests that the alleged agreements be cancelled or reformed to comply with the law. Plaintiff has taken advantage of Defendant to a grossly unfair degree and the alleged agreement should either be cancelled or reformed to a fair one.

Plaintiff Violated the DTPA

6. Deceptive Trade Practices Act (DTPA) is designed to protect consumers from any deceptive trade practice made in connection with the purchase or lease of any goods or services and, to such end, the DTPA must be given its most comprehensive application without doing any violence to its terms. Bus & C §§17.41 et seq. *Vinson & Elkins v Moran* (Tex App Hous. (14 Dist.), Mar 27, 1997) 946 SW2d 381, rehearing overruled (Jun 12, 1997), rule 130(d) motion filed (Jun 20, 1997).

7. In determining whether an act is actionable under the Deceptive Trade Practices--Consumer Protection Act (DTPA), question is whether the deceptive trade act or practice was committed in connection with a transaction(s) in goods or services. Bus & Com C §17.50(a). *Bekins Moving & Storage Co. v. Williams,* 947 S.W.2d 568 (Tex. App. Texarkana 1997), reh'g overruled, (May 28, 1997). "Consumer" status under the Deceptive Trade Practices Act (DTPA) is defined by the plaintiff's relationship to the goods or services, not by his relationship to his opponent. Bus & Com C §17.45(4). Moritz v. Bueche, 980 S.W.2d 849 (Tex. App. San Antonio 1998).

8. Consumers are a consumer and the transaction made the basis of Plaintiff's suit is actionable under the DTPA. Several, if not all of the fees or interest charged by Plaintiff are excessive penalties. They bear no relation to the damages sustained or costs for said services and are clearly unconscionable. Unconscionability under the Deceptive Trade Practices Act (DTPA) is an objective standard for which scienter is irrelevant. Bus & Com C §§17.45(4), 17.50(a). *Insurance Co. of North America v. Morris,* 981 S.W.2d 667 (Tex. 1998). Generally, an act is "false," "misleading," or "deceptive" under Deceptive Trade Practices—Consumer Protection Act (DTPA), if it has the capacity to

deceive an ignorant, unthinking, or credulous person. Bus & Com C §17.50(a)(1). *Bekins Moving & Storage Co. v. Williams*, 947 S.W.2d 568 (Tex. App. Texarkana 1997), reh'g overruled, (May 28, 1997).

9. A finding of unconscionable action must be found if either (1) the consumers took advantage of consumer's lack of knowledge to grossly unfair degree, with resulting unfairness that was glaringly noticeable, flagrant, complete, and unmitigated, or (2) there was gross (glaring and flagrant) disparity between value received and consideration paid. *Brown v. Galleria Area Ford, Inc.*, 752 S.W.2d 114, 116 (Tex. 1988)--decided under prior version of statute.

Plaintiff's Breached the Alleged Agreement

10. The agreement Plaintiff, has alleged is applicable in the past, reads in relevant part that Plaintiff must notify Consumers in writing of an increase in fees. Plaintiff has failed to provide the written notice on numerous occasions. Such failure has deprived Consumers of an opportunity to contest the change as per the alleged agreement.

Plaintiff Increased Fees Prior to the Effect Date of a Change

11. Plaintiff is also implementing the increase at least one month prior to its' right to as per the alleged agreement. Specifically, said agreement requires a moratorium of the fee increase for at least one billing period. Contrary, to said agreement Plaintiff has assessed all increases immediately. In fact, the only notice, if any, was provided through charging the account at a higher rate.

Plaintiff Failed to Document & Authenticate its Claims

12. Plaintiff has failed to produce alleged agreements or the back-up data for any transactions that occurred. Plaintiff has only provided summaries Consumers therefore are unable to audit the account for accuracy. Plaintiff has incomplete agreements. Without all the agreements used by the Plaintiff, the Consumers cannot ascertain or audit

Plaintiff's compliance with the agreement. Plaintiff has also failed to provide any of the back up documentation to authorize it to charge certain service fees.

Course of Deceptive Conduct with Amending and Changing the Agreement

13. The alleged account agreements were amended at will to include charges that defendant never agreed too and terms that also are denied as agreed. The amendments were confusing and occurred randomly and deceptively.

Pleadings are in the Alternative

14. All matters are plead whenever required in the alternative and Defendant reserves the right to election when appropriate.

PRAYER

WHEREFORE, DEFENDANT, prays that **PLAINTIFF** take nothing by its suit; and for all such further relief to which he may be justly entitled.

WHEREFORE, DEFENDANT further requests that **PLAINTIFF** be cited to appear and answer, and that on final trial, **DEFENDANT** have judgment against **PLAINTIFF** as for all lawful and appropriate remedies as follows:

1. General damages in a sum within the jurisdictional limits of the Court.
2. Special damages for a sum within the jurisdictional limits of the Court.
3. Prejudgment interest as provided by law.
4. Attorney's fees. Including but not limited to attorney fees and all costs of appeal.
5. Postjudgment interest as provided by law.
6. Costs of suit.
7. Exemplary damages.
8. All lawful and appropriate penalties and damage provisions either statutory or at the common law.
9. That the alleged account agreement is cancelled or reformed to meet the true intentions of the parties.
10. Such other and further relief to which Defendant may be justly entitled.

/s/

CAUSE NO. [redacted]

[redacted]	§	IN THE JUSTICE COURT
	§	
v.	§	PRECINCT 1, PLACE 2
	§	
[redacted]	§	HARRIS COUNTY, TEXAS

DEFENDANT'S COMBINED DISCOVERY

TO: Plaintiff, by and through its attorney.

Defendant serves these Interrogatories as allowed by Texas Rule of Civil Procedure 197. Plaintiff must produce all requested documents (as they are kept in the ordinary course of business or organized and labeled to correspond with categories in each request) for inspection and copying, and respond to these interrogatories not more than 30 days after service at the office of Defendant's counsel.

Defendant serves this Request for Production on Plaintiff in exhibit "a" as allowed by Texas Rule of Civil Procedure 196. Plaintiff must produce all requested documents (as they are kept in the ordinary course of business or organized and labeled to correspond with categories in each request) for inspection and copying, not more than 30 days after service at the office of Defendant's lead counsel.

Defendant serves these Admission Requests on Plaintiff as allowed by Texas Rule of Civil Procedure 198. Plaintiff must admit or deny each request, in writing, and respond to these requests not more than 30 days after service at the office of Defendant's counsel.

Defendant serves this 194 Request and pursuant to the Texas Rule of Civil Procedure Plaintiff must provide responses to the disclosure not more that 30 days after the service of this request at the office of Defendant's counsel

EXHIBIT "A"

DEFINITIONS AND INSTRUCTIONS

1. Pursuant to TEX. R. CIV. P., you are requested to separately number each item which will be produced pursuant to this Request with a separate and distinct number or similar identifying designation, and to file your written response to this Request stating, with regard to each Request, the identification or exhibit numbers of the specific items being produced in response to each such Request. Items which are required to be produced in response to more than one Request may be listed by number in response to each such Request, but the item itself need only be produced one time. All items to be produced are to be forwarded to the undersigned attorney for the Defendant attached to or together with your written response.

2. Discovery extends to materials in either your possession or in your constructive possession; constructive possession exists as long as you have a superior right to compel the production from a third party (including an agency, authority or representative) who has possession, custody or control, even though you do not have actual physical possession. A party may not evade discovery requests by answering that he does not know or does not have the information requested when, by resorting to means available to him, he can ascertain the facts inquired about. *Watson v. Godwin*, 425 S.W.2d 424 (Tex.Civ.App. - Amarillo 1968, writ ref'd n.r.e.); *McPeak v. Texas Dept. of Public Safety*, 346 S.W.2d 138 (Tex.Civ.App. - Dallas 1961).

3. With regard to any Request for to which you object on the ground that the item is overly broad, or is not properly limited in some way, you are requested to state in your answer or objection:

> (a) What categories of information, if any, you do not object to providing, and to provide such information in your answers to this document.
>
> (b) What categories of information are in existence that you do object to providing, and the reason why you claim that such information or categories of information is not calculated to lead to the discovery of evidence relevant to this case.

4. With regard to any Requests to which you object on the ground of attorney-client privilege, work-product privilege or some other privilege or exemption from discovery, you are requested to identify specifically each item which is in existence to which such objection applies, to state the specific legal objection to such discovery, and to state the specific facts which you claim support such legal objection.

5. It is not proper ground for objection to discovery that materials are claimed to be "confidential", "proprietary", or a "trade secret". *Jampole v. Touchy*, 673 S.W.2d 569 (Tex. 1984). With regard to any such documents, please be advised that Defendant's counsel will be willing to make agreements with you not to disclose such documents to

competitors, and is willing to make such arrangements immediately so as not to delay production of such documents. If such arrangements are needed, please contact this office immediately, and sufficiently far in advance of the discovery deadline to allow such arrangements to be finalized.

6. "**Person**" means any natural person, corporation, proprietorship, partnership, professional corporation, joint venture, association, group, governmental agency or agent, whether foreign or domestic.

7. "**You**", "**your**", "**Plaintiff**" or "Plaintiffs" means and refers to the Plaintiff, in this suit, and all employees, agents, independent contractors, predecessors, successors or representatives of the Plaintiff.

8. "**Defendant's Name**" means and refers to Defendant, the Defendant in the above styled and numbered cause.

9. "**Documents**" incorporates the definition of **document** in TEX.R.CIV.P. 192.3(b), i.e., including papers, books, accounts, drawings, graphs, charts, photographs, electronic or videotape recordings, and any other data compilations from which information can be obtained and translated by you into reasonably usable form. It also refers to any medium by which information is reported, including papers of any kind or character, photographs in any method or medium by which information is utilized or generated by computers. **Document** is used in its broadest sense and includes any original, reproduction or copy of any kind, typed, recorded, graphic, printed, written or documentary matter, including without limitation correspondence, memoranda, interoffice communications, notes, diaries, contracts, documents, drawings, plans, specifications, estimates, vouchers, permits, written ordinances, minutes of meetings, invoices, billings, checks, reports, studies, telegrams, notes of telephone conversations, and notes of any and all communications, and every other means of recording any tangible thing, any form of communications, or representations including letters, words, pictures, sounds or symbols, or combinations thereof. The scope of this request is with respect to documents and information that evidence the right to collect all dollar amounts sought in the suit herein, charged to the account herein and applicable agreements in place from the inception of the account. This request also includes only documentation reasonably calculated to lead to the discovery of admissible evidence in this cause.

10. "**Account**" shall mean the account(s) made the basis of Plaintiff's suit. If more than one account is involved then the term account shall refer to each individual account and the response to these requests requires that you identify the account and the applicable response.

11. "**Request for Privilege Log**" Defendant requests that Plaintiff supply a privilege log, if applicable, if said log upon request is required for any of the responses.

12. "**Identify,**" when used with reference to a person (which includes natural persons, partnerships, corporations, and other legal entities), means to state that

person's full name, last known residence or business address, and telephone number; and(b) **"Identify"**, when used with reference to a document, means to state the document's signor or signors, the addressee or addressees, the date of the document, the author of the document, a reasonably detailed description of its contents, and the person currently having custody and control of said document. In lieu of identifying all such documents, and provided that you will do so without a formal motion to produce under Rule 167, you may attach copies thereof to your answers to these requests..

13. Your failure to respond, as required by the Texas Rules of Civil Procedure, to these requests within the time required may result in the entry of a judgment against you, the assessment of additional attorney's fees against you, or other sanctions of the Court as provided in Rule 215.

I. INTERROGATORIES - INSTRUCTIONS AND DEFINITIONS

YOU ARE INSTRUCTED THAT:

1. Each interrogatory must be answered separately and fully, in writing, under oath, on the basis of all information available to you.

2. Each answer must be preceded by the interrogatory to which it pertains.

3. The answers must be signed and verified by the person making them and must be submitted to the undersigned no later than thirty (30) days after your receipt of petition and citation. The provisions of Rule 14 shall not apply.

4. According to the provisions of the TRCP, each interrogatory is continuing in nature so as to require supplementary answers if you or your attorney should obtain information that (a) the answer was incorrect when made, or (b) though correct when made, the answers becomes no longer true, or (c) if you expect to call an expert witness whose name has not been previously disclosed in response to an appropriate interrogatory.

5. If you are held or are sued in more than one capacity or if your answers would be different if sued in any different capacity, such as a partner, agent, corporate officer or director, or the like, then you are requested to answer separately in each capacity.

6. Your failure to respond, as required by the Texas Rules of Civil Procedure, to these interrogatories within the time required may result in the entry of a judgment against you, the assessment of additional attorney's fees against you, or other sanctions of the Court as provided in Rule 215.

II. REQUEST FOR PRODUCTION - DEFINITIONS

For the purposes of the request for production of documents, the following definitions shall apply:

A. You: "You" or "Your" shall mean, Plaintiff and any of its representatives, agents, successors in interest, assigns, and any other persons or entitled acting or purporting to act on behalf of said Plaintiff, whether as alter ego or otherwise.

B. Plaintiff(s): "Plaintiff" or "Plaintiffs" shall mean the party seeking recovery in this action for the alleged account sought.

C. Defendant(s): "Defendant" and each person and/or entity acting or purporting to act on its behalf.

D. And: "And," as well as "or", shall be construed either disjunctively or conjunctively as necessary to bring within the scope of this notice documents that might otherwise be construed to be outside its scope; and as used herein, the singular shall include the plural and the plural shall include the singular, except as the context may otherwise require.

E. Document(s): "Document" or "documents" shall mean and include all matters within the scope of the Texas Rules of Civil Procedure. Specifically, Plaintiff may obtain discovery of the existence, description, nature, custody, condition, location and contents of any and all documents (including papers, books, accounts, drawings, graphs, charts, photographs, electronic or video tape recordings and any other data compilations from which information can be obtained and translated, if necessary, by Plaintiff into reasonably usable form) and any other tangible things which contain matters relevant to the subject matter of this action.

F. Possession, Custody, or Control: The terms "possession, custody, or control" as used herein shall mean documents actually within the possession, custody or control of the witness and each consultant, agent, employee, officer, director, partner, and representative (including, without limitation, attorneys and accountants) of the witness or each former employee of the witness or each other person acting or in

concert with them, and include documents which were prepared by, obtained, or placed in the possession, custody, or control of any such person within the scope of his duties or relationship to the witness or documents which the witness has a right to copy or have access to, and documents which have been placed in the temporary possession, custody, or control of any third party by any of the foregoing persons within limitation of the terms "Possession, Custody, or Control" as used in the preceding sentence, a document is deemed to be in your POSSESSION, CUSTODY, OR CONTROL if you have the right to secure the document or a photocopy thereof from another person, another entity, whether public or private, having actual physical possession, custody, or control thereof.

G.Communications: "Communication(s)" shall mean and include all letters, telegrams, telexes, cables, telephone conversations, and records and notations made in connection therewith, notes, memoranda of conversations, sound recordings, magnetic tapes or other written, reported, recorded, or graphic matter relating to any exchange of information between you and the Plaintiff, you and the Defendant, or between the Plaintiff and the Defendant, any other person or entity, and further including any "document" described above relating to such communications.

III. ADMISSIONS-INSTRUCTIONS AND DEFINITIONS

You are hereby instructed that the aforementioned definitions in the previous instructions shall apply to the admission requests. The admissions requests are due within thirty (30) days after service.

Defendant requests that answers to these discovery requests contain separate responses should said answer be different with respect to the particular date of the incident, vehicle and operator. Please indicate in your response said differences, otherwise, we will assume that your answer is the same with respect to the incident, vehicle and operator.

IV. GENERAL INSTRUCTIONS

If any discovery request herein CANNOT BE ANSWERED, because a particular word or phrase needs further definition, please contact the undersigned in writing.

EXHIBIT "A" INTERROGATORIES

1. This interrogatory pertains to all fees charged to the account and sought collected only, including but not limited to the following fees:

a) "Membership Fee";
b) "Transaction Fee for Balance Transfers";
c) "Transaction Fee for Cash Advances";
d) "Minimum Finance Charge";
e) "Minimum Amount Due";
f) "Annual Percentage Rate of Purchases";
g) "Annual Percentage Rate of Cash Advances";
h) "Variable Percentage Rate for Purchases and Cash Advances";
i) "Over the Credit Limit Fee";
j) "Credit Shield Premium";
k) "Late Fee";
l) "Credit Protector"
m) "Interest" and
j) All other charges you contend could be charged to this account.

State the name of the fee and fee (in dollars or percentage whichever is applicable) that may be assessed an individual and how said fee was calculated at the inception of Defendant's account, how Defendant was notified as to the amount of the fee, changes thereto and identify any changes to said fee and the effective date of said change.

If there have been any changes in the fee charged from the inception of Defendant's account to present, please identify how said change in the methodology to change the fee and how Defendant was notified of the change and the basis, if any, for determining the amount of time that subscribers would be given from the date of notification of a change to the effective date of the change.

Please state how the collection of a particular fee is characterized for both your internal and external accounting. (For example, when a late fee is collected, is the amount of money characterized as income, a counter-expense, and/or etc.)

Identify all documents that support your response(s) to this request.

This request is limited to all charges that are contended owed and due that are included in the alleged amount owed and due sought in this suit..

ANSWER:

2. Identify each person answering these interrogatories, supplying information, or assisting in any way with the preparation of the answers to these interrogatories. Identify all documents that support your response(s) to this request.

ANSWER:

3. If you contend there was consideration for the credit account(s) upon which Plaintiff sues, state the factual basis for your contention. Identify all documents that support your response(s) to this request.

ANSWER:

4. If you contend Defendant did not perform his contractual obligations, state the factual basis for your contention. Identify all documents that support your response(s) to this request.

ANSWER:

5. If you contend that you performed all conditions precedent or that all conditions precedent necessary to file suit occurred, state the factual basis for your contention. Identify all documents that support your response(s) to this request.

ANSWER:

6. Please state the date on which the Defendant first made an application for account nos. made the basis of this suit with your company. Identify all documents that support your response(s) to this request.

ANSWER:

7. On what date was this account approved? Identify all documents that support your response(s) to this request.

ANSWER:

8. What are the names, addresses and job titles of the employees of Plaintiff, who handled the transaction in question? Identify all documents that support your response(s) to this request.

ANSWER:

9. Please supply the names of all firms from whom credit information is normally obtained by Plaintiff, before approving any credit application. Identify all documents that support your response(s) to this request.

ANSWER:

10. Please supply the names of all firms from whom credit information was obtained by Plaintiff before approving Defendant's account. Identify all documents that support your response(s) to this request.

ANSWER:

11. Please supply the names of all firms from whom credit information was forwarded by Plaintiff pertaining to Defendant's account. Identify all documents that support your response(s) to this request.

ANSWER:

12. Please list all goods and services that Plaintiff alleges were purchased on Account made the basis of this suit from the inception of said account(s). Identify all documents that support your response(s) to this request.

ANSWER:

13. Explain in detail, each step in the origination of defendant's credit card account. Include in your answer the process by which plaintiff's general ledger accounting records are changed to reflect the origination of a credit card account.

ANSWER:

14. Explain in detail, each step in the origination of defendant's credit card account. Include in your answer the process by which plaintiff's general ledger accounting records are changed to reflect the origination of a credit card account.

ANSWER:

15. Please state whether the interest of the originator of the disputed account has been sold, transferred or conveyed since its inception and origination?

ANSWER:

16. Please state whether the disputed account is automatically insured against fraudulent use, or must the card holder pay a premium for such protection?

ANSWER:

17. If the answer to the previous question is that the card holder must pay a premium for the insurance, is the premium included in the minimum payment amount, interest payment or annual "membership" fee?

ANSWER:

18. Is the disputed account automatically insured against default, or must the card holder pay a premium for such protection?

ANSWER:

19. If the answer to the previous question is that the card holder must pay a premium for the insurance, is the premium included in the minimum payment amount, interest payment or annual "membership" fee?

ANSWER:

20. Specify the name and function of the computer systems and software used by plaintiff in the production of billing statements and statements of account for the account that is the subject of this cause of action.

ANSWER:

21. Specify the name and function of the computer systems and software used by plaintiff to record and report financial accounting information for the account that is the subject of this cause of action, for purposes of compliance with the Sarbanes-Oxley Act of 2002.

ANSWER:

22. State whether the named plaintiff loaned credit to defendant in the disputed account.

ANSWER:

23. Please list any changes plaintiff made to the interest rate charged to the disputed account, during the life of the account.

ANSWER:

24. Please list any changes made to the fees charged to the disputed account, during the life of the account.

ANSWER:

25. Please list any changes made to the penalties charged to the disputed account, during the life of the account.

ANSWER:

26. Identify all discoverable documents reviewed to execute any affidavit in this cause.

EXHIBIT "A" INTERROGATORY PRODUCTION REQUEST

1. All documents identified in the prior interrogatory requests.

ANSWER:

EXHIBIT "A" PRODUCTION REQUEST

1) All written agreements that pertain to the account. Including but not limited to the any account applications, account agreements, changes to agreements, notice of changes, electronic account notices.

2) All statements of account sought.

3) All written notification or change in terms of the account pertaining to the agreement.

4) All written late fee changes, over the credit limit fee changes, interest changes or other written changes pertaining to fees that can be charged to the account and the amount of said fee that can be charged.

5) All written changes to the agreements.

6) All card carrier agreements pertaining to the account.

7) Written proof for the receipt of documents forwarded to Defendant by Plaintiff.

8) All electronic phone logs and diary logs that pertain to the account.

9) The written record retention policy as to how records pertaining to the account are to be maintained by Plaintiff.

10) Call logs, electronic file notes and other electronic entries that were recorded that evidence account activity or relate to the account.

11) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you in your decision to charge the following fees:

a) "Membership Fee";
b) "Transaction Fee for Balance Transfers";
c) "Transaction Fee for Cash Advances";
d) "Minimum Finance Charge";
e) "Minimum Amount Due";
f) "Annual Percentage Rate of Purchases";
g) "Annual Percentage Rate of Cash Advances";
h) "Variable Percentage Rate for Purchases and Cash Advances";
i) "Over the Credit Limit Fee";
j) "Credit Shield Premium";
k) "Late Fee";
l) "Creditor Protector" and
m) all other charges you contend could be charged to this account.

This request is limited to fees charged the account.

12) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you to formulate the provision in the agreement for the following fees:

a) "Membership Fee";
b) "Transaction Fee for Balance Transfers";
c) "Transaction Fee for Cash Advances";
d) "Minimum Finance Charge";
e) "Minimum Amount Due";
f) "Annual Percentage Rate of Purchases";
g) "Annual Percentage Rate of Cash Advances";
h) "Variable Percentage Rate for Purchases and Cash Advances";
i) "Over the Credit Limit Fee";
j) "Credit Shield Premium";
k) "Late Fee";
l) "Creditor protector" and
m) all other charges you contend could be charged to this account.

This request is limited to fees charged the account and alleged owed and due herein.

13) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you to determine the amount charged for the following fees:

a) "Membership Fee";
b) "Transaction Fee for Balance Transfers";

c) "Transaction Fee for Cash Advances";
d) "Minimum Finance Charge";
e) "Minimum Amount Due";
f) "Annual Percentage Rate of Purchases";
g) "Annual Percentage Rate of Cash Advances";
h) "Variable Percentage Rate for Purchases and Cash Advances";
i) "Over the Credit Limit Fee";
j) "Credit Shield Premium";
k) "Late Fee";
l) "Credit Protector" and
m) all other charges you contend could be charged to this account.

This request is limited to fees charged the account and alleged owed and due herein.

14) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you in your decision to charge the interest rate charged for cash advances.

15) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you in your decision to charge interest for and amount charged for purchases.

16) Any documents, surveys, cost studies, or other documents as defined by the TRCP utilized by you in your decision to charge the interest rate charged for the default rate.

17) All documents that evidence Plaintiff is owner of the account(s) that it seeks to collect.

18) All documentary records reviewed by any witness that has testified in this cause.

19) All letters for any type forwarded by Plaintiff to Defendant from the inception of the account to the present time.

20) All demand for payment and/or demand letters of any kind from Plaintiff to Defendant from the inception of the account to present time.

21) All documents and records of any kind (which are not attorney work product) that prove or tend to prove the time spent by your attorney in representing you in connection with the matters at issue in the above styled and numbered cause (both before and after the lawsuit was filed), including but not being limited to, invoices, billings, and/or computer records which reflect all of the work performed by your attorney for the above styled and numbered cause.

22) The Power of Attorney and any other contracts between you and your attorney for representation of you in your claims against Defendant.

23) All account agreements between Plaintiff and Defendant that bear the signature of Defendant.

24) All documents propounded by Plaintiff to Defendant, which inform Defendant of the right to reject the terms of a proposed change to any account agreement with Plaintiff.

25) All notices of changes in the terms of the credit card arrangement or changes in interest rate sent by Plaintiff to Defendant.

26) Any and all documents that reflect written notice as per the "Changing This Agreement" paragraph of the agreement you allege is applicable herein.

27) In the "Changing this Agreement" section of the agreement you contend is applicable states "However if we cause a fee, rate or minimum payment to increase, we will mail you written notice at least 15 days before the beginning of the billing period in which the changes becomes effective", please provide all written notice that you contend was forwarded as per the "Changing this Agreement" section of said agreement.

28) All manuals, training materials, and similar documents used in training, overseeing, or supervising of your personnel and your agents retained to inform cardholders of the initial agreement and any subsequent changes thereto.

29) All manuals, training materials, and similar documents used in training, overseeing, or supervising of your collections handling personnel and your agents retained to collect accounts such as the one made the basis of this suit.

30) All "Electronic or Magnetic Data" as per TRCP 196.4 on a CD or Floppy Disc in Microsoft Word that exits including but not limited to any and all discovery requested by Defendant, all of Plaintiff's Instruments filed in this cause and all of Plaintiff's discovery forwarded and responded in this cause.

31) A printout of all computerized notes that you maintain that pertains to the account. You may redact privileged information, this request includes and is not limited to the collection notes, account notes, telephone calls, and all other electronic entries that are maintained.

32) All written documents that were forwarded to any credit bureau, agency, or third party by you pertaining to the Defendant's account.

33) All documents, notes, records of memoranda of any kind (which are not attorney work product or attorney-client communications) generated by your attorney which prove or tend to prove the work performed by your attorney for the above styled and numbered cause.

34) A copy of the notary log book's page for who notarized any Affidavits utilized as summary judgment evidence, verified testimony, or any matter herein.

35) A copy of the debt collection policy of Plaintiff in effect six (6) months prior to the filing of this suit.

36) A copy of the debt collection policy of Plaintiff's debt collector in effect six (6) months prior to the filing of this suit.

37) All electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail systems usage) sent or received by anyone relating to the issues in this lawsuit.

38) All data bases (including all records and field structural information in such databases), containing any reference to and/or information about the issues in this lawsuit.

39) All logs of activity on any computer system which may have been used to process or store electronic data containing information about the issues in this lawsuit.

40) All word processing files and file fragments containing information about the issues in this lawsuit.

41) With regard to electronic data created by application programs which process financial, accounting and billing information, all electronic data files and file fragments containing information about the issues in this lawsuit.

42) All files and file fragments containing information from electronic calendars and scheduling programs regarding the issues in this lawsuit.

43) All electronic data files and file fragments created or used by electronic spreadsheet programs where such data files contained information about the issues in this lawsuit.

44) A true and correct copy of all electronic data on personal computers used by anyone under the control of Plaintiff and/or their Secretaries and Assistants relating to the issues in this lawsuit, including all active files and file fragments.

45) All floppy diskettes, magnetic tapes and cartridges, compact disks, zip drives, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to the issues in this lawsuit.

46) All records, electronic or otherwise, containing the names of all employees, representatives, and debt collectors who acted on behalf of Plaintiff in connection with

the claims alleged in this suit.

47) All audio recordings of any conversation or communication between employees, representatives, and debt collectors who acted on behalf of Plaintiff in connection with the claims alleged in this suit.

48) A copy of any credit bureau report concerning Defendant obtained by Plaintiff during the five (5) years prior to the filing of this suit.

49) All records, electronic or otherwise, reflecting any contact with Defendant initiated by employees, representatives, and debt collectors who acted on behalf of Plaintiff in connection with the claims alleged in this suit during the six (6) months prior to the filing of this suit.

50) A certified copy of any and all documentary evidence of plaintiff's authority to operate a credit card enterprise, including but not limited to any applicable corporate charter and articles of incorporation.

51) A verified copy, front and back, of the original contract/agreement between the plaintiff and defendant with respect to the disputed account herein, in its entirety.

52) A verified copy, front and back, of the application allegedly executed by the defendant related to the disputed account herein, in its entirety.

53) A verified copy, front and back, of the Arbitration Agreement allegedly executed by the Parties with respect to the disputed account, in its entirety.

54) A verified copy of the complete set of original bookkeeping entries made by plaintiff from the origination of the disputed account to charge off, including, but not limited to all general ledger and accounting entries used to support plaintiff's compliance with the requirements of the Sarbanes-Oxley Act of 2002, H.R. 3763.

55) Certified Electronic copies of all accounting records pertaining to the disputed account.

56) Certified copies of all original accounting records evidencing a series of loans of money from the plaintiff to the defendant.

57) Certified copies of all original accounting records evidencing the payment of money from the plaintiff to any and all vendors, on defendant's behalf.

58) All documents evidencing payment by plaintiff to merchants, service providers or vendors, for each and every purchase of goods or services allegedly made by defendant using the disputed charge account for which plaintiff is seeking recovery herein.

59) Certified Electronic copies of all billing records pertaining to the disputed account.

60) Certified copies of all documents which named plaintiff intends to use as evidence of a lawful statement of claim against defendant from the plaintiff named in the caption of this cause of action.

61) Copies of any and all documents related to the sale, assignment, transfer or conveyance of the disputed account.

62) All documents intended to be used by plaintiff as evidence to show that the named plaintiff is the owner or holder in due course of the contract, note or other negotiable instrument that is the subject of this cause of action.

63) A certified copy of any document identifying the current owner or holder in due course of the contract, note or other instrument that is the basis for this cause of action.

64) Copies of all correspondence between the named plaintiff and defendant, relative to the account or instrument that is the basis for this cause of action.

65) Any and all documents including mailings and promotional materials that Defendant received from Plaintiff.

66) All documents reflecting communication between Plaintiff and Experian Information Solutions, Inc., TRW, Inc., and Equifax Credit Services regarding the account.

67) All tape recordings between Plaintiff or any of its agents and Defendant.

68) Any and all communications between you and any third party that relates to claims in this lawsuit.

EXHIBIT "A" REQUEST FOR ADMISSIONS

ADMIT OR DENY THAT

1. Plaintiff has no evidence to offer by which it can deny the allegations contained in the Defendant's Answer in this case.

2. Plaintiff has no witness to offer who can deny the allegations contained in Defendant's Answer filed in this case.

3. Plaintiff has no evidence to offer by which it can prove any of the allegations contained in the Plaintiff's Original Petition filed in this case.

4. Plaintiff has no witness to offer who can prove any of the allegations contained in the Plaintiff's Operative Petition filed in this case.

5. Plaintiff or its attorney is a "debt collector" as defined by Tex. Fin. Code § 392.001(6).

6. Plaintiff's designated agent(s) as witness(es) does not have personal knowledge of the matters set forth in his verification attached to Plaintiff's Original Petition.

7. Plaintiff's claim against Defendant includes illegal penalties disguised as liquidated damage items for various charges including, "late charges", "over-limit charges", and/or "miscellaneous charges", designed to increase the credit card interest rate.

8. Prior to filing suit, the Plaintiff obtained the services of its counsel herein to act as its agent in Plaintiff's collection efforts against the Defendant.

9. Plaintiff's counsel is a "debt collector" as defined by 15 U.S.C.§1692a(6) and Tex. Fin. Code §392.001(6).

10. Plaintiff's lawyer is a "third-party debt collector" as defined by Tex. Fin. Code §392.001(7).

11. Plaintiff's lawyer is an "independent debt collector" as per Tex. Fin. Code §392.306.

12. Plaintiff's lawyer filed this collection case for Plaintiff.

13. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g(a) Notice.

14. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g(a) Notice.

15. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g validation.

16. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g name and address of the original creditor.

17. The Debt Collector for Plaintiff told the Defendant that the legal collection process would continue until the Defendant entered into a repayment agreement or Plaintiff obtained a judgment.

18. The Debt Collector for Plaintiff told the Defendant that the judgment could result in a lien placed against his home.

19. Plaintiff's designated agent, did not review any documents either before, or at the time, Plaintiff signed the statement attached to Plaintiff's Original Petition.

20. Plaintiff employed a debt collector for Plaintiff.

21. The Debt Collector for Plaintiff spoke to Defendant on the telephone.

22. The Debt Collector Plaintiff told the Defendant that the judgment could result in a lien placed against his car.

23. The Debt Collector for Plaintiff told the Defendant that the judgment could result in a wage garnishment.

24. Plaintiff did not send Defendant an effective 15 U.S.C. § 1692g validation.

25. Plaintiff did not send defendant 15 U.S.C. § 1692g name and address of the original creditor.

26. The Debt Collector for Plaintiff told the Defendant that Plaintiff could satisfy a judgment from any asset Defendant has.

27. In violation of Tex. Fin. Code 392.301(a)(8), the Plaintiff threatened to take an action prohibited by law.

28. In violation of Tex. Fin. Code 392.301(a)(8), the Plaintiff misrepresented the character of a consumer debt.

29. Defendant's home is not an asset available to Plaintiff to satisfy a potential judgment in this case.

30. Defendant's car is not an asset available to Plaintiff to satisfy a potential judgment in this case.

31. The Debt Collector for Plaintiff made misrepresentations to the Defendant.

32. Wage garnishment is not available to Plaintiff regarding its claim against Defendant.

33. In violation of 15 U.S.C. § 1692d, the Plaintiff engaged in conduct the natural consequence of which was to harass, oppress, or abuse a person in connection with the collection of a debt.

34. In violation of 15 U.S.C. § 1692e, U.S.C. § 1692e(2)(A) and (B), U.S.C § 1692e(4), U.S.C. § 1692e(5) and U.S.C. § 1692e(10) and the "least sophisticated consumer standard," the Plaintiff used objectively false representations and/or false, deceptive, or misleading representations or means in connection with the collection of a consumer debt.

35. Plaintiff failed to conduct an investigation of any dispute asserted by the Defendant.

36. Plaintiff failed to admit, deny, or otherwise act on any dispute asserted by the Defendant.

37. Plaintiff failed to furnish Defendant with any consumer forms for giving a Tex. Fin. Code § 392.202 Notice.

38. Plaintiff failed to furnish Defendant with any assistance in preparing a Tex. Fin. Code § 392.202 Notice.

39. Plaintiff has no written agreement with the Defendant.

40. Plaintiff has no agreement bearing the Defendant's signature.

41. Plaintiff maintains an employment file on the Debt Collector who telephoned the Defendant.

42. Plaintiff's attorney is engaged directly or indirectly in consumer debt collection (any action, conduct or practice in collecting debts alleged to be created by an individual primarily for personal, family, or household purposes).

43. Plaintiff's attorney has regularly collected or attempted to collect, directly or indirectly, consumer debts owed or due or asserted to be owed or due another.

44. Plaintiff's attorney was required to obtain a debt collector's bond and file a copy thereof with the Texas Secretary of State.

45. The Plaintiff was required to obtain a debt collector's bond and file a copy thereof with the Texas Secretary of State.

46. The Defendant notified Plaintiff's attorney and/or the Plaintiff that the Debt was disputed by the Defendant.

47. After the Defendant notified Plaintiff and/or the Plaintiff that the Debt was disputed by the defendant, the Plaintiff and/or its attorney(ies) continued to report the Debt to consumer credit reporting bureaus.

48. The Plaintiff and/or Plaintiff's attorney never reported to any consumer credit reporting bureau that the Debt was being disputed by the Defendant.

49. The Plaintiff's claim against Defendant is barred by limitations.

50. Plaintiff never sent the Defendant any validation for the amount due on the Debt.

51. Plaintiff never satisfied any 15 U.S.C. § 1692g(b) request made by the Defendant.

52. After notice of Defendant's representation by counsel, the Plaintiff's lawyer directly sent Defendant correspondence on the Plaintiff's behalf.

53. After notice of Defendant's representation by counsel, the Plaintiff was requested to provide written correspondence.

54. Plaintiff never responded to the Defendant's written correspondence requests.

55. After notice of representation, one of the Defendant's lawyer sent correspondence on the Defendant's behalf.

56. Plaintiff never responded to the written correspondence referred to in Admission request 55.

57. Plaintiff's debt collector never responded to correspondence to verify the dent.

58. There is a written Power of Attorney and any other contracts between you and your attorney for the representation of you in your claims against Defendant.

59. There is a written account agreement(s) between Plaintiff and Defendant.

60. There is a written account agreement(s) between Plaintiff and Defendant which bear the signature of Defendant.

61. You have provided all of the written account agreements between Plaintiff and Defendant from the inception of the account through present.

62. That you always timely provided written notice of changes in the terms of the credit card agreement.

63. That you have all invoices and/or statements from Plaintiff to Defendant from the inception of Accounts to the present time, which reflect or list what goods or services you contend make up the transactions for the amount due.

64. That you have individual checks for each transaction that you contend Defendant charged via check.

65. That you have individual transaction receipts for each transaction that you contend Defendant charged.

66. That you have individual documents signed by Defendant for each transaction that you contend Defendant charged.

67. That you have the individual documents for each transaction that you contend Defendant charged that you are claiming in this suit.

68. That plaintiff is not licensed with the Secretary of State of Texas to transact business as a foreign corporation.

69. Admit that plaintiff and defendant did not execute a written contract related to the disputed account in the above-captioned cause of action.

70. Admit that plaintiff and defendant never executed a written agreement to arbitrate disputes.

71. Admit that it is plaintiff's position that defendant's alleged use of the credit card constituted consideration for the credit card agreement.

72. Admit that the alleged credit card agreement was amended some time after the disputed account was originated, to include a clause requiring that disputes be brought before the National Arbitration Forum.

73, Admit that the consideration for the amendment of the credit card agreement was the defendant's alleged continued use of the credit card.

74. Admit that defendant objected to the arbitration of disputes at the National Arbitration Forum.

75. Admit that Plaintiff's attorney is a debt collector as that term is used in the Fair Debt Collection Practices Act.

76. Admit that plaintiff has charged off the disputed amount claimed on herein.

77. Admit that plaintiff has taken a tax write-off or other tax adjustment with respect to the disputed account that it has claimed on herein.

78 Admit that the plaintiff never loaned money to the defendant.

79. Admit that the named plaintiff failed to disclose to the defendant the fact that it did not loan money to the defendant.

80. Admit that defendant has disputed the statement of account related to the account that is the subject of this cause of action.

81. Admit that the named plaintiff received defendant's notice of dispute and demand for validation and documentation on the disputed account.

82. Admit that the named plaintiff failed to provide defendant validation and verification of the alleged debt.

83. Admit that the account that is the subject of this cause of action is currently in dispute.

84. Admit that plaintiff filed or issued an insurance claim related to the disputed account.

85. Admit that named plaintiff received money, credit, or some other valuable consideration in payment or settlement on an insurance claim related to the alleged default in the disputed account herein.

86. Admit that Plaintiff either directly or indirectly through its agents or assigns, sold, assigned, transferred or otherwise conveyed its interest in the disputed account to Its attorney..

87. Admit that defendant does not owe plaintiff any debt related to the account that is the basis of this cause of action.

EXHIBIT "A" RULE 194 REQUEST

Pursuant to TEX.R.CIV.P. 194, you are requested to disclose within thirty (30) days of service of this request, the information or material described in TEX.R.CIV.P. 194.2(a)-(i).

Certificate of Service

This is to certify that on the 16TH Day of APRIL 2012 pursuant to TRCP, a true and correct copy of this instrument has been sent by fax to:

EXHIBIT "A"
DEFENDANT'S RESPONSE TO PLAINTIFF'S REQUEST FOR DISCLOSURE

194.2(a): Defendant believes that the proper parties are known BUT not plead

194.2(b): None known.

194.2(c): Violations of the debt collection act. Usury, Fraud, Unconscionability, Excuse, unlawful liquidated damage provision, failure of consideration, improper notice, plaintiff is not entitled to recover in the capacity in which it sues. Proof of written agreement, not given, excessive demand for payment, and taking of advantage of Defendant to a grossly unfair degree as the terms of the account were unilaterally changed until there was no benefit of bargain and an onerous penalty stream of charges ensued including interest and fees. Defendant was overwhelmed and could not audit the account for accuracy to determine if the charges to the account were lawful. See Defendant's operative answer.

Plaintiff has not established ownership of the account. Recession, Reformation and illegal contract. Illusory contract that fails for mutuality of obligation amongst other matters. Statute of Limitations. Plaintiff cannot prove an agreement

Defendant did not receive, agree or have complete admissible proof to review for the relevant time for damages sought herein. Defendant may better respond to this request if Plaintiff can identify the alleged agreements, modifications, applicable time frames for said agreement and identify the alleged transactions sought as damages in this suit. Plaintiff does not waive any rights to arbitration, or choice of law should an agreement be identified, response herein shall not waive any rights pertaining to said agreement(s) including arbitration. Defendant also reserves the rights for all damages thereto. Plaintiff has never made a proper demand for an amount due. Consequently, Plaintiff has failed to meet its burden of a proper demand for attorney fees under 38.001.The aforementioned is merely a summary of Defendant's legal theories and factual allegations and is not intended to include all of them.

194.2(d) Reasonable and Necessary Attorney Fees, Statutory Damages for Violations of the Federal and State Debt Acts, Damages found by the finder of fact, Loss of Credit Standing and the Like.

194.2(e) Defendant through defendant's attorney.

194.2(f) Discoverable information will be provided if it exists.

Expert Designation

[redacted]

194.2(f)2 Attorney fees and Plaintiff's damages.

194.2(f)3 He may testify as reasonableness and necessary attorney fees in this matter. He may also testify as to the calculation of Plaintiff's damages made the basis of this suit.

194.2(f)4(A) All discoverable documents this expert has had access to are located at the his law offices and will be made available at all reasonable times, counsel schedule permitting, upon request.

194.2(f)(B) Education

[redacted]

Employment

[redacted]

Litigation and general practice

Admitted to Texas Bar [redacted] and several Federal Districts and Circuits. Including 5th circuit and 5th Circuit Court of Appeals.

194.2(g) Not applicable.
194.2(h) None.
194.2(i) Discoverable information will be provided if it exists.
194.2(j) Not Applicable.
194.2(k) Not Applicable.

EXHIBIT "A"

List of Objections

The following list of objections is presented for the sake of convenience and clarity. Each objection will be referenced as an objection to each request for discovery to which such objection is asserted. A reference to any of the listed objection(s) is intended to be and shall be treated as though the objection was set forth verbatim.

Objection No. 1:

The request is overly broad, has no limit, and unnecessarily seeks discovery into matters that are protected from disclosure by the **attorney work product privilege,** Tex. R. Civ. P. Rule 192.5.

Objection No. 2:

This request is overly broad, has no limit, and unnecessarily seeks discovery into matters that are protected from disclosure by the **consulting expert privilege,** Tex. R. Civ. P. Rule 192.3(3)c.

Objection No. 3:

This request is overly broad, has no limit, and unnecessarily seeks discovery into matters that are protected from disclosure by the **party communication privilege,** Tex. R. Civ. P. Rule 192.5

Objection No. 4:

This request is overly broad, has no limit, and unnecessarily seeks discovery into matters that are protected from disclosure by the **attorney-client privilege,** Tex. R. Civ. P. Rule 192.5.

Objection No. 5:

This request is **confusing, vague and ambiguous.**

Objection No. 6:

This request is overly broad, general in nature and **fails to state with reasonable particularity** the specific documents and/or information sought. *Davis v. Pate,* 915 S.W.2d 76, 79 n.2 (Tex-App Corpus Christi 1996, original proceeding)

Objection No. 7:

This request required **speculation and/or conjecture** on the part of respondent to answer and is an impermissible request.

Objection No. 8:

The information sought is **not reasonably calculated** to lead to the discovery of admissible evidence. Tex. R. Civ. P. Rule 192.3(a); *Axelson v. McIlhany,* 798 S.W.2d 550, 553 (Tex. 1990).

Objection No. 9:

The discovery sought pertains to experts and this particular request is **not a permissible form of discovery** to obtain said information. Tex. R. Civ. P. Rule 195.1; *In Re Guzman:* 19 S.W.2d 522, 524-525 (Tex-App – Texarkana 1992 original proceeding)

Objection No. 10:

The information sought to respond to this discovery is **not reasonably and/or readily available** to respondent.

Objection No. 11:

This is an **improper request and/or discovery tool** to obtain the information sought.

Objection No. 12:

The information sought has been requested and **provided in another form.** *Sears, Roebuck & Company v. Ramirez,* 824 S.W.2d. 558, 559 (Tex. 1992).

Objection No. 13:

The information sought is one, if not all of the following **undue burden**, unduly burdensome, harassing, annoying, and involves an unnecessary expense to respond. Tex. Civ. P. Rule 192.

Objection No. 14:

This request **invades protected personal, constitutional and property rights** to respond, Tex. R. Civ. P. Rule 192.6(b); *Hoffman v. Court of Appeals*, 756 S.W.2d 723, 723 (Tex. 1988).

Objection No. 15:

This request requires respondent to **marshal all of its proof to respond.** Tex. R. Civ. P. Rule 194.2 c; 197.1; 194 – *comment 2;* and 197 *comment 1*

Objection No. 16:

Improper request as it seeks a **legal conclusion**.

Objection No. 17:

Proponent of this request has **equal access** to the information requested.

Objection No. 18:

This request has been **asked and answered.**

Objection No. 19:

Proponent has **failed to adequately identify applicable agreements** and the times said agreements were applicable.

Objection No. 20:

Proponent has **failed to the adequately identify transactions** alleged owed and due.

Objection No. 21:

Proponent has **failed to adequately identify the back up data** utilized to calculate the amount due.

Objection No. 22:

Respondent cannot answer this request at this time because after a reasonable inquiry the information known easily obtainable is insufficient to enable respondent to admit or deny this request.

Objection No. 23:

The requests required a party to admit a proposition of law. *Humble Sand & Gravel v. Gomez*, 48 S.W.3d 487, 505-06 (C.A.- Texarkana 2001, pet granted 5-30-02); *Esparza v. Diaz*, 802 S.W.2d. 772, 775 (C.A. – Houston {14th Dist} 1990, no writ).

Objection No. 24:

This request is improper and has not been properly served upon Respondent in accordance with the Texas Rules of Civil Procedure ("TRCP"). TRCP 191.4(a)1 proscribes the filing of discovery requests with the clerk. Proponent of the discovery has not only filed its requests with the clerk, but has also disguised the discovery in a pleading. TRCP 192.2 allows for permissible forms of discovery to be combined in the same document, but it does not allow the combination of pleadings and discovery. TRCP 192.7 defines written discovery as requests for disclosure, requests for production and inspection and copying of documents and tangible things, request for entry onto property, interrogatories and request for admissions. The discovery sought was filed with the clerk and combined with a pleading in contravention of the TRCP and is improper.

Objection to Instructions and Definitions:

Defendant objects to the instructions and definitions to the extent that they impose duties, or definitions and instructions other than those as per the Texas Rules of Civil Procedure (TRCP). Including but not limited to the definition of the term document and the right to challenge the admissibility of exhibits made a part of a question or response in this suit.

Explanation in support of Responses:

Defendant did not receive, agree or have complete admissible proof to review for the relevant time for damages sought herein. Defendant may better respond to this request if Plaintiff can identify the alleged agreements, modifications, applicable time frames for said agreement and identify the alleged transactions sought as damages in this suit. Plaintiff does not waive any rights to arbitration, or choice of law should an agreement be identified, response herein shall not waive any rights pertaining to said agreement(s) including arbitration.

EXHIBIT "A"

1) Objection 24 and w/o waving Objections 5, 6, 7, 16, 19, 20, 21, 22, and 23. W/O waving Deny.
2) See response 1.
3) See response 1.
4) See response 1.
5) See response 1.
6) See response 1.
7) See response 1.
8) See response 1.
9) See response 1.
10) See response 1.
11) See response 1.
12) See response 1.
13) See response 1.
14) See response 1.
15) See response 1.
16) See response 1.
17) See response 1.
18) See response 1.
19) See response 1.
20) See response 1.
21) See response 1.
22) See response 1.
23) See response 1.
24) See Response 1.
25) Objection 24 w/o same Admit.
26) See Response 1.
27) See Response 1.

EXHIBIT C

NO. [redacted]

[redacted]	}	IN THE JUSTICE COURT
VS.	}	PRECINCT 1, PLACE 2 OF
[redacted]	}	HARRIS COUNTY, TEXAS

DEFENDANT'S ORIGINAL ANSWER, COUNTERCLAIM AND REQUEST FOR DISCLOSURES

Defendant, [redacted], files this Original Answer and Counterclaim to Plaintiff's Original Petition, and Request for Disclosures to the Plaintiff, and shows the Court the following:

Defendant generally denies each and every allegation in Plaintiff's Original Petition, alleges that the same are not true in whole or in part, and demands strict proof thereof by a preponderance of the evidence upon a trial hereof.

Defendant denies the account on which Plaintiff files suit because not each and every item of the account made the basis of Plaintiff's suit is just or true.

Defendant denies the account on which Plaintiff files suit because Defendant has never had an open account with Plaintiff or Plaintiff's predecessor, a written or oral contract for goods or services with Plaintiff or Plaintiff's predecessor, or any business dealings with Plaintiff or Plaintiff's predecessor on which an account could be founded.

Allegations Common To Affirmative Defenses and All Counts in Counterclaim

The debt which Plaintiff attempts to collect in its Petition is or was originally due to another company.

Plaintiff has used the United States mail service in the regular collection or attempted collection of debts owed to another.

Defendant is a natural person, residing in Texas, allegedly obligated to pay a purported debt.

EXHIBIT "C"

Plaintiff has collected or attempted to collect from Defendant on an alleged debt.

Plaintiff is a "debt collector", as defined by 15 USCS § 1692a(6).

Plaintiff seeks recovery of the debt alleged in its Petition to have been due to a creditor other than Plaintiff. Plaintiff has collected and attempted to collect debts owed to another, and utilizes the services of collection law firms in such collection.

Plaintiff seeks recovery of the amount alleged in its Petition whereby it seeks to obtain the right to pursue payment on an account receivable originally belonging to an original creditor.

Defendant purchased merchandise primarily for personal, family or household purposes and not for business, which resulted in an account with an original creditor, not Plaintiff.

Defendant did not purchase any merchandise or services from the original creditor.

Plaintiff purports to have purchased the debt which Defendant incurred through the purchase of merchandise primarily for personal, family, or household purposes from others and not from the original creditor.

Defendant is a "consumer", as that term is defined by 15 USCS §1692a(3).

The obligation which Plaintiff alleges Defendant is obligated to pay is a "debt" as that term is defined by 15 USCS §1692a(5).

AFFIRMATIVE DEFENSES

Defense to Plaintiff's Alleged Assignment of Contract/Debt

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Defendant is not liable to Plaintiff because, upon information and belief, there was no valid assignment of rights to Plaintiff by the original creditor; therefore, Plaintiff is not a proper party in interest and lacks standing to sue.

Defense of Lack of Privity

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Defendant is not liable to Plaintiff because of lack of privity between the parties.

No Breach of Contract

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Plaintiff cannot prove a valid contract with Defendant. Upon information and belief, no contract exists between Defendant and the original creditor. Therefore, there can be no breach of a contract.

Plaintiff cannot prove its damages on its contract claim. Therefore, Plaintiff cannot recover on its breach of contract claim.

Defenses to Plaintiff's Suit on Account Stated and Debt

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Plaintiff's claims on account stated pursuant to TRCP 185 are defective because a credit card account does not create the sort of debtor-creditor relationship required in order to bring a suit on account.

Plaintiff's Petition is defective as an account stated claim because a credit card account cannot be the basis for an account stated claim. There are no items identified which were sold by Plaintiff to Defendant. The account does not meet the requirements of an account stated.

Therefore, Plaintiff's account stated claim should be dismissed because an account stated claim cannot be brought on a credit card account.

Plaintiff's suit on account or debt fails to state any claim upon which relief may be granted as it sets forth no ultimate facts demonstrating:

a. That there was an offer, acceptance, and consideration;

b. The correctness of the account;

c. That there was a history of transactions between the parties;

d. The reasonableness of the charge;

e. That a meeting of the minds occurred; and

f. That the interest rate charged by the original creditor was agreed on by Defendant.

The affidavit accompanying Plaintiff's Petition fails to support Plaintiff's cause of action for the following reasons, including, but not limited to the following:

a. The affidavit of [redacted] (hereinafter "affiant") executed on [redacted] is not based upon personal knowledge of the [redacted] account.

b. The affiant is not an employee or records custodian of the original creditor and, therefore, lacks personal knowledge of the transactions giving rise to the debt.

c. The affiant is not an employee or records custodian of the original creditor and, therefore, lacks personal knowledge of the manner, method, or mode by which any records memorializing transactions giving rise to the alleged debt are prepared or kept.

d. The document to which the affidavit refers is purported to be a business record of the Plaintiff, who neither provided goods, services and/or merchandise to the Defendant, nor created the original records of the transactions giving rise to the purported debt at or near the time of the transaction.

e. Neither the affidavit nor the alleged records purport to show that the charges alleged to embody the purported amount owed are reasonable.

f. Neither the affidavit nor the alleged records are purported to having been kept in the regular course of business of the original creditor.

g. Defendant objects to the Affidavit and its attempted document proffer because the document attached to Plaintiff's affidavit is not a statement of account as required by statute.

Defense of the Cause of Action for Quantum Meruit or Unjust Enrichment

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Plaintiff cannot maintain a cause of action for quantum meruit for the following reasons:

a. Plaintiff neither had nor has any relationship with Defendant.

b. Plaintiff never had any agreement or implied contract with Defendant.

c. Plaintiff never had any agreement or implied contract with Defendant for any terms of repayment, interest or attorney fees.

d. Without any agreement for a charge of interest, Plaintiff is not entitled to interest in excess of that which can be charged without an agreement. Plaintiff cannot prove what amount of the claimed amount is principal and what amount is interest. Therefore, Plaintiff cannot collect any of the claimed amount.

e. On information and belief, Defendant never had an implied agreement with Plaintiff's alleged assignor for interest or attorney fees. Therefore, without any agreement for interest or attorney fees, Defendant cannot collect interest or attorney fees.

f. Plaintiff cannot prove the elements of quantum meruit, i.e.:

(1) That there was an offer, acceptance, and consideration;

(2) The correctness of the account;

(3) The reasonableness of the charge; and

(4) That a meeting of the minds occurred.

Defense to Plaintiff's Claim of Money Had and Received

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

There is no evidence of any loans made to Defendant or any money had and received by Defendant from the original creditor. There is no evidence of any loans made to Defendant or any money had and received by Defendant from Plaintiff.

Defense of Statute of Limitations

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Defendant is not liable to Plaintiff because, upon information and belief, Plaintiff's claim is barred by the applicable Statute of Limitations, set out in Texas Civil Practice & Remedies Code §§ 16.004 and 16.051 as the debts complained of were incurred more than four years before the date of Plaintiff's Petition.

Defense of Failure to Allege Specific Transactions

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Defendant is not liable to Plaintiff because Plaintiff's claim is barred for failure to allege specific transactions on the account relating to the alleged debt.

Dispute of Conditions Precedent

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Defendant denies that all conditions precedent for Defendant's liability and Plaintiff's recovery have been performed or have occurred, for the following reasons:

1. Plaintiff's cause of action for account stated fails because Defendant never had any prior dealings with the original creditor.

2. Plaintiff and Defendant have not entered into a valid contract.

3. Plaintiff cannot prove that Defendant and the original creditor ever entered into an agreement or contract.

4. Plaintiff cannot prove that it has an assignment of Defendant's account; therefore, all of Plaintiff's claims fail.

5. Plaintiff's cause of action for quantum meruit is not valid because a cause of action for quantum meruit cannot be brought on a credit card account and there can be no implied agreement for interest in excess of that agreed upon by parties. Therefore, Plaintiff is not entitled to any interest.

6. Plaintiff cannot prove what services or goods were delivered to Defendant or that any charges are reasonable. Therefore, Plaintiff cannot maintain a cause of action for quantum meruit.

COUNTERCLAIM

The Defendant, [redacted], as Counter-Plaintiff in the above styled and numbered cause, complains of the Plaintiff, [redacted], as Counter-Defendant, and for cause of action will show the following:

Count I: Violations of 15 USCS §1692, et seq., the Fair Debt Collection Practices Act (FDCPA)

Defendant re-alleges and by reference adopts all allegations contained in the preceding paragraphs.

Upon information and belief, Plaintiff has committed the following violations of the FDCPA:

1. As set out in Plaintiff's Original Petition, Plaintiff is attempting to collect interest on the alleged principal balance without a contract providing for payment of the interest.[1]

2. As set out in Plaintiff's Original Petition, Plaintiff is attempting to collect amounts representing late fees on the principal balance without a contract providing for the payment of the late fees by pleading for the alleged total owed to the original creditor in Plaintiff's Original Petition, when part of the alleged debt constituted late fees.[2]

3. As set out in Plaintiff's Original Petition, Plaintiff is attempting to collect amounts representing over-limit fees on the principal balance without a contract providing for the payment of the over-limit fees by pleading for the alleged total owed to the original creditor in Plaintiff's Original Petition, when part of the alleged debt constituted over-limit fees.[3]

4. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting the character of the debt by asserting that the total represented principal when it in fact represented only a portion of principal, with the rest being interest and fees by pleading for the alleged total owed to the original creditor in its Original Petition when part of the alleged debt was interest and late fees, not principal.[4]

5. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting to Defendant that Defendant was indebted to Plaintiff when Plaintiff was not a creditor of Defendant because Plaintiff has no assignment of the alleged debt from the original creditor.[5]

6. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting to Defendant the amount of the alleged debt, including in the balance interest and late fees not available to Plaintiff by law because no agreement exists allowing Plaintiff to recover the late fees and the rate of interest pled.[6]

---

[1] 15 USCS § 1692f(1)
[2] 15 USCS § 1692f(1)
[3] 15 USCS § 1692f(1)
[4] 15 USCS § 1692e(2)(A)
[5] 15 USCS § 1692e(2)(A)
[6] 15 USCS § 1692e(2)(A)

7. As set out in Plaintiff's Original Petition, Plaintiff is omitting material facts relating to an assignment of interest providing Plaintiff with the right to pursue this cause of action by representing to Defendant that it is the assignee of the original creditor when, in law, it is not.[7]

8. Misrepresenting that Defendant has breached a contract when Defendant had no contract with the original creditor or with Plaintiff.[8]

9. As set out in Plaintiff's Original Petition, Plaintiff is attempting to collect a debt that is not collectable because of the Statute of Limitations.[9]

10. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting to Defendant that Plaintiff has a legal right to pursue collection of a debt barred by the statute of limitations.[10]

11. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting the collectability of the debt by filing suit when Plaintiff knew or should have known that the amounts it was seeking were not collectable at law by pleading a cause of action for account stated on a debt which arose on a credit card because Defendant did not have any previous accounts or dealings with the original creditor or with Plaintiff.[11]

12. As set out in Plaintiff's Original Petition, Plaintiff is misrepresenting the collectability of the debt by filing suit when Plaintiff knew or should have known that the amounts it was seeking were not collectable at law by pleading a cause of action for open account and/or quantum meruit on a debt which arose on a credit card because a credit card debt cannot be the basis of such causes of action.[12]

13. Filing suit in a legal entity in which the Defendant does not reside, i.e., filing in a precinct in which the Defendant does not reside.

The Fair Debt Collection Practices Act provides for statutory damages of One Thousand dollars ($1,000.00) for violations of the FDCPA, costs of the action, and reasonable attorney's fees.

---

[7] 15 USCS § 1692e(2)(A)
[8] 15 USCS §§ 1692e(2)(A) and (B) and 1692f(1)
[9] 15 USCS § 1692e(2)(B)
[10] 15 USCS § 1692f(1)
[11] 15 USCS § 1692e(2)(A) and (5)
[12] 15 USCS § 1692e(2)(A) and (5)

ATTORNEY'S FEES AND COSTS

It was necessary for Defendant to secure the services of [redacted], a licensed attorney, to prepare and prosecute this counterclaim. A reasonable attorney fee and costs should be granted against Plaintiff and in favor of Defendant for the use and benefit of Defendant's attorney; or, in the alternative, Defendant requests that reasonable attorney fees and expense through final judgment after appeal be taxed as costs and be ordered paid directly to Defendant's attorney, who may enforce the order for fees in the attorney's own name.

The undersigned counsel also represents clients in civil appeals. Based on the undersigned counsel's experience working on such matters, in the event either party appeals any judgment in this case to any Court of Appeals, Defendant will incur an additional $7,500.00 in attorney's fees and related expensed. If any party seeks a Petition for Review of this case by the Texas Supreme Court, Defendant will incur an additional $5,000.00 in attorney's fees and related expense. Should the Texas Supreme Court accept any party's Petition for Review in this case, Defendant will incur an additional $5,000.00 in attorney's fees and related expenses.

REQUEST FOR DISCLOSURES

Pursuant to TEX.R.CIV.P. 194, Plaintiff is requested by Defendant to disclose within thirty (30) days of service of this request, the information or material described in TEX.R.CIV.P. 194.2.

PRAYER

THEREFORE, Defendant requests judgment for the following:

A. That the Court deny all relief to Plaintiff and that Plaintiff's suit be dismissed at Plaintiff's cost;

B. That Counter-Plaintiff have Judgment against Counter-Defendant for statutory damages in the total amount of One Thousand Dollars ($1,000.00) for violation of the Fair Debt Collection Practices Act;

C. That Plaintiff be required to make reports to all credit reporting businesses in order to correct negative entries made in

violation of the TDCPA;

D. That attorney's fees be awarded as requested above;

E. Pre-judgment and post-judgment interest as allowed by law;

F. Costs of court; and

G. All other relief, general and special, at law or in equity, to which Defendant and Counter-Plaintiff may be entitled.

/s/

RFA Responses

1. Defendant applied for the credit card as referenced in Plaintiff's Original Petition.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

2. Based upon Defendant's request, the account made a basis for Plaintiff's Original Petition was opened.

RESPONSE: Admit only that [redacted] opened up an account for me.

3. Defendant understood from the time the account made a basis of Plaintiff's Original Petition was opened that use of the credit card results in a loan being made to Defendant for the amount charged or cash advance requested.

RESPONSE: Deny.

4. Defendant understood from the time the account made a basis of Plaintiff's Original Petition was opened that Defendant is required and obligated to repay all charges or cash advances incurred on the account.

RESPONSE: Admit that Defendant understood that he was required to repay all legitimate merchant charges and cash advances. Deny that Defendant is obligated to repay anything to Plaintiff.

5. Defendant fully understood the risk and obligations associated with credit card accounts.

RESPONSE: Deny.

6. Defendant made the purchases and took cash advances using the credit card made a basis of Plaintiff's Original Petition.

RESPONSE: Admit.

7. Plaintiff is the present owner and holder of said account.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

8. Plaintiff is the party entitled to sue on said account.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

9. That the account reflected by the exhibits attached to Plaintiff's Petition in this cause is just and true.

RESPONSE: Deny.

10. The account reflected by the exhibits to Plaintiff's Petition in this cause is due.

RESPONSE: Deny.

11. The account reflected by the exhibits attached to Plaintiff's Petition in this cause is the balance due Plaintiff after all just and lawful offsets, payments and credits have been allowed.

RESPONSE: Deny.

12. Defendant received monthly statements showing the amount of charges or cash advances incurred for that monthly period, along with any payments or credits to the account, and specifying the monthly installment being due and owing.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

13. The monthly statement received by Defendant specifically advised of Defendant's right to dispute any error contained in the monthly statement.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

14. Since the account was opened, Defendant has not notified Plaintiff of any dispute or error regarding any information contained in any monthly statement.

RESPONSE: Admit.

15. Defendant did promise to pay Plaintiff for said account.

RESPONSE: Deny.

16. Plaintiff has requested Defendant to pay Plaintiff for said account.

RESPONSE: Admit.

17. Defendant has failed to pay Plaintiff for said account.

RESPONSE: Admit only that Defendant has not paid Plaintiff.

18. Plaintiff made written demand upon Defendant for payment of said account.

RESPONSE: Admit.

19. Written demand was made for payment of said account more than 30 days prior to filing this lawsuit.

RESPONSE: Admit.

20. Defendant's last payment on said account was on or about [redacted]

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

21. Defendant has breached the contract made a basis of Plaintiff's Original Petition.

RESPONSE: Defendant cannot admit or deny this request because Defendant and his attorney have insufficient information or knowledge of the request's subject matter to respond. A reasonable inquiry was made, but the information known or easily obtainable was insufficient to enable Defendant to admit or deny the matter.

22. Defendant presently owes Plaintiff the amount of $[redacted] on

said account plus accrued interest.
RESPONSE: Deny.

23. At no time prior to the filing of this lawsuit did Defendant or Defendant's representative request verification of the debt from Plaintiff or its agents.
RESPONSE: Admit.

24. At no time prior to the filing of this lawsuit did Defendant or Defendant's representative dispute the debt owing on the account made a basis of Plaintiff's Original Petition.
RESPONSE: Admit.

25. Defendant is not a member of any military service with assignments or orders that would give the Defendant a right to a delay under the law.
RESPONSE: Admit.

26. A reasonable attorney fee for Plaintiff's attorney for the prosecution of this lawsuit would be at least the amount of $2,000.00.
RESPONSE: Deny.

RFD Responses

1. The correct names of the parties to the lawsuit;

RESPONSE: Plaintiff and Counter-Defendant is [redacted] Defendant and Counter-Plaintiff is [redacted]

2. The name, address, and telephone number of any potential parties;

RESPONSE: None.

3. The legal theories and, in general, the factual bases of the responding party's claims or defenses;

RESPONSE:

A. Defendant's defenses are:

(1) Defective TRCP 185 claim because a credit card account cannot be the basis of a Rule 185 sworn account claim, and a credit card account cannot be the basis of an open account or an account stated.
(2) The Plaintiff cannot prove a contract between Plaintiff and Defendant or that a debt is owed by Defendant to Plaintiff. Therefore, Plaintiff's breach of contract claim or claim for debt fails.
(3) There can be no recovery under quantum meruit or unjust enrichment because Plaintiff cannot prove all the necessary elements.
(4) Plaintiff cannot prove the necessary elements of a claim for money had and received.
(5) No assignment of contract.
(6) Lack of privity between the parties.
(7) Plaintiff's claim is barred due to the Four-Year Statute of Limitations

B. Counter-Plaintiff's claims are:

(1) Claims for damages for violation of 15 U.S.C. §§ 1692, the Fair Debt Collection Practices Act ("FDCPA") because Plaintiff did at least the following:

(a) Attempted to collect amounts representing interest on the principal balance without a contract providing for payment of the interest.

(b) Attempted to collect attorney fees without a contract providing for the payment of attorney fees.

(c) Misrepresented the character of the debt by asserting that the total represented principal when it in fact represented only a portion of principal, with the rest being interest and fees.

(d) Misrepresented the collectability of the debt by filing suit when Plaintiff knew or should have known that the amounts it was seeking were not collectable at law because a credit card account cannot be the basis of an open account or account stated cause of action, and quantum meruit is barred by the Statute of Limitations.

(e) Misrepresented to Defendant that Defendant was indebted to Plaintiff when Plaintiff was not a creditor of Defendant.

(f) Misrepresented to Defendant the legal status of the purported

debt as owing and collectable when no agreement existed between the parties for the payment of such a debt.

(g) Misrepresented to Defendant that there exists an agreement between Plaintiff and Defendant for the payment of the alleged debt.

(h) Misrepresented to Defendant the amount of the alleged debt, including in the balance interest, late fees and other charges not available to Plaintiff by law in a cause of action on open account and account stated because the underlying debt is a credit card account.

(i) Omitted material facts relating to an assignment of interest providing Plaintiff with the right to pursue this cause of action because Plaintiff has no assignment of Defendant's account.

(j) Misrepresented the character, extent or amount of Defendant's debt, or misrepresented the status of Defendant's debt in a judicial proceeding because a credit card account cannot be the basis of open account and account stated causes of action.

(k) Represented that Defendant's debt might be increased by the addition of attorney's fees or other charges when there was no written contract or statute which authorized the fees or charges.

(l) Filed a lawsuit in which a cause of action is alleged which is not available to Plaintiff in Texas.

(m) Threatened to take action that cannot legally be taken in the State of Texas.

(n) Attempted to collect a debt that is not collectable because of the Statute of Limitations.

(o) Misrepresented to Defendant that Plaintiff has a legal right to pursue collection of a debt barred by the statute of limitations.

(p) Filed suit in a legal entity in which the Defendant does not reside, i.e., filed in a precinct in which the Defendant does not reside.

(2) Reasonable and necessary attorney's fees authorized by the Fair Debt Collection Practices Act.

4. The amount and method of calculating economic damages;

RESPONSE: The Fair Debt Collection Practices Act provides for actual damages, statutory damages up to One Thousand dollars ($1,000.00) for violations, costs of the action, and reasonable attorney's fees.

A. Defendant's economic damages are $1,000.00 for the following violations of the FDCPA committed by the Plaintiff:

(a) Plaintiff is attempting to collect interest on the alleged principal balance without a contract providing for payment of the interest.

(b) Plaintiff is attempting to collect amounts representing late fees on the principal balance without a contract providing for the payment of the late fees by pleading for the alleged total owed to the original creditor in Plaintiff's Original Petition, when part of the alleged debt constituted late fees.

(c) Plaintiff is misrepresenting the character of the debt by asserting that the total represented principal when it in fact represented only a portion of principal, with the rest being interest and fees by pleading for the alleged total owed to the original creditor in its Original Petition when part of the alleged debt was interest and late fees, not principal.

(d) Plaintiff is misrepresenting the collectability of the debt by filing suit when Plaintiff knew or should have known that the amounts it was seeking were not collectable at law by pleading a cause of action for open account on a debt which arose on a credit card because a credit card debt cannot be the basis of an open account.

(e) Plaintiff is misrepresenting to Defendant that Defendant was indebted to Plaintiff when Plaintiff was not a creditor of Defendant because Plaintiff has no assignment of the alleged debt from the original creditor.

(f) Plaintiff is misrepresenting to Defendant the amount of the alleged debt, including in the balance interest and late fees not available to Plaintiff by law because no agreement exists allowing Plaintiff to recover the late fees and the rate of interest pled.

(g) Plaintiff is omitting material facts relating to an assignment of interest providing Plaintiff with the right to pursue this cause of action by representing to Defendant that it is the assignee of the original creditor when, in law, it is not.

(h) Plaintiff misrepresented to Defendant that Plaintiff has a legal right to pursue collection of a debt barred by the statute of limitations.

(i) Plaintiff attempted to collect a debt that is not collectable because of the Statute of Limitations.

(j) Plaintiff filed suit in a legal entity in which the Defendant does not reside, i.e., filed in a precinct in which the Defendant does not reside.

B. Reasonable and necessary attorney's fees for the prosecution of Counter-Plaintiff's Counterclaim at the rate of $400.00 per hour. At least $1,200.00 incurred to date.

5. The name, address, and telephone number of persons having knowledge of relevant facts, and a brief statement of each identified person's connection with the case;

RESPONSE: [redacted] is the Defendant and Counter-Plaintiff and has knowledge concerning the facts of the case.

[redacted] He is the attorney for the Defendant and Counter-Plaintiff, and has knowledge of Defendant and Counter-Plaintiff's reasonable and necessary attorney fees.

[redacted] and [redacted] of [redacted], phone: [redacted]. They are the attorneys for the Plaintiff/Counter-Defendant in this case.

6. For any testifying expert:

A. the expert's name, address and telephone number;

B. the subject matter on which the expert will testify;

C. the general substance of the expert's mental impressions and opinions and a brief summary of the bases for them, or if the expert is not retained by, employed by, or otherwise subject to the control of the responding party, documents reflecting such information;

D. if the expert is retained by, employed by, or otherwise subject to the control of the responding party:
(1) all documents, tangible things, reports, models, or data compilations that have been provided to, reviewed by, or prepared by or for the expert in anticipation of the expert's testimony; and

(2) the expert's current resume and bibliography.

RESPONSE:

A. the expert's name, address and telephone number;

RESPONSE: [redacted]

B. the subject matter on which the expert will testify;

RESPONSE: [redacted] may testify regarding the nature, extent, amount and reasonableness of attorney's fees, or rebut any attorney fee testimony offered by Plaintiff or any other party.

C. the general substance of the expert's mental impressions and opinions and a brief summary of the bases for them, or if the expert is not retained by, employed by, or otherwise subject to the control of the responding party, documents reflecting such information;

RESPONSE: He has personal knowledge of the services rendered and to be rendered on behalf of Defendant and Counter-Plaintiff. He is licensed to practice law in the State of Texas, is familiar with the attorney fees customarily charged by attorneys in this county and throughout Texas for handling similar matters, and is familiar with attorney services normally required to properly represent clients in this and similar contested litigation matters. The services rendered and to be rendered were or will be performed by [redacted] at hourly rates that were, are and will be normal, customary, usual and reasonable in this county and throughout Texas. The attorney services rendered are in connection with the representation of Defendant and Counter-Plaintiff in this matter.

D. if the expert is retained by, employed by, or otherwise subject to the control of the responding party:
(1) all documents, tangible things, reports, models, or data compilations that have been provided to, reviewed by, or prepared by or for the expert in anticipation of the

expert's testimony; and

(2) the expert's current resume and bibliography.

RESPONSE: See his resume attached hereto as Exhibit 1 or previously provided.

7. Any indemnity and insuring agreements described in Rule 192.3(f);

RESPONSE: None.

8. Any settlement agreements described in Rule 192.3(g);

RESPONSE: None.

9. Any witness statements described in Rule 192.3(h);

RESPONSE: None.

10. In a suit alleging physical or mental injury and damages from the occurrence that is the subject of the case, all medical records and bills that are reasonably related to the injuries or damages asserted or, in lieu thereof, an authorization permitting disclosure of such medical records and bills.

RESPONSE: Not applicable.

11. In a suit alleging physical or mental injury and damages from the occurrence that is the subject of the case, all medical records and bills obtained by the responding party by virtue of an authorization furnished by the requesting party.

RESPONSE: Not applicable

12. The name, address, and telephone number of any person who may be designated as a responsible third party.

RESPONSE: None.

1st Rogs to TT

DEFINITIONS AND INSTRUCTIONS

The Defendant provides the following definitions for the purpose of clarifying the meaning of various words and phrases contained herein in order to help the Plaintiff understand the objectives of Defendant's discovery efforts and to locate and furnish the relevant information and materials. It is therefore expressly stipulated and agreed by Defendant that an affirmative response on the part of the Plaintiff will not be construed as an admission that any definition contained herein is either factually correct or legally binding on the Plaintiff.

Information. This term is intended to include reference to both facts and applicable principles. This word should not be construed to be limited by any method of acquisition or compilation, and should, therefore, be construed to include oral information, as well as documents. You are requested to furnish all information in your possession and all information available to you, not merely such information as you know of your own personal knowledge, but also all knowledge that is available to you, your employees, officers and agents by reason of inquiry, including inquiry of their representatives.

Representative. This term shall be liberally construed and shall include, but not be limited to: all agents, employees, officials, officers, executives, directors, and any others who directly or indirectly represent the Plaintiff in any manner.

Statement: Written or Recorded. This term, as used herein, refers to (a) a written statement signed or otherwise adopted or approved by the person making it, and (b) a stenographic, mechanical, electrical or other type of recording, or any transcription thereof, which is a substantially verbatim recital of a statement made by the person and contemporaneously recorded, in conformity with the definition of statement pursuant to Rule 192.

"Person" means natural persons, corporations, partnerships, all other forms of legal entities, and the officers, directors, employees, agents, partners and personal representatives thereof.

The words "and" or "or" shall not be construed to limit the scope of this request due to either its disjunctive or conjunctive form.

The singular form of a word shall be interpreted to include the plural, and the plural form shall be interpreted to include the singular.

The terms "you" and **"Plaintiff"**, as well as a party's full or abbreviated name or a pronoun referring to a party, means the Plaintiff in the above styled and numbered lawsuit and, where applicable, its agents, representatives, officers, directors, employees, corporate agents, subsidiaries, members, and any other person or persons acting for or purportedly acting on behalf of the Plaintiff.

As used herein, the term **"Defendant"** means the Defendant named in the above styled and numbered lawsuit, his or her attorneys, agents and any other person or persons acting for or purportedly acting on his or her behalf.

As used herein, the term **"original creditor"** means the creditor who initially extended credit and/or opened up an account for Defendant and, where applicable, its agents, representatives, officers, directors, employees, corporate agents, subsidiaries, members, attorneys, and any other person or persons acting for or purportedly acting on their behalf.

As used herein, **"Account"** means and refers to the account ending in [redacted] opened by the original creditor for Defendant.

As used herein, "**default**" means 30 days after the last payment on the account.

"**Communications**" refer to both written and oral communications, video and audio.

"**Identify,**" "**Identification**" or "**Identity**" means:

(a) In the case of a person who is an individual: (i) his or her complete name; (ii) his or her present home and business addresses; (iii) his or her present employer and position; and (iv) the source of his or her knowledge about any of the information provided in response to the interrogatory or request for production. If the present address or employer of any such person is not known, please so indicate and state his or her last known employer.

(b) In the case of an organization: (i) its full name; (ii) the address of its principal place of business or management; (iii) the name of its chief executive officer; and (iv) the identity of all persons within the organization having knowledge of the facts asserted in response to the interrogatory or request for production.

(c) In the case of a document: (i) the type of document (e.g., memorandum, letter, note, report, record, collation, ledger, photograph, tape); (ii) the date on which the document was created; (iii) the date which appears on the document; (iv) the person who prepared it; (v) the person for whom it was prepared; (vi) all persons who received copies of it; (vii) its present location and custodian; (viii) its title or subject matter in brief. If the present location and custodian of any document is not known, please so indicate and state the last known location and custodian of such document.

(d) In the case of an act or event: (i) its date of occurrence; (ii) the place of occurrence; (iii) the identity of each person present and the name of the person or organization for whom such person acted or with whom such person was associated at the time of the occurrence; (iv) what was said and done by each person in connection with the occurrence; and (v) the identity of all other persons to whom such person represented or with whom such person was associated.

(e) In the case of an oral statement or communication; (i) the name of each person who participated in the communication and the name of each such person who was present at the time it was made; (ii) the date when such communication was made; (iii) the place where such communication was made, including the places from which and to which such communication was transmitted; (iv) what each person said, or if not known, the substance of such person's statement; and (v) the identity of each document pertaining to such oral communication.

As used herein, the term "**document**" shall mean the original, and if not available, any copy of the original, of writings of every kind, including, but not limited to, any correspondence, drawings, changes to such drawings, sketches, books, records, logs, reports, memoranda, abstracts, advertisements, agreements, appointment records, audio recordings, whether transcribed or not, balance sheets, bills, bills of lading, blanks, books of account, cablegrams, certificates, charters, communications, charts, checks, compilations from which information can be obtained or translated through detection devices, papers, transcriptions or summaries of conversations, delivery records, diaries, drafts, drafts of documents, electronic or mechanical recordation in whatever medium, discs, plans and specifications, graphs, tapes, slides ,cards, wires, computer programs, computer print-outs, entries, estimates, expense records, field noted, films, financial analyses,

financial statements, form, handbooks, telegrams, income statements, indices, instruments, intra-office and inter-office communications, invoices, itemizations, journals, letters, licenses, manuals, maps, meeting reports, minutes, notes order forms, orders, opinions, payroll records, permits, photocopies, photographs, planographs, press releases, prospectuses, publications, receipts, recordings, records, records of account, reports, requisitions, resolutions, statements, statistical records, studies, summaries, system analyses, time records, training manuals, evaluations, warehouse receipts, and any other electronic or mechanical recordings or transcripts or any other device or instrument from which information can be perceived, or which is used to memorialize human thought, speech or action in the possession, custody or control of Plaintiff, wherever located, including all premises and residences of Plaintiff and all the residences and premises of any of its attorneys, agents or representatives.

"**Relating to**" shall mean consisting of, referring to, reflecting or in any way logically or factually connected with the matters discussed. A document "relating to" a given subject is any document identifying, referring to, dealing with, evidencing, commenting upon, having as a subject, describing, summarizing, analyzing, explaining, detailing, outlining, defining, interpreting, or pertaining to that subject, including, without limitation, documents referring to the presentation of other documents.

Any information responsive to these interrogatories which, nonetheless, is not provided by reason of a claim of privilege or work product, or for any other reason, shall be identified by: 1) general subject matter; 2) identity of person(s) to whom the information, or any portion thereof, has already been revealed; 3) source of the information; 4) method of communication to Plaintiff or manner in which Plaintiff first acquired knowledge of the information at issue; and 5) the basis upon which the information is being withheld.

With respect to any interrogatory requiring you to identify any document, you may, in lieu thereof, attach a copy of such document to your answer.

"**Describe**" or "**description**" means to state specifically and in detail all facts which the persons answering this discovery knows are true, as well as all facts, which said person believes or has reason to believe, are true.

CONTINUING REQUEST FOR SUPPLEMENTATION

Defendant hereby makes a continuing request that Plaintiff comply with the duty, pursuant to the Texas Rules of Civil Procedure, to seasonably supplement your response to these Interrogatories if you obtain information upon the basis of which:

1. Plaintiff knows that any response herein was incorrect or incomplete when made; or
2. Plaintiff knows that the response, although correct and complete when made is no longer true and complete and the circumstances are such that failure to amend the answer is in substance misleading.

INTERROGATORIES

1. State the name, address, telephone number, and relationship to Plaintiff of each person who prepared or assisted in the preparation of the responses to these Interrogatories and, for each person listed, identify the Interrogatory number(s) which he or she prepared or assisted in the preparation of the answer. (Do not identify anyone who simply typed or reproduced the responses.)

RESPONSE:

2. State the total amount sought in this action, and specify how much of this total amount represents:

a. Total amount owed to the original creditor for merchant charges, cash advances and convenience checks;

b. Total amount which the original creditor represented to you was owed to it;

c. Interest charged by the original creditor;

d. Interest charged by you;

e. Fees of any type charged by the original creditor.

RESPONSE:

3. Identify documents you claim represent business records regarding the amounts you are seeking in this action, and for each such document indicate the entity or person who created the document.

RESPONSE:

4. State facts known to you that demonstrate that the account purchased from the original creditor was correct including, without limitation, identifying all persons with personal knowledge of those facts.

RESPONSE:

5. Identify facts known to you that demonstrate that the charges on the account were fair and reasonable.

RESPONSE:

6. Identify all holders of the debt that is the basis of this action beginning with the original creditor and ending with you.

RESPONSE:

7. List each investigative step taken by you, the date and result of that step and the person(s) with knowledge that such a step was taken, and identify documents that relate to any investigation concerning the debt.

RESPONSE:

8. On what date was the account opened for the Defendant by the original creditor?

RESPONSE:

9. When do you allege that you purchased or acquired this account?

RESPONSE:

10. State the name, address, location and telephone number of each person known to you or your attorney whom you expect to call as a trial witness at the time of trial of this cause.

RESPONSE:

11. Have you ever sent any letters to Defendant in an attempt to collect the alleged debt on this account?

RESPONSE:

12. When was the last payment made to the original creditor on the subject account?

RESPONSE:

13. When did the account go into default with the original creditor?
RESPONSE:

14. For each agreement you contend was offered to and accepted by the defendant, including but not limited to the original account agreement, any amendment to the agreement, any notice of a change in any term of the agreement, or any schedule of interest rates or fees applicable to the account, explain how the agreement was offered to and accepted by the Defendant.
RESPONSE:

15. Explain how each document containing the terms of any agreement for the account or reflecting any amount due on the account was delivered to the defendant, including but not limited to, the original account agreement, any amendment to the agreement, any notice of a change in a term of the agreement, any schedule of interest rates or fees applicable to the account. Include in your explanation the date the document was delivered and a description of the manner in which it was delivered, including, if the document was delivered by the Postal Service or other courier, the location to which it was addressed and whether the document was returned undelivered.
RESPONSE:

16. Explain how any statement of payments, charges, fees or interest for the account was delivered to the defendant. Include in your explanation the date the document was delivered and a description of the manner in which it was delivered, including, if the document was delivered by the Postal Service or other courier, the location to which it was addressed and whether the document was returned undelivered.
RESPONSE:

17. For each document you have produced that you contend applies to the account and that does not contain the defendant's identifying information, such as the defendant's name, social security number, account number, or signature, explain how you know the document applies to the account.
RESPONSE:

18. For each document you have produced that you contend applies to the account that does not contain the defendant's identifying information, such as the defendant's name, social security number, account number, or signature, and that was created by someone other than you, identify the source of the document by stating the date you obtained the document and identifying the person from whom you obtained the document.
RESPONSE:

1st RFAs to Π

1. "Person" means any natural person, corporation, firm, association, partnership, joint venture, proprietorship, governmental body, or any other organization, business, or legal entity, and all predecessors or successors in interest, and the officers, directors, employees, agents, partners and personal representatives thereof.

2. The words "and" or "or" shall not be construed to limit the scope of this request due to either its disjunctive or conjunctive form.

3. The singular form of a word shall be interpreted to include the plural, and the plural form shall be interpreted to include the singular.

4. The terms "you" and "Plaintiff", as well as a party's full or abbreviated name or a pronoun referring to a party, means the Plaintiff in the above styled and numbered lawsuit and, where applicable, its agents, representatives, officers, directors, employees, corporate agents, subsidiaries, members, and any other person or persons acting for or purportedly acting on behalf of the Plaintiff. This shall not include in any way the original creditor as defined below.

5. The terms "you" or "your" mean the Plaintiff in this suit, its division, subsidiaries, present and former officers, agents, employees, and all other persons acting on behalf of the Plaintiff or its divisions and subsidiaries. This shall not include in any way the original creditor as defined below.

6. As used herein, the term "Defendant" means the Defendant named in the above styled and numbered lawsuit, his or her attorneys, agents and any other person or persons acting for or purportedly acting on his or her behalf.

7. As used herein, the term "original creditor" means the creditor who initially extended credit and/or opened up an account for Defendant and, where applicable, its agents, representatives, officers, directors, employees, corporate agents, subsidiaries, members, attorneys, and any other person or persons acting for or purportedly acting on their behalf.

8. "Communications" refer to both written and oral communications, video and audio, of which the Plaintiff has knowledge, information or belief.

9. In the event that you deny only part of a request, you are directed to specify the precise component that you are denying and the part you are admitting.

10. In the event that you object to a request as overbroad or otherwise too expansive, you are directed to answer the portion which is deemed acceptable in scope.

11. In the event you object to any request based on any privilege, you are directed to identify the nature and scope of the privilege and to answer to the extent the privilege is not invoked or applicable.

12. "Account" means and refers to the account ending in [redacted] opened by original creditor for Defendant.

13. "Debt" means and refers to any balance on an account alleged to be due to Plaintiff from Defendant.

14. "Amount Claimed" means and refers to $[redacted].

15. Nothing in these requests shall be deemed to exceed the scope of permitted discovery under the Texas Rules of Civil Procedure, and to the extent any request could be so construed, it is to be construed as complying, where possible.

ADMIT OR DENY THE FOLLOWING:

1. You are a debt collector as that term is defined under the Fair Debt Collection Practices Act, 15 U.S.C. § 1692a(6).
RESPONSE:

2. The debt underlying the Lawsuit was in default on the date you allege that you acquired the debt.
RESPONSE:

3. You use the United States Postal Service to collect debts.
RESPONSE:

4. You have used the telephone to contact the Defendant.
RESPONSE:

5. You have sent letters to the Defendant through the United States Postal Service to attempt to collect a debt.
RESPONSE:

6. You use the United States Postal Service to attempt to collect debts.
RESPONSE:

7. You purchase the debts of others.
RESPONSE:

8. You collect on debts purchased by you.
RESPONSE:

9. You are not the original creditor of the defendant.
RESPONSE:

10. The Amount Claimed includes amounts that were charged to defendant by the original creditor as interest.
RESPONSE:

11. The Amount Claimed includes amounts that were charged to defendant by the original creditor as late fees.
RESPONSE:

12. The Amount Claimed includes amounts that were charged to defendant by the original creditor as over limit fees.
RESPONSE:

13. You furnished no goods or services to the defendant which resulted in any portion of the Amount Claimed.
RESPONSE:

14. You allege that you acquired from a third party unrelated to you the debt alleged to be due from Defendant.
RESPONSE:

15. The debt comprising the Amount Claimed is from a credit card.

RESPONSE:

16. You represented to Defendant that the Debt was legally collectable under the laws of the state of Texas.
RESPONSE:

17. The basis of Defendant's account with the original creditor was a credit card account.
RESPONSE:

18. The original creditor issues credit cards to customers.
RESPONSE:

19. The original creditor loaned money to Defendant for purchases by Defendant.
RESPONSE:

20. Defendant made purchases from vendors using the original creditor's credit card issued to Defendant.
RESPONSE:

21. The Defendant is a natural person.
RESPONSE:

22. The Defendant is a consumer.
RESPONSE:

23. The debt on which this lawsuit is based arose from purchases made for family or household purposes.
RESPONSE:

24. You only purchase consumer debt.
RESPONSE:

25. You only collect on consumer debt.
RESPONSE:

26. The debt on which the lawsuit is based is not a commercial debt.
RESPONSE:

27. No employee of Plaintiff is an employee of the Original Creditor.
RESPONSE:

28. There is no written assignment of the Account in your possession, custody or control.
RESPONSE:

29. There is no agreement which the Defendant entered into for the payment of interest on any account made the basis of this suit.
RESPONSE:

30. There is no agreement which the Defendant entered into for the payment of late fees on any account made the basis of this suit.
RESPONSE:

31. There is no agreement which the Defendant entered into for the payment of over limit fees on any account made the basis of this suit.
RESPONSE:

32. There is no agreement which the Defendant entered into providing for the payment to you of attorney fees for the collection of the Debt on any account made the basis of this suit.
RESPONSE:

33. Some or all of the Debt is not legally collectable under the laws of the state of Texas.
RESPONSE:

34. The original creditor did not sell any merchandise or services to Defendant.
RESPONSE:

35. No charges were made on the original account underlying the alleged debt made the basis of this lawsuit within the four years immediately preceding the filing of this lawsuit.
RESPONSE:

36. No payments were made on the original account underlying the alleged debt made the basis of this lawsuit within fifty months immediately preceding the filing of this lawsuit.
RESPONSE:

37. You have no documents which prove that the original creditor had a valid contract with the Defendant.
RESPONSE:

38. You do not own the alleged account of the Defendant which is the subject of this lawsuit.
RESPONSE:

39. The original creditor did not have a valid contract with the Defendant.
RESPONSE:

40. You have violated the FDCPA in your attempts to collect the alleged debt made the basis of this lawsuit.
RESPONSE:

1st RFP to Π

DEFINITIONS AND INSTRUCTIONS

1. "Person" means natural persons, corporations, partnerships, all other forms of legal entities, and the officers, directors, employees, agents, partners and personal representatives thereof.

2. The words "and" or "or" shall not be construed to limit the scope of this request due to either its disjunctive or conjunctive form.

3. The singular form of a word shall be interpreted to include the plural, and the plural form shall be interpreted to include the singular.

4. The terms "you" and "Plaintiff" means the Plaintiff in the above styled and numbered lawsuit, its officers, members, agents and any other person or persons acting for or purportedly acting on behalf of the Plaintiff.

5. As used herein, the term "Defendant" means the Defendant in the above styled and numbered lawsuit, his or her attorneys, agents and any other person or persons acting for or purportedly acting on his or her behalf.

6. "Communications" refer to both written and oral communications, video and audio.

7. "Identify," "Identification" or "Identity" means:

(a) In the case of a person who is an individual: (i) his or her complete name; (ii) his or her present home and business addresses; (iii) his or her present employer and position; and (iv) the source of h is or her knowledge about any of the information provided in response to the interrogatory or request for production. If the present address or employer of any such person is not known, please so indicate and state his or her last known employer.

(b) In the case of an organization: (i) its full name; (ii) the address of its principal place of business or management; (iii) the name of its chief executive officer; and (iv) the identity of all persons within the organization having knowledge of the facts asserted in response to the interrogatory or request for production.

(c) In the case of a document: (i) the type of document (e.g., memorandum, letter, note, report, record, collation, ledger, photograph, tape); (ii) the date on which the document was created; (iii) the date which appears on the document; (iv) the person who prepared it; (v) the person for whom it was prepared; (vi) all persons who received copies of it; (vii) its present location and custodian; (viii) its title or subject matter in brief. If the present location and custodian of any document is not known, please so indicate and state the last known location and custodian of such document.

(d) In the case of an act or event: (i) its date of occurrence; (ii) the place of occurrence; (iii) the identity of each person present and the name of the person or organization for whom such person acted or with whom such person was associated at the time of the occurrence; (iv) what was said and done by each person in connection with the occurrence; and (v) the identity of all other persons to whom such person represented or with whom such person was associated.

(e) In the case of an oral statement or communication; (i) the name of each person who participated in the communication and the name of each

such person who was present at the time it was made; (ii) the date when such communication was made; (iii) the place where such communication was made, including the places from which and to which such communication was transmitted; (iv) what each person said, or if not known, the substance of such person's statement; and (v) the identity of each document pertaining to such oral communication.

8. As used herein, the term "document" shall mean the original, and if not available, any copy of the original, of writings of every kind, including, but not limited to, any correspondence, drawings, changes to such drawings, sketches, books, records, logs, reports, memoranda, abstracts, advertisements, agreements, appointment records, audio recordings, whether transcribed or not, balance sheets, bills, bills of lading, blanks, books of account, cablegrams, certificates, charters, communications, charts, checks, compilations from which information can be obtained or translated through detection devices, papers, transcriptions or summaries of conversations, delivery records, diaries, drafts, drafts of documents, electronic or mechanical recordation in whatever medium, discs, plans and specifications, graphs, tapes, slides, cards, wires, computer programs, computer print-outs, entries, estimates, expense records, field notes, films, financial analyses, financial statements, form, handbooks, telegrams, income statements, indices, instruments, intra-office and inter-office communications, invoices, itemizations, journals, letters, licenses, manuals, maps, meeting reports, minutes, notes order forms, orders, opinions, payroll records, permits, photocopies, photographs, planographs, press releases, prospectuses, publications, receipts, recordings, records, records of account, reports, requisitions, resolutions, statements, statistical records, studies, summaries, system analyses, time records, training manuals, evaluations, warehouse receipts, and any other electronic or mechanical recordings or transcripts or any other device or instrument from which information can be perceived, or which is used to memorialize human thought, speech or action in the possession, custody or control of Plaintiff, wherever located, including all premises and residences of Plaintiff and all the residences and premises of any of its attorneys, agents or representatives.

9. Any information responsive to these Requests for Production which, nonetheless, is not provided by reason of a claim of privilege or work product, or for any other reason, shall be identified by: 1) general subject matter; 2) identity of person(s) to whom the information, or any portion thereof, has already been revealed; 3) source of the information; 4) method of communication to Plaintiff or manner in which Plaintiff first acquired knowledge of the information at issue; and 5) the basis upon which the information is being withheld.

10. Plaintiff shall furnish all information available to it as of the date of its answers hereto and shall supplement such answers pursuant to the Texas Rules of Civil Procedure.

11. As used herein, the term "original creditor" means the creditor who initially extended credit and/or opened up an account for Defendant and, where applicable, its agents, representatives, officers, directors, employees, corporate agents, subsidiaries, members, attorneys, and any other person or persons acting for or purportedly acting on their behalf.

12. As used herein, the term "account" means and refers to the account ending in [redacted] opened by original creditor for Defendant.

13. As used herein, the term "debt" means and refers to any balance on an account alleged to be due to Plaintiff from Defendant.

14. As used herein, the term "guarantee" means and refers to a promise to be responsible for the debt of another.

DOCUMENTS

1. The original agreement between the original creditor and the Defendant and any documents that you allege modified such an agreement from its original form, if any.
RESPONSE:

2. Any alleged contract executed between you and the Defendant.
RESPONSE:

3. The alleged application executed by the Defendant with the original creditor.
RESPONSE:

4. All documents which modify the original agreement between the original creditor and the Defendant.
RESPONSE:

5. Each document sent by the original creditor to the Defendant changing the rate of interest on Defendant's account with the original creditor.
RESPONSE:

6. Documents which identify each transaction that makes up the total amount sought in this action, including for each transaction the following:
   A. The date on which the transaction took place.
   B. The amount of the transaction.
   C. The specific items or services purchased.
   D. The price of each item purchased.
   E. The person purchasing the item or service.
   F. The identity of all persons with personal knowledge as to the facts set forth in response to items a-e above.
RESPONSE:

7. The alleged assignment of the alleged debt to you from the original creditor and/or alleged assignment documents in the chain of title from the original creditor to you.
RESPONSE:

8. All documents identified in your response to Defendant's First Interrogatories to Plaintiff.
RESPONSE:

9. Any and all documents, reports, compilations, or other materials relied upon by any retained expert in this matter.
RESPONSE:

10. All of Defendant's account statements from Defendant's original creditor.
RESPONSE:

11. Any documents which evidence that any charges were made on the underlying account within the four years immediately preceding the filing of this lawsuit.

RESPONSE:

12. Any documents which evidence that any charges were made on the underlying account within 1,465 days before the filing of this lawsuit.
RESPONSE:

13. All internal notes and memoranda generated by you (excepting any work product) concerning this account from the date it was purchased to the present.
RESPONSE:

14. Documents reflecting when the last payment was made to the original creditor on the account.
RESPONSE:

15. Documents from the original creditor reflecting the account history with the original creditor.
RESPONSE:

16. All documents on the subject account which were provided to you by the original creditor when the account was acquired by you.
RESPONSE:

17. All documents on the subject account which were provided to you by any alleged predecessor in title.
RESPONSE:

18. Any of your documents reflecting the debtor history or debt history obtained by you from the original creditor on the account.
RESPONSE:

19. Any debtor history report for this account.
RESPONSE:

20. Any debtor reports received by you from the original creditor on the account.
RESPONSE:

21. All letters or other correspondence sent by you to the Defendant from the date you allege you acquired the account to the present.
RESPONSE:

22. All correspondence sent by the Defendant to you from the date you allege you acquired the account to the present.
RESPONSE:

23. For each agreement, amendment to an agreement, or notice of change to the terms of the account you contend was offered to and accepted by the defendant, produce every document that evidences such offer or acceptance.
RESPONSE:

24. For each document listed below that was delivered to the defendant, produce all documents indicating the date the document was delivered and the manner in which it was delivered, including, if the document was delivered by the Postal Service or other courier, the location to which it was addressed and whether the document was returned undelivered:

a. The original account agreement for the account.

b. Any amendment to the agreement for the account.
c. Any notice of a change in any term of the account, including but not limited to a change in the rate of interest or amount of any fee applicable to the account.
d. Any schedule of interest rates or fees applicable to the account.
e. Any credit card issued in connection with the account.
f. Any statement of payments, charges, fees or interest for the account.

RESPONSE:

25. For each document you have produced that you contend applies to the account and that does not contain some piece of the defendant's identifying information, such as the defendant's name, social security number, account number, or signature, produce every document containing information from which it may be determined whether the document applies to the account.

RESPONSE: