

[OCC-4810-33-P 16.66%]

[FRB-6210-01-P 16.66%]

[FDIC-6714-01-P 16.66%]

[OTS-6720-01P 16.66%]

[NCUA-7535-01-U 16.66%]

[FTC-6750-01-P 16.66%]

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 41

[Docket No. 06-xx]

RIN 1557-AC87

FEDERAL RESERVE SYSTEM

12 CFR Parts 211 and 222

Docket No. xxxx

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

No. 2006-19

RIN 1550-AC04

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 7xx

Docket No. xxxx

RIN xxxx

FEDERAL TRADE COMMISSION

16 CFR 681

Docket No. xxxx

RIN xxxx

**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).

ACTION: Joint notice of proposed rulemaking.

SUMMARY: The OCC, Board, FDIC, OTS, NCUA and FTC (the Agencies) request comment on a proposal that would implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). As required by section 114, the Agencies are jointly proposing guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. The Agencies also are proposing joint regulations requiring each financial institution and creditor to establish reasonable policies and procedures for

implementing the guidelines, including a provision requiring credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances.

In addition, the Agencies are proposing joint regulations under section 315 that provide guidance regarding reasonable 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.

DATES: Comments must be submitted on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: The Agencies will jointly review all of the comments submitted.

Therefore, you may comment to any of the Agencies and you need not send comments (or copies) to all of the Agencies. Because paper mail in the Washington area and at the Agencies is subject to delay, please submit your comments by e-mail whenever possible. Commenters are encouraged to use the title “Red Flags Rule” in addition to the docket or RIN number to facilitate the organization and distribution of comments among the Agencies. Interested parties are invited to submit comments in accordance with the following instructions:

OCC: You should designate OCC in your comment and include Docket Number 06-___. You may submit comments by any of the following methods:

- **Federal eRulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **OCC Web Site:** <http://www.occ.treas.gov>. Click on “Contact the OCC,” scroll down and click on “Comments on Proposed Regulations.”
- **E-mail address:** regs.comments@occ.treas.gov.

- **Fax:** (202) 874-4448.
- **Mail:** Office of the Comptroller of the Currency, 250 E Street, SW.,

Public Reference Room, Mail Stop 1-5, Washington, DC 20219.

- **Hand Delivery/Courier:** 250 E Street, SW., Attn: Public Reference Room, Mail Stop 1-5, Washington, DC 20219.

Instructions: All submissions received must include the agency name (OCC) and docket number or Regulatory Information Number (RIN) for this notice of proposed rulemaking.

In general, the OCC will enter all comments received into the docket without change, including any business or personal information that you provide.

You may review the comments received by the OCC and other related materials by any of the following methods:

- **Viewing Comments Personally:** You may personally inspect and photocopy comments received at the OCC's Public Reference Room, 250 E Street, SW., Washington, DC. You can make an appointment to inspect comments by calling (202) 874-5043.

- **Viewing Comments Electronically:** You may request e-mail or CD-ROM copies of comments that the OCC has received by contacting the OCC's Public Reference Room at regs.comments@occ.treas.gov.

- **Docket:** You may also request available background documents using the methods described earlier.

Board: You may submit comments, identified by Docket No. R-xxxx, by any of the following methods:

- Agency Web Site: <http://www.federalreserve.gov>. Follow the instructions for

submitting comments at

<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, N.W., Washington, DC 20551.

All public comments are available from the Board's web site at

www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm as submitted, except as necessary 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 in Room MP-500 of the Board's Martin Building (20th and C Streets, N.W.) between 9:00 a.m. and 5:00 p.m. on weekdays.

FDIC: You may submit comments, identified by RIN number by any of the following methods:

- **Agency Web Site:**

<http://www.fdic.gov/regulations/laws/federal/propose.html>.

Follow instructions for submitting comments on the Agency Web site.

- **E-mail:** Comments@FDIC.gov. Include the RIN number in the subject line of the message.

- **Mail:** Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 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.
- **Instructions:** All submissions received must include the agency name and RIN for this rulemaking. 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 E-1002, 3502 North Fairfax Drive, Arlington, VA, 22226, between 9 a.m. and 5 p.m. on business days.

OTS: You may submit comments, identified by No. 2006-19, by any of the following methods:

- **Federal eRulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **E-mail:** regs.comments@ots.treas.gov. Please include No. 2006-19 in the subject line of the message and include your name and telephone number in the message.
- **Fax:** (202) 906-6518.
- **Mail:** Regulation Comments, Chief Counsel's Office, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552, Attention: No. 2006-xx.
- **Hand Delivery/Courier:** Guard's Desk, East Lobby Entrance, 1700 G Street, NW., from 9:00 a.m. to 4:00 p.m. on business days, Attention: Regulation Comments, Chief Counsel's Office, Attention: No. 2006-19.

Instructions: All submissions received must include the agency name and number or Regulatory Information Number (RIN) for this rulemaking. All comments received will be posted without change to <http://www.ots.treas.gov/pagehtml.cfm?catNumber=67&an=1>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.ots.treas.gov/pagehtml.cfm?catNumber=67&an=1>. In addition, you may inspect comments at the Public Reading Room, 1700 G Street, NW, by appointment. To make an appointment for access, call (202) 906-5922, send an e-mail to public.info@ots.treas.gov, or send a facsimile transmission to (202) 906-7755. (Prior notice identifying the materials you will be requesting will assist us in serving you.) We schedule appointments on business days between 10:00 a.m. and 4:00 p.m. In most cases, appointments will be available the next business day following the date we receive a request.

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 Proposed Rule 717, Identity Theft Red Flags," 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, Virginia 22314-3428.

- **Hand Delivery/Courier:** Same as mail address.

FTC: Comments should refer to “The Red Flags Rule, Project No. Rxxxxx,” and may be submitted by any of the following methods. Comments containing confidential material must be filed in paper form, must be clearly labeled “Confidential,” and must comply with Commission Rule 4.9(c).¹

- **E-mail:** <https://secure.commentworks.com/ftc-redflags>. To ensure that the Commission considers an electronic comment, you must file it on the web-based form found at this web link and follow the instructions on that form.
- **Federal eRulemaking Portal:** <http://www.regulations.gov>. You may visit this web site to read this request for public comment and to file an electronic comment. The Commission will consider all comments that regulations.gov forwards to it.
- **Mail or Hand Delivery:** A comment filed in paper form should refer, both in the text and on the envelope, to the name and project number identified above, and

¹ 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).

should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room 159-H (Annex C), 600 Pennsylvania Avenue, NW., Washington, DC 20580.

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>.

FOR FURTHER INFORMATION CONTACT:

OCC: Amy Friend, Assistant Chief Counsel, (202) 874-5200; Deborah Katz, Senior Counsel, or Andra Shuster, 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, Counsel, or Ky Tran-Trong, Senior Attorney, Division of Consumer and Community Affairs, (202) 452-3667; Andrew Miller, Counsel, Legal Division, (202) 452-3428; 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: Glenn Gimble, Senior Project Manager, Operation Risk, (202) 906-7158; Kathleen M. McNulty, Technology Program Manager, Information Technology Risk Management, (202) 906-6322; or Richard Bennett, 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, Division of Privacy and Identity Protection, Bureau of Consumer Protection, (202) 326-3228, Federal Trade Commission, 600 Pennsylvania, Avenue, NW., Washington D.C. 20580

SUPPLEMENTARY INFORMATION: This notice contains the following sections:

I. Section 114 of the FACT Act

A. Background

The President signed the FACT Act into law on December 4, 2003. Pub. L. 108-159 (2003). The FACT Act added several new provisions to the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. 1681 et seq., that relate to the detection, prevention, and

mitigation of identity theft.² Section 114 amends section 615 of the FCRA and requires the Agencies to jointly issue guidelines for financial institutions and creditors regarding identity theft with respect to their account holders and customers. 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 required under section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l), which requires verification of the identity of persons opening new accounts.

Section 114 also directs the Agencies to consider including reasonable guidelines providing that 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,” when a transaction occurs in connection with a consumer’s credit or deposit account that has been inactive for two years.

In addition, the Agencies must jointly prescribe 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.

The joint regulations must include a provision generally requiring credit and debit card issuers to assess the validity of change of address requests. In particular, 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

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).

procedures designed to prevent identity theft. Under these circumstances, 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.

Section 114 broadly describes elements that belong in the regulations and those that belong in the "guidelines" without defining this term. The Agencies are proposing to implement the requirements of section 114 through regulations (Red Flag Regulations) requiring each financial institution and creditor to implement a written Identity Theft Prevention Program (Program). The Program must contain reasonable policies and procedures to address the risk of identity theft. The Agencies also are proposing guidelines that identify patterns, practices, and specific forms of activity that indicate a possible risk of identity theft (Red Flag Guidelines or Appendix J). As required by statute, the Agencies will update the Red Flag Guidelines as often as necessary. The proposed Red Flag Regulations require financial institutions and creditors to incorporate relevant indicators of identity theft into their Programs. The Agencies request comment on whether the elements described in section 114 have been properly allocated between the proposed regulations and the proposed guidelines.

As required by section 114, the Agencies also are proposing joint regulations requiring credit card issuers to implement reasonable policies and procedures to assess the validity of a change of address.

B. Proposed Red Flag Regulations

1. Overview

The Agencies are proposing Red Flag Regulations that adopt a flexible risk-based approach similar to the approach used in the “Interagency Guidelines Establishing Information Security Standards”³ issued by the Federal banking agencies (FDIC, Board, OCC and OTS), and the “Standards for Safeguarding Customer Information”⁴ issued by the FTC, (collectively, Information Security Standards), to implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801.

Under the proposed Red Flag Regulations, financial institutions and creditors must have a written Program that is based upon the risk assessment of the financial institution or creditor and that includes controls to address the identity theft risks identified. Like the program described in the Agencies’ Information Security Standards, this Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities, and be flexible to address changing identity theft risks as they arise. A financial institution or creditor may wish to combine its program to prevent identity theft with its information security program, as these programs are complementary in many ways.⁵

³ 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).

⁴ 16 CFR part 314.

⁵ The Agencies note, however, that some creditors covered by the proposed Red Flag Guidelines are not financial institutions subject to Title V of the GLBA and, therefore, are not required to have an information

Briefly summarized, under the proposed Red Flag Regulations, the Program of each financial institution or creditor must be designed to address the risk of identity theft to customers and the safety and soundness of the financial institution or creditor. The Program must include policies and procedures to prevent identity theft from occurring, including policies and procedures to:

- Identify those Red Flags that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor;
- Verify the identity of persons opening accounts;
- Detect the Red Flags that the financial institution or creditor identifies as relevant in connection with the opening of an account or any existing account;
- Assess whether the Red Flags detected evidence a risk of identity theft;
- Mitigate the risk of identity theft, commensurate with the degree of risk posed;
- Train staff to implement the Program; and
- Oversee service provider arrangements.

The proposed Red Flag Regulations also require the board of directors or an appropriate committee of the board to approve the Program. In addition, the board, an appropriate committee of the board, or senior management must exercise oversight over the Program's implementation. Staff implementing the Program must report to its board, an appropriate committee or senior management, at least annually, on compliance by the financial institution or creditor with the Red Flag Regulations. These Regulations are described in greater detail in the section-by-section analysis that follows.

security program under the GLBA. Moreover, the term "customer" is defined more broadly in the proposed Red Flag Regulations than in the Information Security Standards.

2. Proposed Red Flag Regulations: Section-by-Section Analysis⁶

§ __.90 Duties regarding the detection, prevention, and mitigation of identity theft

§ __.90(a) Purpose and Scope

Proposed § __.90(a) sets forth the statutory authority for the proposed Red Flag Regulations, namely, section 114 of the FACT Act, which amends section 615 of the FCRA, 15 U.S.C. 1681m. It also defines the scope of this section; each of the Agencies has tailored this paragraph to describe those entities to which this section applies.

§ __.90(b) Definitions.

Proposed § __.90(b) sets forth the definitions of various terms that apply to this section.

1. Account. Section 114 of the FACT Act does not use the term “account.” However, for ease of reference, the Agencies believe it is helpful to identify a single term to describe the relationships covered by section 114 that an account holder or customer may have with a financial institution or creditor. Therefore, for purposes of the Red Flag Regulations, the Agencies propose to use the term “account” to broadly describe the various relationships an account holder or customer may have with a financial institution or creditor that may become subject to identity theft.⁷

The proposed definition of “account” is similar to the definition of “customer relationship” found in the Agencies’ privacy regulations.⁸ In particular, the proposed

⁶ The OCC, Board, FDIC, OTS and NCUA propose putting the Red Flag Regulations and Guidelines in the FCRA part of their regulations, 12 CFR parts 41, 222, 334, 571, and 717, respectively. In addition, the FDIC proposes to cross-reference the Red Flag 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.

⁷ The Agencies recognize that, in other contexts, the FCRA defines the term “account” narrowly to describe certain deposit relationships. See 15 U.S.C. 1681a(r)(4).

⁸ See 12 CFR 40.3(i)(1) (OCC); 12 CFR 216.3(i)(1) (Board); 12 CFR 332.3(i)(1) (FDIC); 12 CFR 573.3(i)(1) (OTS); 12 CFR 716.3(i)(1) (NCUA); and 16 CFR 313.3(i)(1) (FTC).

definition of “account” is “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).”⁹ The definition gives examples of an “account” including an extension of credit for personal, family, household or business purposes (such as a credit card account, margin account, or retail installment sales contract, including a car loan or lease), and a demand deposit, savings or other asset account for personal, family, household or business purposes (such as a checking or savings account). While the proposed definition of “account” is expansive, the risk-based nature of the proposed Red Flag Regulations affords each financial institution or creditor flexibility to determine which relationships will be covered by its Program through a risk evaluation process.

The Agencies request comment on the scope of the proposed definition of “account.” In particular, the Agencies solicit comment on whether reference to “financial products and services 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” is appropriate to describe the relationships that an account holder or customer may have with a financial institution or creditor that should be covered by the Red Flag Regulations. The Agencies also request comment on whether the definition of “account” should include relationships that are not “continuing” that a person may have with a financial institution or creditor. In addition, the Agencies

⁹ See 12 CFR 225.86 for a description of activities that are “financial in nature or incidental to a financial activity.”

request comment on whether additional or different examples of accounts should be added to the Regulations.

2. Board of Directors. The proposed Red Flag Regulations discuss the role of the board of directors of a financial institution or creditor. However, the Agencies recognize that some of the financial institutions and creditors covered by the Regulations will not have a board of directors. Therefore, in addition to its plain meaning, the proposed definition of “board of directors” includes, in the case of a foreign branch or agency of a foreign bank, the managing official in charge of the branch or agency. In the case of any other creditor that does not have a board of directors, “board of directors” is defined as a designated employee.

3. 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 are proposing to define “customer” to encompass both “customers” and “account holders.” Thus, “customer” means a person that has an account with a financial institution or creditor.

The proposed definition of “customer” is broader than the definition of this term in the Information Security Standards. The proposed definition applies 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.¹⁰

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. Although the definition of “customer” is broad, a financial institution or creditor would

¹⁰ See 15 U.S.C. 1681a(b).

have the discretion to determine which type of customer accounts will be covered under its Program, since the proposed Red Flag Regulations are risk-based.¹¹ The Agencies solicit comment on the scope of the proposed definition of “customer.”

4. Identity Theft. The proposed definition of “identity theft” states that this term has the same meaning as in 16 CFR 603.2(a). Section 111 of the FACT Act added several new definitions to the FCRA, including “identity theft.” However, section 111 granted authority to the FTC to further define this term.¹² The FTC exercised this authority and issued a final rule, which became effective on December 1, 2004, that defines “identity theft” as “a fraud committed or attempted using the identifying information of another person without authority.”¹³ The FTC’s rule defines “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, such as a name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, or employer or taxpayer identification number.¹⁴

This definition of “identity theft” in the FTC’s rule would be applicable to the Red Flag Regulations. Accordingly, “identity theft” within the meaning of the proposed Red Flag Regulations includes both actual and attempted identity theft.

5. Red Flag. The proposed definition of a “Red Flag” is a pattern, practice, or specific activity that indicates the possible risk of identity theft. This definition is based

¹¹ Under proposed § __.90(d)(1), this determination must 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.

¹² 15 U.S.C. 1681a(q)(3).

¹³ 69 FR 63922 (Nov. 3, 2004) (codified at 16 CFR 603.2(a)).

¹⁴ See 16 CFR 603.2(b) for additional examples of “identifying information,” including unique biometric identifiers.

on the statutory language. Section 114 states that in developing the Red Flag Guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate “the possible existence” of identity theft. In other words, the Red Flags identified by the Agencies must be indicators of “the possible existence” of “a fraud committed or attempted using the identifying information of another person without authority.”¹⁵

Section 114 also states that the purpose of the Red Flag Regulations is to identify “possible risks” to account holders or customers or to the safety and soundness of the institution or “customer”¹⁶ from identity theft. The Agencies believe that a “possible risk” of identity theft may exist even where the “possible existence” of identity theft is not necessarily indicated. For example, electronic messages to customers of financial institutions and creditors directing them to a fraudulent website in order to obtain their personal information (“phishing”), and a security breach involving the theft of personal information often are a means to acquire the information of another person for use in committing identity theft. Because of the linkage between these events and identity theft, the Agencies believe that it is important to include such precursors to identity theft as Red Flags. Defining these early warning signals as Red Flags will better position financial institutions and creditors to stop identity theft at its inception. Therefore, the Agencies have defined “Red Flags” expansively to include those precursors to identity theft which indicate “a possible risk” of identity theft to customers, financial institutions, and creditors.

¹⁵ See 16 CFR 603.2(a)(defining “identity theft”).

¹⁶ Use of the term “customer” here appears to be a drafting error and likely should read “creditor.”

The Agencies request comment on the scope of the definition of “Red Flags” and, specifically, whether the definition of Red Flags should include precursors to identity theft.

6. Service Provider. The proposed definition of “service provider” is a person that provides a service directly to the financial institution or creditor. This definition is based upon the definition of “service provider” in the Agencies’ standards implementing section 501(b) of the GLBA.¹⁷

§ __.90(c) Identity Theft Prevention Program.

Proposed paragraph § __.90(c) describes the primary objectives of the Program. It states 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 the safety and soundness of the financial institution or creditor, in the manner described in § __.90(d). The program must address financial, operational, compliance, reputation, and litigation risks.

The risks of identity theft to a customer may include financial, reputation and litigation risks that occur when another person uses a customer’s account fraudulently, such as by using the customer’s credit card account number to make unauthorized purchases. The risks of identity theft to the safety and soundness of the financial institution or creditor may include: compliance, reputation, or litigation risks for failure to adequately protect customers from identity theft; operational and financial risks from absorbing losses to customers who are the victims of identity theft; or losses to the

¹⁷ 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 xx (credit unions); 16 CFR part 314 (FTC regulated financial institutions).

financial institution or creditor from opening an account for a person engaged in identity theft. Addressing identity theft in these circumstances would not only benefit customers, but would also benefit the financial institution or creditor, and any person (who has no relationship with the financial institution or creditor) whose identity has been misappropriated.

In addition, proposed paragraph § __.90(c) states 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. Thus, the proposed Red Flag Regulations are flexible and take into account the operations of smaller institutions.¹⁸

Proposed paragraph § __.90(c) also states 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. The Program must also address changes in methods of identity theft, methods to detect, prevent, and mitigate identity theft, in the types of accounts the financial institution or creditor offers, and changes in its business arrangements, such as mergers and acquisitions, alliances and joint ventures, and service provider arrangements.

Thus, to ensure the Program's effectiveness in addressing the risk of identity theft to customers and to its own safety and soundness, each financial institution or creditor must monitor, evaluate, and adjust its Program, including the type of accounts covered, as appropriate. For example, a financial institution or creditor must periodically reassess whether to adjust the types of accounts covered by its Program and whether to adjust the

¹⁸ Agencies "are expected to take into account the limited personnel and resources available to smaller institutions and craft such regulations and guidelines in a manner that does not unduly burden these smaller institutions." See 149 Cong. Rec. E2513 (daily ed. December 8, 2003)(statement Rep. Oxley).

Red Flags that are a part of its Program based upon any changes in the types and methods of identity theft that it experiences.

§ __.90(d) Development and Implementation of Identity Theft Prevention Program.

1. Identification and Evaluation of Red Flags

i. Risk-based Red Flags

Under proposed paragraph § __.90(d)(1)(i), the Program must 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). The Red Flags identified must reflect changing identity theft risks to customers and to the financial institution or creditor as they arise. At a minimum, the Program must incorporate any relevant Red Flags from Appendix J, 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.

The proposed Red Flags enumerated in Appendix J are indicators of a possible risk of identity theft that the Agencies compiled from literature on the topic, information from credit bureaus, financial institutions, creditors, designers of fraud detection software, and the Agencies' own experiences. Some of the Red Flags may, by themselves, be reliable indicators of a possible risk of identity theft, such as a photograph on identification is not consistent with the appearance of the applicant. Some Red Flags may be less reliable except in combination with additional Red Flags, such as where a home phone number and address submitted on an application match the address and

number provided by another applicant. Such a match may be attributable to identity theft or, for example, it may indicate that the two applicants who share a residence are opening separate accounts.

The Agencies expect that the final Red Flag Regulations will apply to a wide variety of financial institutions and creditors that offer many different products and services, from credit cards to certain cell phone accounts. The Agencies are not proposing to prescribe which Red Flags will be relevant to a particular type of financial institution or creditor. For this reason, the proposed Regulations provide that each financial institution and creditor must identify for itself which Red Flags are relevant to detecting the risk of identity theft, based upon the risk evaluation described in § __.90(d)(1)(ii).

The Agencies recognize that some Red Flags that are relevant today may become obsolete as time passes. While the Agencies expect to update Appendix J periodically,¹⁹ 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. The Agencies may, however, be able to issue supervisory guidance more rapidly. Therefore, proposed paragraph § __.90(d)(1)(i) provides that each financial institution and creditor must have policies and procedures to identify any additional Red Flags that are relevant to detecting a possible risk of identity theft from applicable supervisory guidance, from 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.

¹⁹ Section 114 directs the Agencies to update the guidelines as often as necessary. See 15 U.S.C. 1681m(e)(1)(a).

Given the changing nature of identity theft, a financial institution or creditor must incorporate Red Flags on a continuing basis so that its Program reflects changing identity theft risks to customers and to the financial institution or creditor as they arise.

Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft. The Agencies request comment on whether the enumerated sources of Red Flags are appropriate.

The Agencies understand that many financial institutions and creditors already have implemented sophisticated policies and procedures to detect and prevent fraud, including identity theft, through such methods as detection of anomalous patterns of account usage. Often these policies and procedures include the use of complex computer-based products, such as sophisticated software. The Agencies attempted to draft this section in a flexible, technologically neutral manner that would not require financial institutions or creditors to acquire expensive new technology to comply with the Red Flag Regulations, and also would not prevent financial institutions and creditors from continuing to use their own or a third party's computer-based products. The Agencies note, however, that a financial institution or creditor that uses a third party's computer-based programs to detect fraud and identity theft must independently assess whether such programs meet the requirements of the Red Flag Regulations and Red Flag Guidelines and should not rely solely on the representations of the third party.

The Agencies request comment on the anticipated impact of this proposed paragraph on the policies and procedures that financial institutions and creditors currently have to detect, prevent, and mitigate identity theft, including on third party computer-based products that are currently being used to detect identity theft.

ii. Risk Evaluation

Proposed paragraph § __.90(d)(1)(ii) provides 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.

This provision describes a key part of the Program of a financial institution or creditor. Under proposed paragraph § __.90(d)(1)(ii), the financial institution or creditor must define the scope of its Program by assessing which of its accounts are subject to a risk of identity theft. For example, the financial institution or creditor must assess whether it will identify Red Flags in connection with extensions of credit only, or whether other types of relationships, such as deposit accounts, are likely to be subject to identity theft and should, therefore, be included in the scope of its Program. It must also assess whether to include solely the accounts of individual customers, or whether other types of accounts, such as those of small businesses, will be included in the scope of its Program. The financial institution or creditor must determine which Red Flags are relevant when it initially establishes its Program, and whenever it is necessary to address changing risks of identity theft.

The factors enumerated in proposed § __.90(d)(1)(ii) are nearly identical to those that each financial institution must consider when designing procedures for verifying the identity of customers opening new accounts in accordance with the Customer

Identification Program (CIP) rules, issued to implement section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l).²⁰ The Agencies believe that these CIP factors are equally relevant in the Red Flags context. For example, the Red Flags that may be relevant when an account is opened in a face-to-face transaction may be different from those relevant to an account that is opened remotely, by telephone, or over the Internet.

The Agencies solicit comment on whether the factors that must be considered are appropriate and whether any additional factors should be included.

2. Identity Theft Prevention and Mitigation

Proposed § __.90(d)(2) states 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 describes the following policies and procedures that the Program must include. Some of the policies and procedures relate solely to account openings. Others relate to existing accounts.

i. Verify Identity of Persons Opening Accounts

Proposed paragraph § __.90(d)(2)(i) states 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 is designed to address the risk of identity theft to a financial institution or creditor that occurs in connection with the opening of new accounts.

Some financial institutions and creditors already are subject to the CIP rules, which require verification of the identity of customers opening accounts. A financial institution or creditor may satisfy the proposed requirement in § __.90(d)(2)(i) to have

²⁰ 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).

policies and procedures for verifying the identity of a person opening an account by applying the policies and procedures for identity verification it has developed to comply with the CIP rules. However, the financial institution or creditor must use the CIP policies and procedures to verify the identity of any “customer,” meaning any person that opens a new account, in connection with any type of “account” that its risk evaluation indicates could be the subject of identity theft. By contrast, 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.” The Agencies are not proposing any exclusions from either of these terms given the risk-based nature of the Red Flag Regulations.²¹

The Agencies recognize, however, that not all financial institutions and creditors that must implement the Red Flag Regulations are required to comply with the CIP rules. This provision would allow any financial institution or creditor to follow the CIP rules to satisfy the Red Flag requirements to obtain identifying information about, and verify the identity of, a person opening an account. This approach is designed to ensure that, as stated in section 114, the Red Flag Guidelines are not inconsistent with the policies and procedures required by the CIP rules.

ii. Detect Red Flags

Proposed paragraph. § __.90(d)(2)(ii) states that the Program must include reasonable policies and procedures to detect the Red Flags identified pursuant to paragraph § __.90(d)(1).

iii. Assess the Risk of Identity Theft

²¹ See, e.g., 31 CFR 103.121(a).

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

Factors indicating that a Red Flag does not evidence a risk of identity theft might include: patterns of spending that are inconsistent with established patterns of activity on an account because the customer is traveling abroad, or an inconsistency between the social security number on an account application and a consumer report because numbers inadvertently were transposed during the application process.

iv. Address the Risk of Identity Theft

Proposed paragraph § __.90(d)(2)(iv) states that 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 Regulations then provide an illustrative list of measures that a financial institution or creditor may take,²² including:

A. Monitoring an account for evidence of identity theft;

B. Contacting the customer;

²² In the case of credit, the Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 *et seq.*, applies. 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.* 15 U.S.C. 1681c-1. Consequently, when a credit file contains a fraud or active duty alert, a creditor must take reasonable steps to verify the identity of the individual in accordance with the requirements in 15 U.S.C. 1681c-1 before extending credit, closing an account, or otherwise limiting the availability of credit. The inability of a creditor to verify the individual's identity may indicate that the individual is engaged in identity theft and, in those circumstances, the creditor may decline to open an account, close an account or take other reasonable actions to limit the availability of credit.

C. Changing any passwords, security codes, or other security devices that permit access to a customer's account;

D. Reopening an account with a new account number;

E. Not opening a new account;

F. Closing an existing account;

G. 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;

H. 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

I. 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.

Financial institutions and creditors typically use such measures to mitigate the risk of identity theft. In addition, measures E through G are actions that each financial institution subject to the CIP rules must include in its procedures for responding to circumstances in which it cannot form a reasonable belief that it knows the true identity of a customer.²³ Measure H describes the procedures required in section 112 of the FACT Act, 15 U.S.C. 1681c-1(h), that are applicable to a prospective user of credit reports when a user obtains a credit report that includes a fraud alert or active duty alert. Measure I describes the requirements in section 623 of the FCRA, 15 U.S.C. 1681s-2,

²³ See, e.g., 31 CFR 103.121(b)(2)(iii).

applicable to a furnisher of information to consumer reporting agencies that discovers inaccurate or incomplete information about a consumer.

These measures illustrate various actions that a financial institution or creditor may take depending upon the degree of risk that is present. For example, a financial institution or creditor may choose to contact a customer to determine whether a material change in credit card usage reflects purchases made by the customer or unauthorized charges. However, if the financial institution or creditor is notified that a customer provided his or her password and account number to a fraudulent website, it likely will close the customer's existing account and reopen it with a new account number.

The Agencies solicit comment on whether the enumerated measures should be included as examples that a financial institution or creditor may take and whether additional measures should be included.

3. Train Staff

Under proposed paragraph § __.90(d)(3), each financial institution or creditor must train staff to implement its Program. Proper training will enable staff to address the risk of identity theft. For example, staff should be trained to detect Red Flags with regard to new and existing accounts, such as discrepancies in identification presented by a person opening an account or anomalous wire transfers in connection with a customer's deposit account. Staff should also be trained to mitigate identity theft, for example, by recognizing when an account should not be opened.

4. Oversee Service Provider Arrangements

Proposed paragraph § __.90(d)(4) states that whenever a financial institution or creditor engages a service provider to perform an activity on its behalf that is covered by

§ __.90, the financial institution or creditor must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of paragraphs (c) and (d) of this section. For example, a financial institution or creditor that uses a service provider to open accounts on its behalf, may reserve for itself the responsibility to verify the identity of a person opening a new account, may direct the service provider to do so, or may use another service provider to verify identity. Ultimately, however, the financial institution or creditor remains responsible for ensuring that the activity is being conducted in compliance with a Program that meets the requirements of the Red Flag Regulations.

In addition, this provision would allow a service provider that provides services to 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 Red Flag 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.

Under the Agencies' Information Security Standards, financial institutions must require their service providers by contract to safeguard customer information in any manner that meets the objectives of the Standards. The Standards provide flexibility for a service provider's information security measures to differ from the program that a financial institution implements. By contrast, the CIP regulations do not contain a service provider provision. Instead, the preamble to the CIP regulations simply states that the CIP regulations do not affect a financial institution's authority to contract for services to be performed by a third party either on or off the institution's premises, and

also does not alter an institution's authority to use an agent to perform services on its behalf.²⁴ The Agencies invite comment on whether permitting a service provider to implement a Program, including policies and procedures to identify and detect Red Flags, that differs from the Programs of the individual financial institution or creditor to whom it is providing services, would fulfill the objectives of the Red Flag Regulations. The Agencies also invite comment on whether it is necessary to address service provider arrangements in the Red Flag Regulations, or whether it is self-evident that a financial institution or creditor remains responsible for complying with the standards set forth in the Regulations, including when it contracts with a third party to perform an activity on its behalf.

5. Involve the Board of Directors and Senior Management

Proposed § __.90(d)(5) highlights the responsibility of the board of directors and senior management to develop and implement the Program. The board of directors or an appropriate committee of the board must approve the written Program. The board, an appropriate committee of the board, or senior management is charged with overseeing the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation. In addition, persons charged with overseeing the Program must review reports that must be prepared at least annually by staff regarding compliance by the financial institution or creditor with the Red Flag Regulations. The 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

²⁴ 68 FR 25104 (May 9, 2003)(preamble to CIP rule applicable to banks, savings associations, and credit unions).

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. This report will indicate whether the Program must be adjusted to increase its effectiveness.

The Agencies request comment regarding the frequency with which reports should be prepared for the board, a board committee, or senior management. The Agencies also request comment on whether this paragraph properly allocates the responsibility for oversight and implementation of the Program between the board and senior management.

C. Proposed Red Flag Guidelines: Appendix J

Section 114 of the FACT Act states that in developing the guidelines, the Agencies are directed to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The Agencies are proposing to implement this provision by requiring the Program of a financial institution or creditor to include policies and procedures that require the identification and detection of risk-based Red Flags.

As discussed earlier, the Program must include policies and procedures designed to identify Red Flags relevant to detecting a possible risk of identity theft from among those listed in Appendix J. The proposed Red Flags enumerated in Appendix J are indicators of a possible risk of identity theft that the Agencies compiled from a variety of sources. Appendix J covers Red Flags that may be detected in connection with an account opening or an existing account. 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.

Recognizing that a wide range of financial institutions and creditors and a broad variety of accounts will be covered by the Red Flag Regulations, the proposed Regulations provide each financial institution and creditor with the flexibility to develop policies and procedures to identify which Red Flags in Appendix J are relevant to detecting the possible risk of identity theft.

The proposed list in Appendix J is not meant to be exhaustive. Therefore, proposed § __.90(d)(1) of the Red Flag Regulations also provide that each financial institution and creditor must have policies and procedures to identify additional Red Flags from applicable supervisory guidance that may be issued from time-to-time, 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. Ultimately, the financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent and mitigate identity theft.

The Agencies solicit comment on whether the proposed Red Flags listed in Appendix J are too specific or not specific enough, and whether additional or different Red Flags should be included.

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 Agencies considered whether to incorporate

this provision directly into Appendix J, but determined that the two-year limit may not be an accurate indicator of identity theft given the wide variety of credit and deposit accounts that would be covered by the provision.

The Agencies have concluded, however, that activity in connection with an account that has been inactive for a period of time may be an indicator of a possible risk of identity theft, depending upon the circumstances. Therefore, the Agencies have incorporated a Red Flag on inactive accounts into Appendix J that is flexible and is designed to take into consideration the type of account, the expected pattern of usage of the account, and any other relevant factors.

The Agencies request comment on whether a provision that mirrors the statutory language regarding inactive accounts should be placed directly into Appendix J or the Red Flag Regulations, or whether the more flexible approach to inactive accounts proposed (*i.e.*, listing as a Red Flag the use of an account that has been inactive for a reasonably lengthy period of time) should be retained.

The Agencies also request comment on whether, for ease of use, this appendix should be moved to the end of Subpart J or remain at the end of the part as proposed.

D. Proposed Special Rules for Card Issuers: Section-by-Section Analysis

§ __.91 Duties of card issuers regarding changes of address.

§ __.91(a) Scope.

Section 114 specifically provides that the Agencies must prescribe regulations requiring credit and debit card issuers to assess the validity of change of address requests. Therefore, in addition to the general rule in § __.90 that applies to all financial institutions and creditors, the Agencies are proposing regulations for card issuers, namely

a person described in § __.90(a) that issues a debit or credit card. A financial institution or creditor that is a card issuer may incorporate the requirements of § __.91 into its Program.

§ __.91(b) Definitions.

The proposed regulations include two definitions that are solely applicable to the special rule for card issuers. The first proposed definition is for the term “cardholder.” Section 114 states that the regulations must require the 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 statute. The legislative history 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.”²⁵ Presumably, the request will be valid if the consumer making the request and the cardholder are one and the same “consumer.” Therefore, the proposal defines “cardholder” as a consumer who has been issued a credit or debit card. Further, because “consumer” is defined in the FCRA as an “individual”²⁶ the proposed regulations will cover a request by an individual for a business card. The Agencies request comment on whether this definition of “cardholder” is appropriate.

The second proposed definition is for the phrase “clear and conspicuous.” Section § __.91 includes a provision requiring that any written or electronic notice

²⁵ See 149 Cong. Rec. E2513 (daily ed. December 8, 2003) (statement of Rep. Oxley) (emphasis added).

²⁶ 15 U.S.C. 1681a(c).

provided by a card issuer to the consumer pursuant to the regulations be given in a “clear and conspicuous manner.” The proposed regulations define “clear and conspicuous” based on the definition of this phrase found in the Agencies’ privacy regulations.²⁷

The Agencies request comment on whether, for ease of use, the regulations implementing section 315 should define additional terms, such as “card issuer,” “credit card,” and “debit card,” that are already defined in the FCRA.

§ __.91(c) General Requirements.

As required by section 114, proposed § __.91(c) states that a card issuer that 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) receives a request for an additional or replacement card for the same account, may not honor the request and issue such a card, unless it assesses the validity of the change of address request in at least one of three ways. As specified in section 114, proposed paragraph § __.91(c) provides that, in accordance with the card issuer’s reasonable policies and procedures, and for the purpose of assessing the validity of the change of address, the card issuer must:

(i) Notify the cardholder of the request at the cardholder’s former address and provide to the cardholder a means of promptly reporting incorrect address changes;

(ii) Notify the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or

²⁷ 12 CFR 40.3(b)(1) (OCC); 12 CFR 216.3(b)(1) (Board); 12 CFR 332.3(b)(1) (FDIC); 12 CFR 573.3(b)(1) (OTS); 12 CFR 716.3(b)(1) (NCUA); 16 CFR xx (FTC).

(iii) Use other means of assessing the validity of the change of address, in accordance with the policies and procedures that the card issuer has established pursuant to § __.90.

The proposed rule text specifies that the notification of a change of address must pertain to a “consumer’s” debit or credit account, consistent with the legislative history discussed above.²⁸

The Agencies request comment on this provision and, in particular, whether the Agencies should elaborate further on the means that a card issuer must use to assess the validity of a request for a change of address.

§ __.91(d) Form of Notice.

The Agencies note that section 114 is titled “Establishment of Procedures for the Identification of Possible Instances of Identity Theft.” The Agencies understand that Congress singled out this scenario involving card issuers and placed it in section 114 because it is well known to be a possible indicator of identity theft. The Agencies believe that a consumer needs to be able to recognize the urgent nature of a written or electronic notice that he or she receives from a card issuer pursuant to § __.91(d). Therefore, the proposed regulations prescribe the form that such a notice should take. They state 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. Of course, a card issuer may give notice orally in accordance with the policies and procedures the cardholder has established pursuant to § __.90(b).

²⁸ See 149 Cong. Rec. E2513 (daily ed. December 8, 2003) (statement of Rep. Oxley) (describing this section as relating to “issuers of credit cards and debit cards who receive a consumer request for an additional or replacement card for an existing account.” (Emphasis added.))

The Agencies request comment on whether this section should elaborate further on the form that a notice provided under § __.91(d) must take.

II. 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 section (h). Section 315 requires that, when providing consumer reports to requesting users, nationwide consumer reporting agencies (as defined in section 603(p) of the FCRA) (CRAs) 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 315 also requires the Agencies to jointly issue 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. These regulations must describe reasonable policies and procedures for users of consumer reports to (i) enable them 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. Proposed Regulation Implementing Section 315: Section-by-Section Analysis

§ __.82(a) Scope.

The scope of section 315 differs from the scope of section 114. 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.

§ __.82(b) Definition.

The proposed rule defines “notice of address discrepancy,” a new term introduced in section 315.²⁹ The proposed definition is “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 difference³⁰ 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.”

The Agencies note that the provisions of section 315 requiring CRAs to provide notices of address discrepancy became effective on December 1, 2004. To the extent that CRAs each have developed their own standards for delivery of notices of address discrepancy, it is particularly 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.

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

Proposed § __.82(c) implements the requirement in section 315 that the Agencies prescribe regulations describing reasonable policies and procedures that will enable the user to form a reasonable belief that the user knows “the identity of the person to whom

²⁹ All other terms used in this section of the proposal have the same meanings as set forth in the FCRA (15 U.S.C. 1681a).

³⁰ The term used in the statute, “substantially differs,” is not defined. CRAs are responsible for determining when addresses substantially differ and, hence, when they must send a notice of address discrepancy to a user requesting a consumer report.

the consumer report pertains” when the user receives a notice of address discrepancy. Proposed § __.82(c) states 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. 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.

This section also provides that if a user employs the policies and procedures regarding identification and verification set forth in the CIP rules,³¹ it satisfies the requirement to have policies and procedures to verify the identity of the consumer. This provision takes into consideration 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, such a user could use its existing CIP policies and procedures to satisfy this requirement, so long as it applies them in all situations where it receives a notice of address discrepancy. In addition, any user, such as a landlord or employer, may adopt the CIP rules and apply them in all situations where it receives an address discrepancy to meet this requirement, even if it is not subject to a CIP rule.

The Agencies request comment on whether the CIP procedures are 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

³¹ See, e.g., 31 CFR 103.121(b)(2)(i) and (ii).

report, both in connection with the opening of an account, and in other circumstances where a user obtains a consumer report.³²

The statutory requirement that a user must 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. By contrast, the additional statutory requirement that a user reconcile the address of the consumer with the CRA only applies if the user establishes a continuing relationship with the consumer.

The requirement that the user form a reasonable belief that it knows the identity of the consumer is likely to benefit both consumers and users. For example, this requirement should reduce the likelihood that a user will rely on the wrong consumer report in making a decision about a consumer's eligibility for a product, such as the consumer report of another consumer with the same name who lives at a different address. In addition, these policies and procedures may assist the user to detect whether a consumer about whom it has requested a consumer report is engaged in identity theft or is a victim of identity theft.³³

§ __.82(d)(1) Requirement to furnish consumer's address to a consumer reporting agency.

Proposed § __.82(d)(1) provides that a user must develop and implement reasonable policies and procedures for furnishing to the CRA from whom it received the

³² For example, a user may request a consumer report on a consumer with whom it already has a continuing relationship in order to determine whether to increase the consumer's credit line, or in other circumstances, such as in the case of a landlord or employer, to determine a consumer's eligibility to rent housing or for employment.

³³ Under the Red Flag Guidelines, a notice of address discrepancy received from a consumer reporting agency is a Red Flag. Thus, a user subject to the Red Flag Regulations that receives a notice of address discrepancy will need to determine whether its policies and procedures regarding identity theft prevention and mitigation apply here.

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 set forth in proposed § __.82(d)(1)(i) is 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 will ensure that the user furnishes a new address for the consumer to the CRA only after the user forms a reasonable belief that it knows the identity of the consumer, using the policies and procedures set forth in paragraph § __.82(c).

The second condition, set forth in proposed § __.82(d)(1)(ii), is 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) reiterates this requirement. However, a user also may obtain a notice of address discrepancy in connection with a consumer with whom it already has an existing relationship. Section 315 provides the Agencies with broad authority to prescribe regulations in all circumstances when a user has received a notice of address discrepancy. The Agencies have exercised this authority to provide that the user must also 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, as required by section 315, the third condition set out in proposed § __.82(d)(1)(iii) is 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.

§ __.82(d)(2) Requirement to confirm consumer's address.

The Agencies note that section 315 requires the Agencies 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.) Even when the user is able to form a reasonable belief that it knows the identity of the consumer, there may be many reasons that 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 that is furnished to the CRA is accurate, the Agencies are proposing to interpret the phrase, “such address,” as an address that the user has reasonably confirmed is accurate. This interpretation requires 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 to the CRA. Proposed § __.82(d)(2) contains 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 solicit comment on whether the regulation should include examples of measures to reasonably confirm the accuracy of the consumer's address, or whether different or additional examples should be listed.

§ __.82(d)(3) Timing.

Section 315 specifically addresses 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) states that, with respect to new relationships, the policies and procedures that 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.

However, a user may also receive a notice of address discrepancy in other circumstances, such as when it requests a consumer report for a consumer with whom it already has an existing relationship. As previously noted, section 315 provides the Agencies with broad authority to prescribe regulations in all circumstances when a user has received a notice of discrepancy. Thus, proposed paragraph § __.82(d)(3)(ii) states 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 recognize that the timing provision for newly established relationships may be problematic for users hoping to take full advantage of the flexibility

in the timing for verification of identity afforded by the CIP rules. As required by statute, proposed § __.82(d)(3)(i), the timing provision for new relationships, states 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 mirrors the requirement of the statute, requires 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. However, in this context, and in order to satisfy the requirements of both § __.82(d)(1) and § __.82(d)(3)(i), a user employing the CIP rules will have to both establish a continuing relationship and a reasonable belief that it knows the consumer's identity during the same reporting period.

The Agencies request 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.

III. General Provisions

The Agencies are proposing to amend the first sentence in § __.3, which contains the definitions that are applicable throughout this part. This sentence currently states that the list of definitions in § __.3 apply throughout the part “unless the context requires otherwise.” The Agencies are proposing 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.

IV. Regulatory Analysis

A. Paperwork Reduction Act

I. Request for Comment on Proposed Information Collection

In accordance with the requirements of the Paperwork Reduction Act of 1995, the Agencies may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The Agencies are requesting comment on a proposed information collection. The Agencies also give notice that, at the end of the comment period, the proposed collections of information, along with an analysis of the comments and recommendations received, will be submitted to OMB for review and approval.

Comments are invited on:

(a) Whether the collection of information is necessary for the proper performance of the Agency's functions, including whether the information has practical utility;

(b) The accuracy of the estimates of the burden of the information collection, including the validity of the methodology and assumptions used;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start up costs and costs of operation, maintenance, and

purchase of services to provide information.

At the end of the comment period, the comments and recommendations received will be analyzed to determine the extent to which the information collections should be modified prior to submission to OMB for review and approval. The comments will also be summarized or included in the Agencies' requests to OMB for approval of the collections. All comments will become a matter of public record.

Comments should be addressed to:

OCC:

Communications Division, Office of the Comptroller of the Currency, Public Information Room, Mail stop 1-5, Attention: 1557-NEW, 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. You can

make an appointment to inspect the comments by calling 202-874-5043.

Board: You may submit comments, identified by _____, by any of the following methods:

- Agency Web Site: <http://www.federalreserve.gov>. Follow the instructions for submitting comments on the [http://](http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm)

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, except as necessary 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 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-____, 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 infocollection.comments@ots.treas.gov. OTS will post comments and the 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.

FTC: Interested parties are invited to submit written comments. Comments should refer to “The Red Flags Rule: FTC File No. ____ ” to facilitate the organization of comments. A comment filed in paper form should include this reference 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 J), 600 Pennsylvania Avenue, N.W., 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 below. 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 must be clearly labeled “Confidential.”¹ The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible. 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>. 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.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should

¹Commission 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).

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 will be considered by the Commission and will be available to the public on the FTC website, to the extent practicable, at www.ftc.gov. 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 website. 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>

II. Proposed Information Collection

Title of Information Collection: Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2002.

Frequency of Response: On occasion.

Affected Public:

OCC: National banks and Federal branches and agencies of foreign banks and certain subsidiaries of these entities.

Board: State member banks, bank holding companies, affiliates and certain non-bank subsidiaries of bank holding companies, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations.

FDIC: Insured nonmember banks, insured state branches of foreign banks, and certain subsidiaries of these entities.

OTS: Savings associations and certain of their subsidiaries.

Abstract:

Section 114: As required by section 114, the Agencies are jointly proposing guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. The Agencies also are proposing joint regulations requiring each financial institution and creditor to establish reasonable policies and procedures to address the risk of identity theft that incorporate the guidelines. In addition, credit and debit card issuers must develop policies and procedures to assess the validity of a request for a change of address under certain circumstances.

The information collections in the proposed regulations implementing section 114 would require each financial institution and creditor to create an Identity Theft Prevention Program (Program) and report to the board of directors, a committee thereof or senior management at least annually on compliance with the proposed regulations. Staff must be trained to implement the Program. In addition, each credit and debit card issuer would be required to establish policies and procedures to assess the validity of a change of address request. The proposed regulation requires the card issuer to notify the cardholder in writing, electronically, or orally, or use another means of assessing the validity of the change of address.

Section 315: The Agencies are proposing joint regulations under section 315 that 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 information collections in the proposed regulations implementing section 315 would require each user of consumer reports to develop reasonable policies and procedures that it will employ when it receives a notice of address discrepancy from a consumer reporting agency. The proposed regulation requires 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.

Estimated Burden:³⁴

Section 114: The Agencies estimate that it will initially take financial institutions and creditors 25 hours to create the Program outlined in the proposed rule, 4 hours to prepare an annual report, and 2 hours to train staff to implement the Program.

The Agencies estimate that it will take credit and debit card issuers 4 hours to develop policies and procedures to assess the validity of a change of address request.

The Agencies believe that most of the covered entities already employ a variety of measures to detect and address identity theft that are required by section 114 of the proposed regulation because these are usual and customary business practices that they engage in 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 proposed regulation implementing section 114 as a result of having to comply with other existing regulations and guidance, such as the regulations implementing section 326

³⁴ The Estimated Burden section that follows it reflect the views of all of the Agencies except the FTC, which has prepared a separate analysis.

of the USA PATRIOT Act, 31 U.S.C. 5318(l),³⁵ 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,³⁶ and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs.³⁷ The Agencies also 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. Therefore implementation of this requirement will pose no further burden. Accordingly, these estimates represent the incremental amount of time the Agencies believe it will take to create a written Program that incorporates the policies and procedures that covered entities are likely to already have in place, the incremental time to train staff to implement the Program, to establish policies and procedures to assess the validity of changes of address, and to notify cardholders, as appropriate.

Section 315: The Agencies estimate that it will take users of consumer reports 4 hours to develop policies and procedures that they will employ when they receive a notice of address discrepancy. The Agencies believe that users of credit reports covered by this

³⁵ 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).

³⁶ 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); 16 CFR part 314 (financial institutions that are not regulated by the Board, FDIC, NCUA, OCC and OTS).

³⁷ 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); 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; "Guidance on Identity Theft and Pretext Calling," OCC AL 2001-4 (April 30, 2001); "Phishing and E-mail Scams," OTS CEO Letter #193 (Mar. 8, 2004); "Identity Theft and Pretext Calling," OTS CEO Letter #139 (May 4, 2001). [add other agency cites].

analysis already are furnishing this information to consumer reporting agencies because it is a usual and customary business practice. Therefore, the Agencies estimate that there will be no implementation burden.

Thus, the burden associated with this collection of information may be summarized as follows.

OCC:

Number of respondents: 2,100

Estimated time per response: 39

Developing program: 25

Preparing annual report: 4

Training: 2

Developing policies and procedures to assess validity of changes of address: 4

Developing policies and procedures to respond to notices of address discrepancy: 4

Total estimated annual burden: 81,900

Board:

Number of respondents: 9,876

Estimated time per response: 39 hours

Developing program: 25 hours

Preparing annual report: 4 hours

Training: 2 hours

Developing policies and procedures to assess validity of changes of address: 4 hours

Developing policies and procedures to respond to notices of address discrepancy: 4 hours

Total Estimated Annual Burden: 385,164

FDIC:

Number of respondents: 5,245

Estimated time per response: 39 hours

Developing program: 25 hours

Preparing annual report: 4 hours

Training: 2 hours

Developing policies and procedures to assess validity of changes of address: 4 hours

Developing policies and procedures to respond to notices of address discrepancy: 4 hours

Total Estimated Annual Burden: 204,555 hours

OTS:

Number of respondents: 858

Estimated time per response: 39 hours

Developing program: 25 hours

Preparing annual report: 4 hours

Training: 2 hours

Developing policies and procedures to assess validity of changes of address: 4 hours

Developing policies and procedures to respond to notices of address discrepancy: 4 hours

Total Estimated Annual Burden: 33,462

NCUA:

Number of respondents:

Estimated time per Response:

Developing program:

Preparing annual report:

Training:

Developing policies and procedures to assess validity of changes of address:

Developing policies and procedures to respond to notice of address discrepancy:

Total Estimated Annual Burden:

FTC:

Number of respondents:

Estimated time per response:

Developing program:

Preparing annual report:

Developing policies and procedures to assess validity of changes of address:

Developing policies and procedures to respond to notices of address discrepancy:

Total Estimated Annual Burden:

B. Regulatory Flexibility Act

OCC: When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (RFA), requires the agency to publish an initial regulatory flexibility analysis unless the agency certifies that the rule will not have “a significant economic impact on a substantial number of small entities.”³⁸ 5 U.S.C. 603, 605(b). The OCC has reviewed the impact of the proposed regulations on small banks and certifies that that proposed regulations, if adopted as proposed, would not have a significant economic impact on a substantial number of small entities.

The proposed rulemaking implements sections 114 and 315 of the FACT Act and applies to all national banks, Federal branches and agencies and their operating

³⁸ Small Business Administration regulations define “small entities” to include banks with total assets of \$165 million or less. 13 CFR 121.201.

subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act,³⁹ 1,011 of which have assets of less than or equal to \$165 million.

The proposed regulations implementing section 114 require the development and establishment of a written identity theft prevention program to detect, prevent, and mitigate identity theft. The proposed regulations also require card issuers to assess the validity of a notice of address change under certain circumstances.

The OCC believes that the requirements in 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 accounts. Banks also are likely to have implemented most of the proposed requirements as a result of having to comply with other existing regulations and guidance. For example, national banks are already subject to CIP rules requiring them to verify the identity of a person opening a new account.⁴⁰ A covered entity may use the policies and procedures developed to comply with the CIP rules to satisfy the identity verification requirements in the proposed rules.

National banks complying with the "Interagency Guidelines Establishing Information Security Standards"⁴¹ and guidance recently issued by the FFIEC titled "Authentication in an Internet Banking Environment"⁴² already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems. Banks complying with the OCC's "Guidance on Identity Theft and Pretext

³⁹ For convenience, these entities are referred to as "national banks."

⁴⁰ 31 CFR 103.121; 12 CFR 21.21 (national banks).

⁴¹ 12 CFR part 30, app. B (national banks).

⁴² OCC Bulletin 2005-25 (Oct. 12, 2005).

Calling”⁴³ already will have policies and procedures to verify the validity of change of address requests on existing accounts.

In addition, the flexibility incorporated into the proposed rulemaking provides a covered entity with discretion to design and implement a program that is tailored to its size and complexity and the nature and scope of its operations. In this regard, the OCC believes that expenditures associated with establishing and implementing an identity theft prevention program will be commensurate with the size of the bank.

The OCC believes that the proposed regulations implementing section 114, if adopted as proposed, will not impose undue costs on national banks and will not have a substantial economic impact on a substantial number of small national banks. Nonetheless, the OCC specifically requests 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 requests comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

The regulations implementing section 315 require users of consumer reports to have various policies and procedures to respond to the receipt of an address discrepancy. The FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. The OCC understands that as a matter of good business practice, most national banks currently have policies and procedures in place to respond to these notices when they are provided in connection with both new and existing accounts, by furnishing

⁴³ OCC AL 2001-3 (April 30, 2001).

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. In addition, 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.

Given current practices of national banks in responding to notices of address discrepancy from CRAs, and the existing requirements in the CIP rule, the OCC believes that the proposed regulations implementing section 315, if adopted as proposed, will not impose undue costs on national banks and likely will not have a significant economic impact on a substantial number of national banks. Nonetheless, the OCC specifically requests 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 to minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

FDIC: In accordance with the Regulatory Flexibility Act (5 U.S.C. 601-612) (RFA), an agency must publish an initial regulatory flexibility analysis with its proposed rule, unless the agency certifies 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 million in assets). The FDIC hereby certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities.

Under the proposed rule, financial institutions and creditors must have a written program that includes controls to address the identity theft risks they have identified. With respect to credit and debit card issuers, the program also must include policies and procedures to assess the validity of change of address requests. Users of consumer reports must have reasonable policies and procedures with respect to address discrepancies. The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities, and be flexible to address changing identity theft risks as they arise. A financial institution or creditor may wish to combine its program to prevent identity theft with its information security program, as these programs are complementary in many ways.

The proposed rule would apply to all FDIC-insured state nonmember banks, approximately 3,400 of which are small entities. The proposed 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 proposed rule would also permit institutions to modify existing information security programs to address identity theft. The FDIC also believes that many institutions have already implemented a significant portion of the detection and mitigation efforts required by the proposed rule.

OTS: When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (RFA), requires the agency to publish an initial regulatory flexibility analysis unless the agency certifies that the rule will not have “a significant economic impact on a substantial number of small entities.”⁴⁴ 5 U.S.C. 603, 605(b). OTS has reviewed the

⁴⁴ Small Business Administration regulations define “small entities” to include savings associations with total assets of \$165 million or less. 13 CFR 121.201.

impact of the proposed regulations on small savings associations and certifies that that proposed regulations, if adopted as proposed, would not have a significant economic impact on a substantial number of small entities.

The proposed rulemaking would implement sections 114 and 315 of the FACT Act and would apply to all savings associations (and federal savings association operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act),⁴⁵ 446 of which have assets of less than or equal to \$165 million.

The proposed regulations implementing section 114 would require the development and establishment of a written identity theft prevention program to detect, prevent, and mitigate identity theft. The proposed regulations also would require card issuers to assess the validity of a notice of address change under certain circumstances.

OTS believes that the proposed requirements implementing section 114 of the FACT Act would be consistent with savings associations' usual and customary business practices used to minimize losses due to fraud in connection with new and existing accounts. Savings associations also are likely to have implemented most of the proposed requirements as a result of having to comply with other existing regulations and guidance. For example, savings associations are already subject to CIP rules requiring them to verify the identity of a person opening a new account.⁴⁶ A covered entity may use the policies and procedures developed to comply with the CIP rules to satisfy the identity verification requirements in the proposed rules.

⁴⁵ For convenience, these entities are referred to as "savings associations."

⁴⁶ 31 CFR 103.121; 12 CFR 563.177 (savings associations).

Savings associations complying with the “Interagency Guidelines Establishing Information Security Standards”⁴⁷ and guidance recently issued by the FFIEC titled “Authentication in an Internet Banking Environment”⁴⁸ already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems. Savings associations complying with OTS’s guidance on “Identity Theft and Pretext Calling”⁴⁹ already will have policies and procedures to verify the validity of change of address requests on existing accounts.

In addition, the flexibility incorporated into the proposed rulemaking provides a covered entity with discretion to design and implement a program that is tailored to its size and complexity and the nature and scope of its operations. In this regard, OTS believes that expenditures associated with establishing and implementing a program would be commensurate with the size of the savings associations.

OTS believes that the proposed regulations implementing section 114 would not impose undue costs on savings associations and likely would have a minimal economic impact on small savings associations. Nonetheless, OTS specifically requests comment and specific data on the size of the incremental burden creating a program would have on small savings associations, given their current practices and compliance with existing requirements. OTS also requests comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

⁴⁷ 12 CFR part 570, app. B (savings associations).

⁴⁸ OTS CEO Letter 228 (Oct. 12, 2005).

⁴⁹ “Identity Theft and Pretext Calling,” OTS CEO Letter #139 (May 4, 2001).

The proposed regulations implementing section 315 would require users of consumer reports to have various policies and procedures to respond to the receipt of an address discrepancy. The FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. OTS understands that as a matter of good business practice, most savings associations currently have policies and procedures in place to respond to these notices when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the savings association has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy. In addition, 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.

Given current practices of savings associations in responding to notices of address discrepancy from CRAs, and the existing requirements in the CIP rule, OTS believes that the proposed regulations implementing section 315 would not impose undue costs on savings associations and likely would have a minimal economic impact on small savings associations. Nonetheless, OTS specifically requests comment on whether the proposed requirements differ from small savings associations' current practices and how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

FDIC: In accordance with the Regulatory Flexibility Act (5 U.S.C. 601-612) (RFA), an agency must publish an initial regulatory flexibility analysis with its proposed rule, unless the agency certifies 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 million in assets). The FDIC hereby certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities.

Under the proposed rule, financial institutions and creditors must have a written program that includes controls to address the identity theft risks they have identified. With respect to credit and debit card issuers, the program also must include policies and procedures to assess the validity of change of address requests. Users of consumer reports must have reasonable policies and procedures with respect to address discrepancies. The program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities, and be flexible to address changing identity theft risks as they arise. A financial institution or creditor may wish to combine its program to prevent identity theft with its information security program, as these programs are complementary in many ways.

The proposed rule would apply to all FDIC-insured state nonmember banks, approximately 3,400 of which are small entities. The proposed 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 proposed rule would also permit institutions to modify existing information security programs to address identity theft. The FDIC also believes that many institutions have already implemented a significant portion of the detection and mitigation efforts required by the proposed rule.

C. OCC and OTS Executive Order 12866 Determination

The OCC and the OTS have each determined that this proposed rulemaking, mandated by sections 114 and 315 of the FACT Act, is not a significant regulatory action under Executive Order 12866.

The OCC and OTS believe that national banks and savings associations, respectively, already have procedures in place that fulfill many of the requirements of the proposed regulations because they are consistent with institutions' usual and customary business practices used to minimize losses due to fraud in connection with new and existing accounts. Institutions also are likely to have implemented many of the proposed requirements as a result of complying with other existing regulations and guidance. For these reasons, and for the reasons discussed elsewhere in this preamble, the OCC and OTS each believes that the burden stemming from this rulemaking will not cause the proposed rules to be a "significant regulatory action."

Nevertheless, because the proposed rulemaking implements new statutory requirements, it may impose costs on some national banks and savings associations by requiring them to formalize or enhance their existing policies and procedures. Therefore, the OCC and OTS invite national banks, savings associations and the public to provide any cost estimates and related data that they think would be useful in evaluating the overall costs of this rulemaking. The OCC and OTS will review any comments and cost data provided carefully, and will revisit the cost aspects of the proposed rules in developing final rules.

D. OCC and OTS Executive Order 13132 Determination

The OCC and the OTS have each determined that this proposal does 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. The proposed rule applies 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 this proposed rule does 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) requires 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 sector, of \$100 million or more in any one year (adjusted annually for inflation). 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 believes that the financial institutions subject to their jurisdiction covered by the proposed rules already have identity theft prevention programs because it is a sound business practice. In addition, key elements of the proposed rules are elements in existing regulations and guidance. Therefore, the OCC

and OTS have each determined that this proposed rule will not result in expenditures by State, local, and tribal governments, or by the private sector, that exceed the expenditure threshold. Accordingly, neither the OCC nor OTS has prepared a budgetary impact statement or specifically addressed 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 this proposed rule would 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. Community Bank Comment Request

The Agencies invite your comments on the impact of this proposal on community banks. The Agencies recognize that community banks operate with more limited resources than larger institutions and may present a different risk profile. Thus, the Agencies specifically request comment on the impact of the proposal on community banks' current resources and available personnel with the requisite expertise, and whether the goals of the proposal could be achieved, for community banks, through an alternative approach.

IV. Solicitation of Comments on Use of Plain Language

Section 722 of the Gramm-Leach-Bliley Act, Pub. L. 106-102, sec. 722, 113 Stat. 1338, 1471 (Nov. 12, 1999), requires the OCC, Board, FDIC, and OTS to use plain language in all proposed and final rules published after January 1, 2000. Therefore, these agencies specifically invite your comments on how to make this proposal easier to understand. For example:

- Have we organized the material to suit your needs? If not, how could this material be better organized?
- Are the requirements in the proposed guidelines and regulations clearly stated? If not, how could the guidelines and regulations be more clearly stated?
- Do the proposed guidelines and regulations contain language or jargon that is not clear? If so, which language requires clarification?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the guidelines and regulations easier to understand? If so, what changes to the format would make them easier to understand?
- What else could we do to make the guidelines and regulations easier to understand?

NCUA Regulatory Goal

NCUA's goal is to promulgate clear and understandable regulations that impose minimal regulatory burden. We request your comments on whether the proposed rule is understandable and minimally intrusive if implemented as proposed.

List of Subjects

12 CFR Part 41

Banks, banking, Consumer protection, National Banks, Reporting and recordkeeping requirements.

12 CFR Part 211

Exports, Foreign banking, Holding companies, 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

[to be added]

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 proposes to amend chapter I of title 12 of the Code of Federal Regulations by amending 12 CFR part 41 as follows:

PART 41 – FAIR CREDIT REPORTING

1. The authority citation for part 41 is revised to read as follows:

Authority: 12 U.S.C. 1 et seq., 24(Seventh), 93a, 481, and 1818; 15 U.S.C. 1681c, 1681m, 1681s, 1681w, 6801 and 6805.

Subpart A – General Provisions

2. Amend § 41.3 by revising the introductory text to read as follows:

§ 41.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

Subpart I - Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

3. Revise the heading for Subpart I as shown above.

4. Add § 41.82 to read as follows:

§ 41.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as “users”), and that are national banks, Federal branches and agencies of foreign banks, 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) Definition. For purposes of this section, a notice of address discrepancy means a notice sent to a user of a consumer report 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) Requirement to form a reasonable belief. 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 and for whom it receives a notice of address discrepancy. These policies and procedures must be designed to enable the user either to form a reasonable belief that it knows the identity of the consumer or determine that it cannot do so. A user that employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l) under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules.

(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 it knows the identity of the consumer for whom the consumer report was obtained;
- (ii) Establishes or maintains 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 pertaining to the consumer was obtained.

(2) Requirement to confirm consumer's address. The user may reasonably confirm an address is accurate by:

- (i) Verifying the address with the person to whom the consumer report pertains;

(ii) Reviewing its own records of the address provided to request the consumer report;

(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:

(i) With respect to new relationships, for the reporting period in which it establishes a relationship with the consumer; and

(ii) In other circumstances, for the reporting period in which the user confirms the accuracy of the address of the consumer.

5. Add Subpart J to part 41 to read as follows:

Subpart J – Identity Theft Red Flags

41.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Purpose and scope. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are national banks, Federal branches and agencies of foreign banks, 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, the following definitions apply:

(1) Account means 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). Account includes:

(i) An extension of credit for personal, family, household or business purposes, such as a credit card account, margin account, or retail installment sales contract, such as a car loan or lease; and

(ii) A demand deposit, savings or other asset account for personal, family, household, or business purposes, such as a checking or savings account.

(2) The term board of directors includes:

(i) In the case of a foreign 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.

(3) Customer means a person that has an account with a financial institution or creditor.

(4) Identity theft has the same meaning as in 16 CFR 603.2(a).

(5) Red Flag means a pattern, practice, or specific activity that indicates the possible risk of identity theft.

(6) Service provider means a person that provides a service directly to the financial institution or creditor.

(c) Identity Theft Prevention Program. Each financial institution or creditor must implement a written Identity Theft Prevention Program (Program). The Program must

include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, operational, compliance, reputation, and litigation risks, in the manner discussed in paragraph (d) of this section. The Program must be:

(1) Appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities; and

(2) Designed to address changing identity theft risks as they arise in connection with the experiences 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 it offers, and business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(d) Development and implementation of Program. (1) Identification and evaluation of Red Flags. (i) Risk-based Red Flags. The Program must include policies and procedures to identify Red Flags, singly or in combination, that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor, using the risk evaluation set forth in paragraph (d)(1)(ii) of this section. The Red Flags identified must reflect changing identity theft risks to customers and to the financial institution or creditor as they arise. At a minimum, the Program must incorporate any relevant Red Flags from:

(A) Appendix J;

(B) Applicable supervisory guidance;

(C) Incidents of identity theft that the financial institution or creditor has experienced; and

(D) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.

(ii) Risk evaluation. In identifying which Red Flags are relevant, 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.

(2) Identity theft prevention and mitigation. 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, including policies and procedures to:

(i) Obtain identifying information about, and verify the identity of, a person opening an account. A financial institution or creditor that uses the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l), under these circumstances, satisfies this requirement whether or not the user is subject to the CIP rules;

(ii) Detect the Red Flags identified pursuant to paragraph (d)(1) of this section;

(iii) Assess whether the Red Flags detected pursuant to paragraph (d)(2)(ii) of this section evidence a risk of identity theft. An institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft; and

- (iv) Address the risk of identity theft, commensurate with the degree of risk posed, such as by:
- (A) Monitoring an 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 customer's account;
 - (D) Reopening an account with a new account number;
 - (E) Not opening a new account;
 - (F) Closing an existing account;
 - (G) 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;
 - (H) 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
 - (I) 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.
- (3) Staff training. Each financial institution or creditor must train staff to implement its Program.
- (4) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity on its behalf and the

requirements of its Program are applicable to that activity (such as account opening), the financial institution or creditor must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of paragraphs (c) and (d) of this section.

(5) Involvement of board of directors and senior management. (i) Board approval. The board of directors or an appropriate committee of the board must approve the written Program.

(ii) Oversight by board or senior management. The board of directors, an appropriate committee of the board, or senior management must oversee the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation, and reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with this section.

(iii) Reports. (A) In general. Staff of the financial institution or creditor responsible for implementation of its Program must report to the board, an appropriate committee of the board, or senior management, at least annually, on compliance by the financial institution or creditor with this section.

(B) Contents of report. The report 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.

§ 41.91 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 41.90(a) that issues a debit or credit card.

(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) In general. 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, unless, 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) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

(2) Notifies the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or

(3) Uses other means of assessing the validity of the change of address, in accordance with the policies and procedures the card issuer has established pursuant to section 41.90.

(d) Form of notice. Any written or electronic notice that the card issuer provides under this paragraph shall be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

6. Add and reserve appendices B-I.

7. Add Appendix J to part 41 to read as follows:

**APPENDIX J TO PART 41 – INTERAGENCY GUIDELINES ON
IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION
Red Flags in Connection with an Account Application or an Existing Account
Information from a Consumer Reporting Agency**

1. A fraud or active duty alert is included with a consumer report.
2. A notice of address discrepancy is provided by a consumer reporting agency.
3. 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.
 - d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification

4. Documents provided for identification appear to have been altered.
5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

7. Other information on the identification is not consistent with information that is on file, such as a signature card.

Personal Information

8. Personal information provided is inconsistent when compared against external information sources. *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.

9. Personal information provided is internally inconsistent. *For example,* there is a lack of correlation between the SSN range and date of birth.

10. Personal information provided is associated with known fraudulent activity. *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.

11. Personal information provided is of a type commonly associated with fraudulent activity. *For example:*

- a. The address on an application is fictitious, a mail drop, or prison.
- b. The phone number is invalid, or is associated with a pager or answering service.

12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.

13. The person opening the account or the customer fails to provide all required information on an application.

14. Personal information provided is not consistent with information that is on file.

15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Address Changes

16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional, or replacement checks, convenience checks, cards, or a cell phone, or for the addition of authorized users on the account.

17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

Anomalous Use of the Account

18. A new revolving credit account is used in a manner commonly associated with fraud. *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.

19. An 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.

20. An 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).

Notice from Customers or Others Regarding Customer Accounts

21. The financial institution or creditor is notified of unauthorized charges in connection with a customer's account.

22. The financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in identity theft.

23. The financial institution or creditor is notified that the customer is not receiving account statements.
24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.
25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.
27. An employee has accessed or downloaded an unusually large number of customer account records.
28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.
29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.
30. There are unusually frequent and large check orders in connection with a customer's account.
31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

For the reasons set forth in the joint preamble, the Federal Deposit Insurance Corporation proposes to amend chapter III of title 12 of the Code of Federal Regulations by amending 12 CFR parts 334 and 364 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 and 1819 (Tenth); 15 U.S.C. 1681b, 1681c, 1681m, 1681s, 1681w, 6801 and 6805.

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:

* * * * *

Subpart I – Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

3. Revise the heading for Subpart I as shown above.
4. Add § 334.82 to read as follows:

§ 334.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as “users”), and that are insured state nonmember banks, insured state licensed branches of foreign banks, or

subsidiaries 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 of a consumer report 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) Requirement to form a reasonable belief. 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 and for whom it receives a notice of address discrepancy. These policies and procedures must be designed to enable the user either to form a reasonable belief that it knows the identity of the consumer or determine that it cannot do so. A user that employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l) under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules.

(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 it knows the identity of the consumer for whom the consumer report was obtained;

- (ii) Establishes or maintains 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 pertaining to the consumer was obtained.

(2) Requirement to confirm consumer's address. The user may reasonably confirm an address is accurate by:

- (i) Verifying the address with the person to whom the consumer report pertains;
- (ii) Reviewing its own records of the address provided to request the consumer report;
- (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:

- (i) With respect to new relationships, for the reporting period in which it establishes a relationship with the consumer; and
- (ii) In other circumstances, for the reporting period in which the user confirms the accuracy of the address of the consumer.

5. Add Subpart J to part 334 to read as follows:

Subpart J – Identity Theft Red Flags

334.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Purpose and scope. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are insured state nonmember banks, insured state licensed branches of foreign banks, or subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) Definitions. For purposes of this section, the following definitions apply:

(1) Account means 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). Account includes:

(i) An extension of credit for personal, family, household or business purposes, such as a credit card account, margin account, or retail installment sales contract, such as a car loan or lease; and

(ii) A demand deposit, savings or other asset account for personal, family, household, or business purposes, such as a checking or savings account.

(2) The term board of directors includes:

(i) In the case of a foreign 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.

(3) Customer means a person that has an account with a financial institution or creditor.

(4) Identity theft has the same meaning as in 16 CFR 603.2(a).

(5) Red Flag means a pattern, practice, or specific activity that indicates the possible risk of identity theft.

(6) Service provider means a person that provides a service directly to the financial institution or creditor.

(c) Identity Theft Prevention Program. Each financial institution or creditor must implement a written Identity Theft Prevention Program (Program). The Program must include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, operational, compliance, reputation, and litigation risks, in the manner discussed in paragraph (d) of this section. The Program must be:

(1) Appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities; and

(2) Designed to address changing identity theft risks as they arise in connection with the experiences 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 it offers, and business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(d) Development and implementation of Program. (1) Identification and evaluation of Red Flags. (i) Risk-based Red Flags. The Program must include policies and procedures to identify Red Flags, singly or in combination, that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor, using the risk evaluation set forth in paragraph

(d)(1)(ii) of this section. The Red Flags identified must reflect changing identity theft risks to customers and to the financial institution or creditor as they arise. At a minimum, the Program must incorporate any relevant Red Flags from:

(A) Appendix J;

(B) Applicable supervisory guidance;

(C) Incidents of identity theft that the financial institution or creditor has experienced; and

(D) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.

(ii) Risk evaluation. In identifying which Red Flags are relevant, 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.

(2) Identity theft prevention and mitigation. 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, including policies and procedures to:

(i) Obtain identifying information about, and verify the identity of, a person opening an account. A financial institution or creditor that uses the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l), under these

circumstances, satisfies this requirement whether or not the user is subject to the CIP rules;

(ii) Detect the Red Flags identified pursuant to paragraph (d)(1) of this section;

(iii) Assess whether the Red Flags detected pursuant to paragraph (d)(2)(ii) of this section evidence a risk of identity theft. An institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft; and

(iv) Address the risk of identity theft, commensurate with the degree of risk posed, such as by:

(A) Monitoring an 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 customer's account;

(D) Reopening an account with a new account number;

(E) Not opening a new account;

(F) Closing an existing account;

(G) 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;

(H) 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

(I) 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.

(3) Staff training. Each financial institution or creditor must train staff to implement its Program.

(4) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity on its behalf and the requirements of its Program are applicable to that activity (such as account opening), the financial institution or creditor must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of paragraphs (c) and (d) of this section.

(5) Involvement of board of directors and senior management. (i) Board approval. The board of directors or an appropriate committee of the board must approve the written Program.

(ii) Oversight by board or senior management. The board of directors, an appropriate committee of the board, or senior management must oversee the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation, and reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with this section.

(iii) Reports. (A) In general. Staff of the financial institution or creditor responsible for implementation of its Program must report to the board, an appropriate committee of the board, or senior management, at least annually, on compliance by the financial institution or creditor with this section.

(B) Contents of report. The report 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.

§ 334.91 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 334.90(a) that issues a debit or credit card.

(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) In general. 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, unless, 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) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

(2) Notifies the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or

(3) Uses other means of assessing the validity of the change of address, in accordance with the policies and procedures the card issuer has established pursuant to section 334.90.

(d) Form of notice. Any written or electronic notice that the card issuer provides under this paragraph shall be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

6. Add and reserve appendices B-I.

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**

Red Flags in Connection with an Account Application or an Existing Account

Information from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A notice of address discrepancy is provided by a consumer reporting agency.
3. 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.
 - d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification

4. Documents provided for identification appear to have been altered.
5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.
7. Other information on the identification is not consistent with information that is on file, such as a signature card.

Personal Information

8. Personal information provided is inconsistent when compared against external information sources. *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.
9. Personal information provided is internally inconsistent. *For example,* there is a lack of correlation between the SSN range and date of birth.
10. Personal information provided is associated with known fraudulent activity. *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.
11. Personal information provided is of a type commonly associated with fraudulent activity. *For example:*
 - a. The address on an application is fictitious, a mail drop, or prison.
 - b. The phone number is invalid, or is associated with a pager or answering service.
12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.
13. The person opening the account or the customer fails to provide all required information on an application.

14. Personal information provided is not consistent with information that is on file.
15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Address Changes

16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional or replacement checks, convenience checks, cards, or cell phone, or for the addition of authorized users on the account.
17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

Anomalous Use of the Account

18. A new revolving credit account is used in a manner commonly associated with fraud.
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.

19. An 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.

20. An 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).

Notice from Customers or Others Regarding Customer Accounts

21. The financial institution or creditor is notified of unauthorized charges in connection with a customer's account.
22. The financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in identity theft.
23. The financial institution or creditor is notified that the customer is not receiving account statements.
24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.
25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.
27. An employee has accessed or downloaded an unusually large number of customer account records.
28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.
29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.
30. There are unusually frequent and large check orders in connection with a customer's account.
31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

Part 364 – STANDARDS FOR SAFETY AND SOUNDNESS

8. Add the following sentence at the end of paragraph (b) to § 364.101:

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 sections 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 proposes to amend chapter V of title 12 of the Code of Federal Regulations by amending 12 CFR part 571 as follows:

PART 571 – FAIR CREDIT REPORTING

1. The authority citation for part 571 is revised 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, and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

Subpart A – General Provisions

2. Amend § 571.2(b) to read as follows:

§ 571.1 Purpose and Scope.

* * * * *

(b) *Scope.*

* * * * *

(9) The scope of § 571.82 of Subpart I of this part is stated in § 571.82(a).

(10) The scope of Subpart J of this part is stated in § 571.90(a).

3. Amend § 571.3 by revising the introductory text to read as follows:

571.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

Subpart I - Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

4. Revise the heading for Subpart I as shown above.

5. Add § 571.82 to read as follows:

§ 571.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as “users”), and that are either savings associations whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, federal savings association 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 of a consumer report 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) Requirement to form a reasonable belief. 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 and for whom it receives a notice of address discrepancy. These policies and procedures must be designed to enable the user either to form a reasonable belief that it knows the identity of the consumer or determine that it cannot do so. A user that employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l) under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules.

(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 it knows the identity of the consumer for whom the consumer report was obtained;
- (ii) Establishes or maintains 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 pertaining to the consumer was obtained.

(2) Requirement to confirm consumer's address. The user may reasonably confirm an address is accurate by:

- (i) Verifying the address with the person to whom the consumer report pertains;
- (ii) Reviewing its own records of the address provided to request the consumer report;

- (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:

- (i) With respect to new relationships, for the reporting period in which it establishes a relationship with the consumer; and
- (ii) In other circumstances, for the reporting period in which the user confirms the accuracy of the address of the consumer.

6. Add Subpart J to part 571 to read as follows:

Subpart J – Identity Theft Red Flags

§ 571.90 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Purpose and scope. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting Act (FCRA). It applies to financial institutions and creditors that are either savings associations whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, federal savings association 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, the following definitions apply:

(1) Account means 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). Account includes:

(i) An extension of credit for personal, family, household or business purposes, such as a credit card account, margin account, or retail installment sales contract, such as a car loan or lease; and

(ii) A demand deposit, savings or other asset account for personal, family, household, or business purposes, such as a checking or savings account.

(2) The term board of directors includes:

(i) In the case of a foreign 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.

(3) Customer means a person that has an account with a financial institution or creditor.

(4) Identity theft has the same meaning as in 16 CFR 603.2(a).

(5) Red Flag means a pattern, practice, or specific activity that indicates the possible risk of identity theft.

(6) Service provider means a person that provides a service directly to the financial institution or creditor.

(c) Identity Theft Prevention Program. Each financial institution or creditor must implement a written Identity Theft Prevention Program (Program). The Program must

include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, operational, compliance, reputation, and litigation risks, in the manner discussed in paragraph (d) of this section. The Program must be:

(1) Appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities; and

(2) Designed to address changing identity theft risks as they arise in connection with the experiences of the financial institution or credit with identity theft, and changes in methods of identity theft, methods to detect, prevent, and mitigate identity theft, the types of accounts it offers, and business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(d) Development and implementation of Program. (1) Identification and evaluation of Red Flags. (i) Risk-based Red Flags. The Program must include policies and procedures to identify Red Flags, singly or in combination, that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor, using the risk evaluation set forth in paragraph (d)(1)(ii) of this section. The Red Flags identified must reflect changing identity theft risks to customers and to the financial institution or creditor as they arise. At a minimum, the Program must incorporate any relevant Red Flags from:

(A) Appendix J;

(B) Applicable supervisory guidance;

(C) Incidents of identity theft that the financial institution or creditor has experienced; and

(D) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.

(ii) Risk evaluation. In identifying which Red Flags are relevant, 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.

(2) Identity theft prevention and mitigation. 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, including policies and procedures to:

(i) Obtain identifying information about, and verify the identity of, a person opening an account. A financial institution or creditor that uses the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(l), under these circumstances, satisfies this requirement whether or not the user is subject to the CIP rules;

(ii) Detect the Red Flags pursuant to paragraph (d)(1) of this section;

(iii) Assess whether the Red Flags detected pursuant to paragraph (d)(2)(ii) of this section evidence a risk of identity theft. An institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft; and

- (iv) Address the risk of identity theft, commensurate with the degree of risk posed, such as by:
- (A) Monitoring an 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 customer's account;
 - (D) Reopening an account with a new account number;
 - (E) Not opening a new account;
 - (F) Closing an existing account;
 - (G) 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;
 - (H) 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
 - (I) 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.
- (3) Staff training. Each financial institution or creditor must train staff to implement its Program.
- (4) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity on its behalf and the

requirements of its Program are applicable to that activity (such as account opening), the financial institution or creditor must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of paragraphs (c) and (d) of this section.

(5) Involvement of board of directors and senior management. (i) Board approval. The board of directors or an appropriate committee of the board must approve the written Program.

(ii) Oversight by board or senior management. The board of directors, an appropriate committee of the board, or senior management must oversee the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation, and reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with this section.

(iii) Reports. (A) In general. Staff of the financial institution or creditor responsible for implementation of its Program must report to the board, an appropriate committee of the board, or senior management, at least annually, on compliance by the financial institution or creditor with this section.

(B) Contents of report. The report 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.

§ 571.91 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 571.90(a) that issues a debit or credit card.

(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) In general. The 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, unless, 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) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

(2) Notifies the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or

(3) Uses other means of assessing the validity of the change of address, in accordance with the policies and procedures the card issuer has established pursuant to section 571.90.

(d) Form of notice. Any written or electronic notice that the card issuer provides under this paragraph shall be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

7. Add and reserve appendices B–I.

8. Add Appendix J to part 571 to read as follows:

**APPENDIX J TO PART 571 – INTERAGENCY GUIDELINES ON
IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION
Red Flags in Connection with an Account Application or an Existing Account**

Information from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A notice of address discrepancy is provided by a consumer reporting agency.
3. 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.
 - d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification

4. Documents provided for identification appear to have been altered.
5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

7. Other information on the identification is not consistent with information that is on file, such as a signature card.

Personal Information

8. Personal information provided is inconsistent when compared against external information sources. *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.

9. Personal information provided is internally inconsistent. *For example,* there is a lack of correlation between the SSN range and date of birth.

10. Personal information provided is associated with known fraudulent activity. *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.

11. Personal information provided is of a type commonly associated with fraudulent activity. *For example:*

- a. The address on an application is fictitious, a mail drop, or prison.
- b. The phone number is invalid, or is associated with a pager or answering service.

12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.

13. The person opening the account or the customer fails to provide all required information on an application.

14. Personal information provided is not consistent with information that is on file.

15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Address Changes

16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional, or replacement checks, convenience checks, cards, or a cell phone, or for the addition of authorized users on the account.

17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

Anomalous Use of the Account

18. A new revolving credit account is used in a manner commonly associated with fraud. *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.

19. An 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.

20. An 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).

Notice from Customers or Others Regarding Customer Accounts

21. The financial institution or creditor is notified of unauthorized charges in connection with a customer's account.

22. The financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in identity theft.

23. The financial institution or creditor is notified that the customer is not receiving account statements.
24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.
25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.
27. An employee has accessed or downloaded an unusually large number of customer account records.
28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.
29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.
30. There are unusually frequent and large check orders in connection with a customer's account.
31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

[THIS SIGNATURE PAGE RELATES TO THE NOTICE OF PROPOSED
RULEMAKING TITLED “IDENTITY THEFT RED FLAGS AND ADDRESS
DISCREPANCIES UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS
ACT OF 2003.”]

Dated: _____, 2006.

John C. Dugan,
Comptroller of the Currency.

[THIS SIGNATURE PAGE RELATES TO THE NOTICE OF PROPOSED
RULEMAKING TITLED “IDENTITY THEFT RED FLAGS AND ADDRESS
DISCREPANCIES UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS
ACT OF 2003.”]

By order of the Board of Directors.

Dated at Washington, DC, the ____ day of _____, 2006. Federal Deposit Insurance
Corporation.

Robert E. Feldman
Executive Secretary

[THIS SIGNATURE PAGE RELATES TO THE NOTICE OF PROPOSED
RULEMAKING TITLED “IDENTITY THEFT RED FLAGS AND ADDRESS
DISCREPANCIES UNDER THE FAIR AND ACCURATE CREDIT TRANSACTIONS
ACT OF 2003.”]

Dated:

By the Office of Thrift Supervision,

John M. Reich,
Director.