Federal Register

Friday,
November 9, 2007

Part IV

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

Federal Reserve System
12 CFR Part 222

Federal Deposit Insurance Corporation
12 CFR Parts 334 and 364

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

National Credit Union Administration
12 CFR Part 717

Federal Trade Commission
16 CFR Part 681

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

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 41

[Docket ID OCC–2007–0017]

RIN 1557–AC87

FEDERAL RESERVE SYSTEM

12 CFR Part 222

[Docket No. R–1255]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Parts 334 and 364

RIN 3064–AD00

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 571

[Docket No. OTS–2007–0019]

RIN 1550–AC04

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 717

FEDERAL TRADE COMMISSION

16 CFR Part 681

RIN 3084–AA94

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

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

ACTION: Joint final rules and guidelines.

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

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

FOR FURTHER INFORMATION CONTACT:

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

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

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

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

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

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

SUPPLEMENTARY INFORMATION:

I. Introduction

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

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

[1] Pub. L. 108–159.

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

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

II. Section 114 of the FACT Act

A. Red Flag Regulations and Guidelines

1. Background

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

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

2. Overview of Proposal and Comments Received

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

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

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

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

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

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

3. Overview of final rules and guidelines

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

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

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

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

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

[5] Pub. L. 107–56.

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

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

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

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

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

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

4. Section-by-Section Analysis [8]

Section__.90(a) Purpose and Scope

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

Section__.90(b) Definitions

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

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

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

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

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

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

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

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

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

[11] Pub. L. 106–102.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Development and Implementation of Identity Theft Prevention Program

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

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

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

[26] 16 CFR 603.2(a).

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

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

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

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

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

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

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

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

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

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

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

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

B. The methods it provides to open these accounts;

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

D. Its size, location, and customer base.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Detecting Red Flags

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

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

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

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

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

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

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

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

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

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

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

Responding to Red Flags

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

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

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

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

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

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

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

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

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

[33] Pub. L. 107–56.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section __.90(e) Administration of the Program

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

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

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

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

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

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

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

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

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

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

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

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

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

66 FR 8620 (Feb. 1, 2001) (Preamble to final Information Security Standards.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Supplement A to Appendix J: Examples of Red Flags

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

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

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

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

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

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

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

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

complexity and the nature and scope of its activities.

Inactive Accounts

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

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

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

B. Special Rules for Card Issuers

1. Background

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

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

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

2. Section-by-Section Analysis

Section __.91(a) Scope

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

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

Section __.91(b) Definitions

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

Section __.91(b)(1) Cardholder

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

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

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

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

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

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

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

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

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

1693, *et seq.* The EFTA, and Regulation E, 12 CFR part 205, govern electronic fund transfers. In contrast to section 603(r) of the FCRA, neither the EFTA nor Regulation E defines the term ''debit card.'' Instead, coverage under the EFTA and Regulation E depends upon whether electronic fund transfers can be made to or from an ''account,'' meaning a checking, savings, or other consumer asset account established primarily for personal, family or household purposes. The Board recently issued a final rule expanding the definition of ''account'' under Regulation E to cover payroll card accounts.[41] Therefore, a holder of a payroll card is a ''cardholder'' for purposes of § __.91(b)(1), provided that the card issuer is a ''financial institution'' as defined in section 603(t) of the FCRA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section __.91(e) Form of Notice

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

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

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

III. Section 315 of the FACT Act

A. Background

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

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

B. Section-by-Section Analysis

Section __.82(a) Scope

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

Section __.82(b) Definition

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proposed § __.82(d)(1) provided that a user must develop and implement reasonable policies and procedures for furnishing to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the following three conditions are satisfied. The first condition, in proposed § __.82(d)(1)(i), was that the user must be able to form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained. This condition would have ensured the user would furnish a new address for the consumer to the CRA only after the user had formed a reasonable belief that it knew the identity of the consumer, using the policies and procedures set forth in paragraph § __.82(c).

The second condition, in proposed § __.82(d)(1)(ii), was that the user furnish the address to the CRA if it establishes or maintains a continuing relationship with the consumer. Section 315 specifically requires that the user furnish the consumer's address to the CRA if the user *establishes* a continuing relationship with the consumer. Therefore, proposed § __.82(d)(1)(ii) reiterated this requirement. However, because a user also may obtain a notice of address discrepancy in connection with a consumer with whom it already has an existing relationship, the proposal also provided that the user must furnish the consumer's address to the CRA from whom the user has received a notice of address discrepancy when the user maintains a continuing relationship with the consumer.

Finally, the third condition, in proposed § _.82(d)(1)(iii), provided that if the user regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained, the consumer's address must be communicated to the CRA as part of the information the user regularly provides.

A majority of commenters recommended that the requirement to furnish a confirmed address should not apply to existing accounts. These commenters maintained that such a requirement would exceed the scope of the statute. They also noted that users often do not obtain full consumer reports for existing customers—just credit scores. These commenters noted that limited reports often do not contain an address for a customer. Some commenters also felt existing relationships should be excluded because users already would have verified a consumer's address at the time of account opening.

The Agencies have modified this section as follows. The final rules continue to provide that a user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the CRA when three conditions are present. The first condition, in § _.82(d)(1)(i), has been revised to be consistent with the earlier changes in section § _.82(c) that focus more narrowly on accuracy and require that a user form a reasonable belief that a consumer report relates to the consumer about whom it requested the report. The second condition, in § _.82(d)(1)(ii), now applies only to new accounts and states that a confirmed address must be furnished if the user ''establishes'' a continuing relationship with the consumer. The reference to ''or maintains'' a continuing relationship has been deleted. The Agencies agree with commenters that section 605(h)(2)(B)(ii) does not require the reporting of a confirmed address to a CRA in connection with existing relationships. The Agencies have concluded that users are more likely than a CRA to have an accurate address for an existing customer and, therefore, should not be required by these rules to take additional steps to confirm the accuracy of the customer's address. Users already have an ongoing duty to correct and update information for their existing customers under section 623 of the FCRA, 15 U.S.C. 1681s–2. Accordingly, under the final rules, the obligation to furnish a confirmed address for the consumer to the CRA is applicable only to new relationships. The third condition, in § _.82(d)(1)(iii), has been adopted in the final rule without substantive change.

Section __.82(d)(2) Requirement To Confirm Consumer's Address

In the preamble to the proposal, the Agencies noted that section 315 requires them to prescribe regulations describing reasonable policies and procedures for a user ''to reconcile the address of the consumer'' about whom it has obtained a notice of address discrepancy with the CRA ''by furnishing *such* address'' to the CRA. (Emphasis added.) The

[49] *See, e.g.,* 31 CFR 103.121(b)(3)(i)(D).

[50] *See, e.g.,* 31 CFR 103.121(b)(2)(iii).

Agencies noted that, even when the user is able to form a reasonable belief that it knows the identity of the consumer, there may be many reasons the initial address furnished by the consumer is incorrect. For example, a consumer may have provided the address of a secondary residence or inadvertently reversed a street number. To ensure that the address furnished to the CRA is accurate, the Agencies proposed to interpret the phrase, ''such address,'' as an address the user has reasonably confirmed is accurate. This interpretation would have required a user to take steps to ''reconcile'' the address it initially received from the consumer when it receives a notice of address discrepancy, rather than simply furnishing the initial address it received from the consumer to the CRA. Proposed § __.82(d)(2) contained the following list of illustrative measures that a user may employ to reasonably confirm the accuracy of the consumer's address:

- Verifying the address with the person to whom the consumer report pertains;
- Reviewing its own records of the address provided to request the consumer report;
- Verifying the address through third-party sources; or
- Using other reasonable means.

The Agencies solicited comment on whether these examples were necessary, or whether different or additional examples should be listed.

A number of commenters stated that requiring a user to confirm the address furnished exceeded the scope of the statute. They asserted that the benefit of improvements in the accuracy of addresses and the prevention of identity theft would not outweigh the additional burden of this requirement. A few commenters noted that complying with the CIP rules should be sufficient to verify the address. Commenters also felt that users should have the flexibility to establish their own validation processes based on risk.

As stated earlier, the Agencies believe the purpose of the statute is to enhance the accuracy of information relating to consumers by requiring the user to furnish an address that the user has reasonably confirmed is accurate.[51] Simply providing the CRA with the initial address supplied to the user by the consumer, and which caused the CRA to send a notice of address discrepancy, would not serve this purpose. The Agencies believe the options for confirmation listed in the regulation provide sufficient flexibility for users to confirm consumers' addresses. For this reason, they have been adopted in the final rule as proposed, with minor technical changes. Section __.82(d)(2)(i) has been revised to conform the language with § __.82(c). Section __.82(d)(2)(ii) has been revised to emphasize the verification of the consumer's address rather than the review of the user's records to determine whether the address given by the consumer is the same.

Section __.82(d)(3) Timing

Section 315 specifies when a user must furnish the consumer's address to the CRA. It states that this information must be furnished for the reporting period in which the user's relationship with the consumer is established. Accordingly, proposed § __.82(d)(3)(i) stated that, with respect to new relationships, the policies and procedures a user develops in accordance with § __.82(d)(1) must provide that a user will furnish the consumer's address that it has reasonably confirmed to the CRA as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

The proposed rule also addressed other situations when a user may receive a notice of address discrepancy. Proposed § __.82(d)(3)(ii) stated that in other circumstances, such as when the user already has an existing relationship with the consumer, the user should furnish this information for the reporting period in which the user has reasonably confirmed the accuracy of the address of the consumer for whom it has obtained a consumer report.

The Agencies also noted that, in order to satisfy the requirements of both § __.82(d)(1) and § __.82(d)(3)(i), a user employing the CIP rules would have to establish a continuing relationship and verify the identity of the consumer during the same reporting period.

The Agencies recognized the timing provision for newly established relationships could be problematic for users hoping to take full advantage of the flexibility in timing for verification of identity afforded by the CIP rules. As required by statute, proposed § __.82(d)(3)(i) stated that the reconciled address must be furnished for the reporting period in which the user establishes a relationship with the consumer. Proposed § __.82(d)(1), which also mirrored the requirement of the statute, required the reconciled address to be furnished to the CRA only when the user both establishes a continuing relationship with the consumer and forms a reasonable belief that it knows the identity of the consumer to whom the consumer report relates. Typically, the CIP rules permit an account to be opened (*i.e.*, relationship to be established) if certain identifying information is provided. Verification to establish the true identity of the customer is required within a reasonable period of time *after* the account has been opened. As explained in the preamble to the proposed rules, to satisfy the requirements of both § __.82(d)(1) and § __.82(d)(3)(i), a user employing the CIP rules would have to verify the identity of the consumer using the identifying information it obtained in accordance with the CIP rules within the same reporting period that the user opens the account and establishes a continuing relationship with the consumer.

The Agencies requested comment on whether the timing for responding to notices of address discrepancy received in connection with newly established relationships and in connection with circumstances other than newly established relationships is appropriate. One commenter objected to the requirement that a user employing the CIP rules would have to both establish a continuing relationship and a reasonable belief that it knows the consumer's identity during the same reporting period. A few commenters noted that the timing for reporting should simply be ''reasonable,'' such as the next reporting cycle.

Because the Agencies have determined that the requirement to furnish a confirmed address will apply only to newly established accounts, the Agencies have revised § __.82(d)(3) to remove the references to the timing for furnishing reports in connection with other accounts, contained in the proposal. The final rules reflect the language in section 605(h)(2)(B)(ii), and state that a user's policies and procedures must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

A timing issue still exists for a user that chooses to compare the information in the consumer report with information that the user obtains and uses to verify the consumer's identity in accordance with the CIP rules for the purpose of forming a reasonable belief that a consumer report relates to the consumer

[51] This requirement is consistent with the legislative history which provides that this section is intended to obligate the user to utilize reasonable policies and procedures to resolve discrepancies. *See* H.R. Rep. No. 108–263 at 46 (Sept. 4, 2003) (accompanying H.R. 2622).

about whom it has requested the report. However, the Agencies believe that the benefits of being able to use CIP for this purpose should outweigh any additional burden of having to establish a reasonable belief that a consumer report relates to the consumer about whom it has requested the report within the same reporting period that the user opens the account and establishes a continuing relationship with the consumer.

IV. General Provisions

The OCC, the Board, the FDIC, the OTS, and the NCUA[52] proposed to amend the first sentence in § __.3, which contains the definitions that are applicable throughout this part. This sentence stated that the list of definitions in § __.3 apply throughout the part ''unless the context requires otherwise.'' These agencies proposed to amend this introductory sentence to make clear that the definitions in § __.3 apply ''for purposes of this part, unless explicitly stated otherwise.'' Thus, these definitions apply throughout the part unless defined differently in an individual subpart. There were no comments on this proposal, and the change to § __.3 is adopted as proposed.

OTS proposed nonsubstantive, technical changes to its rule sections on purpose and scope (§ 571.1) and disposal of consumer information (§ 571.83). OTS explained that these changes were necessary in light of the proposed incorporation of the address discrepancy section into subpart I. There were no comments on these proposed changes and they are adopted substantially as proposed. Further, since these changes render the definition of ''you'' in § 571.3(o) superfluous, OTS is removing that definition.

The OCC's final rules add a purpose section at § 41.1. The final rules are simply restoring the purpose section of part 41 that was inadvertently deleted when ''subpart D-Medical Information'' was added to this part.

V. Effective Date

The Agencies received a number of comments regarding the effective date of the final regulations and guidelines, although the proposed rulemaking did not address this issue. While consumer groups recommended that the effective date for compliance with the regulations be the minimum time allowed by law, many financial institutions and creditors requested the time for compliance be extended from between 12 to 24 months from issuance of the final rules. These commenters felt they needed time to take an inventory of their existing systems and develop new programs necessary for compliance. Some commenters noted that they likely would use technological solutions to comply with the rules and that it is necessary to schedule such projects well in advance. Commenters also noted that compliance with the final rules may require systemic and operational changes across business lines and could affect relationships with vendors and third party service providers that would require time to change.

Neither section 114 nor section 315 of the FACT Act specifically addresses the effective date of the regulations issued pursuant to these sections. Under the Administrative Procedure Act (APA), 5 U.S.C. 553(d), agencies must generally publish a substantive rule not less than 30 days before its effective date. In addition, under section 302 of the Riegle Community Development and Regulatory Improvement Act of 1994 (CDRIA),[53] rules issued by the Federal banking agencies that impose additional reporting, disclosure, or other new requirements on financial institutions generally will take effect on the first day of a calendar quarter that begins on or after the date on which the regulations are published in the **Federal Register**. Because these final rules are substantive and impose additional requirements on financial institutions, the Agencies have provided for an effective date of [January 1, 2008], consistent with the APA and CDRIA.

At the same time, the Agencies have determined that it is appropriate to provide all covered entities with a delayed compliance date of November 1, 2008, to comply with the requirements of the final rulemaking. Some financial institutions and creditors already employ a variety of measures that satisfy the requirements of the final rulemaking because these are usual and customary business practices to minimize losses due to fraud, or as a result of already complying with other existing regulations and guidance that relate to information security, authentication, identity theft, and response programs. However, the Agencies recognize that these entities may still need time to evaluate their existing programs, and to integrate appropriate elements from them into the Program and into the other policies and procedures required by this final rulemaking. Further, the Agencies recognize that some covered entities have not previously been subject to any related regulations or guidance, and thus may need more time to implement the final rules and guidelines. Therefore, the Agencies are providing covered entities with a transition period to comply with the requirements contained in the final rulemaking.

VI. Regulatory Analysis

A. Paperwork Reduction Act

In accordance with the requirements of the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*, 5 CFR part 1320 Appendix A.1), the Agencies have reviewed the final rulemaking and determined that it contains collections of information subject to the PRA. The Board made this determination under authority delegated to the Board by the Office of Management and Budget (OMB). The information collection requirements in the final rulemaking may be found in 12 CFR 41.82, 41.90, 41.91, 222.82, 222.90, 222.91, 334.82, 334.90, 334.91, 571.82, 571.90, 571.91, 717.82, 717.90; and 717.91; and 16 CFR 681.1, 681.2, and 681.3.

An agency may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid OMB control number. The information collection requirements contained in this joint final rule were submitted by the OCC, FDIC, OTS, NCUA, and FTC to OMB for review and approval under the Paperwork Reduction Act of 1995. OMB assigned the following control numbers to the collections of information: OMB Control Nos. 1557–0237 (OCC), 3064–0152 (FDIC), 1550–0113 (OTS), 3133–0175 (NCUA), and 3084–0137 (FTC). The Board's OMB Control No. is 7100–0308.[54]

Description of the Collection

Section 114: The proposed rules implementing section 114 required each financial institution and creditor to (1) create an Identity Theft Prevention Program (Program); (2) report to the board of directors, a committee thereof or senior management, at least annually, on compliance with the proposed regulations; and (3) train staff to implement the Program.

In addition, the proposed rules required each credit and debit card issuer (card issuer) to establish policies and procedures to (1) assess the validity

[52] The equivalent language for the FTC already exists in 16 CFR 603.1.

[53] Pub. L. 103–325; 12 U.S.C. § 4802(b).

[54] The information collections (ICs) in this rule will be incorporated with the Board's Disclosure Requirements Associated with Regulation V (OMB No. 7100–0308). The burden estimates provided in this rule pertain only to the ICs associated with this final rulemaking. The current OMB inventory for Regulation V is available at: *http://www.reginfo.gov/public/do/PRAMain.*

of a change of address notification before honoring a request for an additional or replacement card received during at least the first 30 days after it receives the notification; and (2) notify the cardholder in writing, electronically, or orally, or use another means of assessing the validity of the change of address.

Section 315: The proposed rules implementing section 315 required each user of consumer reports to (1) develop reasonable policies and procedures it would employ when it receives a notice of address discrepancy from a CRA; and (2) to furnish an address the user reasonably confirmed is accurate to the CRA from which it receives a notice of address discrepancy.

The information collections in the final rulemaking are the same as those in the proposal.

Comments Received

The Agencies sought comment on the burden estimates for the information collections described in the proposal. The Agencies received approximately 129 comments on the proposed rulemaking. Most commenters maintained that proposal would impose additional regulatory burden and asserted that the estimates of the cost of compliance should be considerably higher than the Agencies projected. A few of these commenters specifically addressed PRA burden, however, they did not provide specific estimates of additional burden hours that would result from the proposal. Some of these commenters stated that staff training estimates were significantly underestimated. Other commenters stated that the costs of compliance failed to consider the cost to third-party service providers that the commenters characterized as being required to implement the Program.

Explanation of Burden Estimates Under the Final Rulemaking

The Agencies believe that many of the comments received regarding burden stemmed from commenters' misreading of the requirements of the proposed rulemaking. The final rulemaking clarifies these requirements, including those that relate to the information collections. It also differs from the proposal as described below.

The Agencies continue to believe that most covered entities already employ a variety of measures to detect and address identity theft that are required by section 114 of the final rulemaking because these are usual and customary business practices that they employ to minimize losses due to fraud. In addition, the Agencies believe that many financial institutions and creditors already have implemented some of the requirements of the final rules implementing section 114 as a result of having to comply with other existing regulations and guidance, such as the CIP regulations implementing section 326 of the USA PATRIOT Act, 31 U.S.C. 5318(l) that require verification of the identity of persons opening new accounts),[55] the Information Security Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801, and section 216 of the FACT Act, 15 U.S.C. 1681w,[56] and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs.[57] The final rulemaking underscores the ability of a financial institution or creditor to incorporate into its Program its existing processes that control reasonably foreseeable risks to customers or to its own safety and soundness from identity theft, such as those already developed in connection with the covered entity's fraud prevention program. Thus, the burden estimate attributable to the creation of a Program is unchanged.

The final rulemaking also clarifies that only relevant staff need be trained to implement the Program, as necessary—meaning that staff already trained, for example, as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as necessary. Despite this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours.

The Agencies' estimates attribute all burden to covered entities, which are entities directly subject to the requirements of the final rulemaking. A covered entity that outsources activities to a third-party service provider is, in effect, reallocating to that service provider the burden that it would otherwise have carried itself. Under these circumstances, burden is, by contract, shifted from the covered entity to the service provider, but the total amount of burden is not increased. Thus, third-party service provider burden is already included in the burden estimates provided for covered entities.

The Agencies continue to believe that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Further, as commenters requested, the final rulemaking clarifies that card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, before a request for an additional or replacement card. Therefore, the estimates attributable to this portion of the rulemaking are unchanged.

Regarding the final rules implementing section 315, the Agencies recognize that users of consumer reports will need to develop policies and procedures to employ upon receiving a notice of address discrepancy in order to: (1) Ensure that the user has obtained the correct consumer report for the consumer; and (2) confirm the accuracy of the address the user furnishes to the CRA. However, under the final rules, a user only must furnish a confirmed address to a CRA for new relationships. Thus, the required policies and procedures will no longer need to address the furnishing of confirmed addresses for existing relationships, and users will not need to furnish to the CRA in connection with existing relationships an address the user reasonably confirmed is accurate.

The Agencies believe that users of credit reports covered by the final rules,

[55] *See, e.g.*, 31 CFR 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 CFR 103.122 (broker-dealers); 31 CFR 103.123 (futures commission merchants).

[56] 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D–2 and part 225, app. F (state member banks and holding companies); 12 CFR part 364, app. B (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, app. A and B, and 12 CFR 717 (credit unions); 16 CFR part 314 (financial institutions that are not regulated by the Board, FDIC, NCUA, OCC and OTS).

[57] *See, e.g.*, 12 CFR part 30, supp. A to app. B (national banks); 12 CFR part 208, supp. A to app. D–2 and part 225, supp. A to app. F (state member banks and holding companies); 12 CFR part 364, supp. A to app. B (state non-member banks); 12 CFR part 570, supp. A to app. B (savings associations); 12 CFR 748, app. A and B (credit unions); Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet (the ''IS Booklet'') *available at http://www.ffiec.gov/guides.htm*; FFIEC ''Authentication in an Internet Banking Environment'' *available at http://www.ffiec.gov/pdf/authentication_guidance.pdf*; Board SR 01–11 (Supp) (Apr. 26, 2001) *available at: http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm*; ''Guidance on Identity Theft and Pretext Calling,'' OCC AL 2001–4 (April 30, 2001); ''Identity Theft and Pretext Calling,'' OTS CEO Letter #139 (May 4, 2001); NCUA Letter to Credit Unions 01–CU–09, ''Identity Theft and Pretext Calling'' (Sept. 2001); OCC 2005–24, ''Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents,'' (July 1, 2005); ''Phishing and E-mail Scams,'' OTS CEO Letter #193 (Mar. 8, 2004); NCUA Letter to Credit Unions 04–CU–12, ''Phishing Guidance for Credit Unions'' (Sept. 2004).

on a regular basis, already furnish information to CRAs in response to notices of address discrepancy because it is a usual and customary business practice—except in connection with new deposit relationships. For the proposed rulemaking, the Agencies had estimated that there would be no implementation burden associated with furnishing confirmed addresses to CRAs. However, as the result of additional research, the Agencies now believe that some burden should be attributable to this collection, to account for information furnished to CRAs for new deposit relationships. Because this burden is offset by the reduction in burden described above, the estimates for the collections attributable to the final rules implementing section 315 remain unchanged.

The Agencies continue to believe that 25 hours to develop a Program, four hours to prepare an annual report, four hours to develop policies and procedures to assess the validity of changes of address, and four hours to develop policies and procedures to respond to notices of address discrepancy, are reasonable estimates.

The potential respondents are national banks and Federal branches and agencies of foreign banks and certain of their subsidiaries (OCC); state member banks, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations (Board); insured nonmember banks, insured state branches of foreign banks, and certain of their subsidiaries (FDIC); savings associations and certain of their subsidiaries (OTS); Federally-chartered credit unions (NCUA); state-chartered credit unions, non-bank lenders, mortgage brokers, motor vehicle dealers, utility companies, and any other person that regularly participates in a credit decision, including setting the terms of credit (FTC).

Burden Estimates

The Agencies estimate the annual burden per respondent is 41 hours (25 hours to develop a Program, four hours to prepare an annual report, four hours for training, four hours for developing policies and procedures to assess the validity of changes of address, and four hours for developing policies and procedures to respond to notices of address discrepancy). The Agencies attribute total burden to covered entities as follows:

OCC:
Number of respondents: 1,806.
Total estimated annual burden: 74,046.
Board:
Number of respondents: 1,172.
Total Estimated Annual Burden: 48,052.
FDIC:
Number of respondents: 5,260.
Total Estimated Annual Burden: 215,660 hours.
OTS:
Number of respondents: 832.
Total Estimated Annual Burden: 34,112.
NCUA:
Number of respondents: 5,103.
Total Estimated Annual Burden: 209,223.
FTC Estimated Burden:[58]
Section 114:
Estimated Hours Burden:

As discussed above, the final regulations require financial institutions and creditors to conduct a risk assessment periodically to determine whether they have covered accounts, which include, at a minimum, consumer accounts. If the financial institutions and creditors determine that they have covered accounts, the final regulations require them to create a written Identity Theft Prevention Program (Program) and they should report to the board of directors, a committee thereof, or senior management at least annually on compliance with the final regulations. The FCRA defines ''creditor'' to have the same meaning as in section 702 of the Equal Credit Opportunity Act (ECOA).[59] Under Regulation B, which implements the ECOA, a creditor means a person who regularly participates in a credit decision, including setting the terms of credit. Regulation B defines credit as a transaction in which the party has a right to defer payment of a debt, regardless of whether the credit is for personal or commercial purposes.[60] Given the broad scope of entities covered, it is difficult to determine precisely the number of financial institutions and creditors that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction, and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the proposed regulations implementing section 114 will affect over 3,500 financial institutions[61] and over 11 million creditors[62] subject to the FTC's jurisdiction, for a combined total of approximately 11.1 million affected entities. As detailed below, FTC staff estimates that the average annual information collection burden during the three-year period for which OMB clearance was sought will be 4,466,000 hours (rounded to the nearest thousand). The estimated annual labor cost associated with this burden is $142,925,000 (rounded to the nearest thousand).

For the proposed rule, FTC staff had divided affected entities into two categories: entities that are subject to a high risk of identity theft and entities that are subject to a low risk of identity theft. Based on comments as well as changes in the final rule, FTC staff believes that the affected entities can be categorized in three groups, based on the nature of their businesses: entities subject to a high risk of identity theft, entities subject to a low risk of identity theft, but having consumer accounts that will require them to have a written Program, and entities subject to a low risk of identity theft, but not having consumer accounts.[63]

A. High-Risk Entities

In drafting its PRA analysis for the proposed regulations, FTC staff believed that because motor vehicle dealers'' loans typically are financed by financial institutions also subject to those regulations, the dealers were likely to use the latter's programs as a basis to develop their own. Therefore, although subject to a high risk of identity theft, their burden would be less than other high-risk entities. Commenters, however, noted among other concerns that some motor vehicle dealers finance

[58] Due to the varied nature of the entities subject to the jurisdiction of the FTC, this Estimated Burden section reflects only the view of the FTC. The banking regulatory agencies have jointly prepared a separate analysis.

[59] U.S.C. 1681a(r)(5).

[60] Regulation B Equal Credit Opportunity, 12 CFR 202 (as amended effective Apr. 15, 2003).

[61] Under the FCRA, the only financial institutions over which the FTC has jurisdiction are state-chartered credit unions. 15 U.S.C. 1681s. As of December 31, 2005, there were 3,302 state-chartered federally-insured credit unions and 362 state-chartered nonfederally insured credit unions, totaling 3,664 financial institutions. *See www.ncua.gov/news/quick_facts/quick_facts.html and* ''Disclosures for Non-Federally Insured Depository Institutions under the Federal Deposit Insurance Corporation Improvement Act (FDICIA),'' 70 FR 12823 (Mar. 16, 2005).

[62] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, which totaled 11,076,463 creditors subject to the FTC's jurisdiction.

[63] In general, high-risk entities may provide consumer financial services or other goods or services of value to identity thieves such as telecommunication services or goods that are easily convertible to cash, whereas low-risk entities may do business primarily with other businesses or provide non-financial services or goods that are not easily convertible to cash.

their own loans. Thus, for this burden estimate, FTC staff no longer is considering motor vehicle dealers separately from other high-risk entities.

As noted above, the Agencies continue to believe that many of the high-risk entities, as part of their usual and customary business practices, already take steps to minimize losses due to fraud. The final rulemaking clarifies that only relevant staff need be trained to implement the Program, as necessary meaning, for example, that staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as incrementally needed. Notwithstanding this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours, as is the FTC for high-risk entities in their initial year of implementing the Program, but FTC staff continues to believe that one hour of recurring annual training remains a reasonable estimate.

The FTC staff maintains its estimate of 25 hours for high-risk entities to create and implement a written Program, with an annual recurring burden of 1 hour. As before, FTC staff anticipates that these entities will incorporate policies and procedures that they likely already have in place. The FTC staff continues to believe that preparation of an annual report will take high-risk entities 4 hours initially, with an annual recurring burden of 1 hour.

B. Low-Risk Entities

A few commenters believed that FTC staff had underestimated the amount of time it would take low-risk entities to comply with the proposed regulations. These commenters estimated that the amount of time would range from 6 to 20 hours to create a program and 1 hour each to train employees and draft the annual report. The FTC staff believes these estimates were based on a misunderstanding of the requirements of the proposed regulations, including that the list of 31 Red Flags in the proposed guidelines was intended to be a checklist. The final regulations clarify that the list of Red Flags is illustrative only. Moreover, the emphasis of the written Program, as required under the final regulations, is to identify risks of identity theft. To the extent that entities with consumer accounts determine that they have a minimal risk of identity theft, they would be tasked only with developing a streamlined Program. Therefore, the FTC staff does not believe that it would take such an entity 6 to 20 hours to develop a Program, 1 hour to train employees, and 1 hour to draft an annual report on risks of identity theft which are minimal or non-existent. Nonetheless, FTC staff believes that it may have underestimated the time low-risk entities may need to initially apply the final rule to develop a Program. Thus, FTC staff has increased from 20 minutes to 1 hour its previously stated estimate for this activity.

The final regulations have been revised from the proposed regulations to alleviate the burden of creating a written Program for entities that determine that they do not have any covered accounts. The FTC staff believes that entities subject to a low risk of identity theft, but not having consumer accounts, will likely determine that they do not have covered accounts. Such entities would not be required to develop a written Program, and thus will not incur PRA burden. The FTC staff estimates that approximately 9,191,496 [64] of the 10,813,525 low-risk entities subject to the requirement to create a written Program under the proposed regulations will not have covered accounts under the final rule. Therefore, these 9,191,496 low-risk entities will not be required to develop a written Program, thereby substantially reducing the original burden hours estimate in the NPRM for low-risk entities.

The FTC staff believes that for entities subject to a low risk of identity theft, but having consumer accounts that will require them to have a written Program, it will take such entities 1 hour to review the final regulations and create a streamlined Program, with an annual recurring burden of 5 minutes. The FTC staff believes that training staff to be attentive to any future risks of identity theft will take low-risk entities 10 minutes, with an annual recurring burden of 5 minutes. The FTC staff believes that preparing an annual report will take low-risk entities 10 minutes, with an annual recurring burden of 5 minutes.

Accordingly, FTC staff estimates that the final regulations implementing section 114 affect the following: 266,602 high-risk entities subject to the FTC's jurisdiction at an average annual burden of 13 hours per entity [average annual burden over 3-year clearance period for creation and implementation of Program ((25+1+1)/3) plus average annual burden over 3-year clearance period for staff training ((4+1+1)/3) plus average annual burden over 3-year clearance period for preparing annual report ((4+1+1)/3)], for a total of 3,466,000 hours (rounded to the nearest thousand); and 1,622,029 low-risk entities that have consumer accounts subject to the FTC's jurisdiction at an average annual burden of approximately 37 minutes per entity [average annual burden over 3-year clearance period for creation and implementation of streamlined Program ((60+5+5)/3) plus average annual burden over 3-year clearance period for staff training ((10+5+5)/3) plus average annual burden over 3-year clearance period for preparing annual report ((10+5+5)/3], for a total of 1,000,000 hours (rounded to the nearest thousand).

The proposed regulations implementing Section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request, including notifying the cardholder or using another means of assessing the validity of the change of address. The FTC received no comments on its burden estimates in the NPRM and FTC staff does not believe that the changes made to the final regulation have altered its original burden estimates. Accordingly, FTC staff maintains that it will take 100 credit or debit card issuers 4 hours to develop and implement policies and procedures to assess the validity of a change of address request for a total burden of 400 hours.

Estimated Cost Burden:

The FTC staff derived labor costs by applying appropriate estimated hourly cost figures to the burden hours described above. It is difficult to calculate with precision the labor costs associated with the proposed regulations, as they entail varying compensation levels of management and/or technical staff among companies of different sizes. In the NPRM, FTC staff had estimated that low-risk entities would use administrative support personnel at an hourly cost of $16.00. A few commenters disagreed that low-risk entities would use administrative support personnel, arguing instead that the Program would be implemented at a managerial level, and the labor cost should be at least $32.00 and possibly even $48.00. Therefore, in calculating the cost figures, FTC staff assumes that for all entities, professional technical personnel and/or managerial personnel will create and implement the Program, prepare the annual report, train employees, and assess the validity of a

[64] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, net of the number of creditors subject to the FTC's jurisdiction, an estimated subset of which comprise anticipated low-risk entities not having covered accounts under the final rule.

change of address request, at an hourly rate of $32.00.[65]

Based on the above estimates and assumptions, the total annual labor costs for all categories of covered entities under the final regulations implementing section 114 are $142,925,000 (rounded to the nearest thousand) [(3,466,000 hours + 400 hours + 1,000,000 hours) x $32.00)].

Section 315:

Estimated Hours Burden:

The Commission did not receive any comments relating to its original burden estimates for the information collection requirements under section 315. Although the final regulations were modified such that they no longer require users to furnish a confirmed address to a CRA for existing relationships, FTC staff does not believe that this modification will significantly alter its original burden estimates. Therefore, FTC staff burden estimates remain unchanged under section 315 from the estimates proposed in the NPRM. Accordingly, FTC staff estimates that the average annual information collection burden during the three-year period for which OMB clearance was sought will be 831,000 hours (rounded to the nearest thousand). The FTC staff continues to assume that the policies and procedures for notice of address discrepancy and furnishing the correct address will be set up by administrative support personnel at an hourly rate of $16.[66] Thus, the estimated annual labor cost associated with this burden is $13,296,000 (rounded to the nearest thousand).

The Agencies have a continuing interest in the public's opinions of our collections of information. At any time, comments regarding the burden estimate, or any other aspect of this collection of information, including suggestions for reducing the burden, may be sent to:

OCC: Communications Division, Office of the Comptroller of the Currency, Public Information Room, Mail stop 1–5, Attention: 1557–0237, 250 E Street, SW., Washington, DC 20219. In addition, comments may be sent by fax to 202–874–4448, or by electronic mail to *regs.comments@occ.treas.gov*. You can inspect and photocopy the comments at the OCC's Public Information Room, 250 E Street, SW., Washington, DC 20219. For security reasons, the OCC requires that visitors make an appointment to inspect comments. You may do so by calling 202–874–5043. Upon arrival, visitors will be required to present valid government-issued photo identification and submit to security screening in order to inspect and photocopy comments.

Board: You may submit comments, identified by R–1255, by any of the following methods:

Agency Web site: *http://www.federalreserve.gov*. Follow the instructions for submitting comments on *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm*.

Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.

E-mail: *regs.comments@federalreserve.gov*. Include docket number in the subject line of the message.

Fax: 202–452–3819 or 202–452–3102.

Mail: Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW., Washington, DC 20551.

All public comments are available from the Board's Web site at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, unless modified for technical reasons. Accordingly, your comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper form in Room MP–500 of the Board's Martin Building (20th and C Streets, NW.) between 9 a.m. and 5 p.m. on weekdays.

FDIC: You may submit written comments, which should refer to 3064–AD00, by any of the following methods:

Agency Web site: *http://www.fdic.gov/regulations/laws/federal/propose.html*.

Follow the instructions for submitting comments on the FDIC Web site.

Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.

E-mail: *Comments@FDIC.gov*.

Mail: Robert E. Feldman, Executive Secretary, Attention: Comments, FDIC, 550 17th Street, NW., Washington, DC 20429.

Hand Delivery/Courier: Guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7 a.m. and 5 p.m.

Public Inspection: All comments received will be posted without change to *http://www.fdic.gov/regulations/laws/federal/propose/html* including any personal information provided. Comments may be inspected at the FDIC Public Information Center, Room 100, 801 17th Street, NW., Washington, DC, between 9 a.m. and 4:30 p.m. on business days.

OTS: Information Collection Comments, Chief Counsel's Office, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552; send a facsimile transmission to (202) 906–6518; or send an e-mail to related index on the OTS Internet site at *http://www.ots.treas.gov*. In addition, interested persons may inspect the comments at the Public Reading Room, 1700 G Street, NW., by appointment. To make an appointment, call (202) 906–5922, send an e-mail to *publicinfo@ots.treas.gov*, or send a facsimile transmission to (202) 906–7755.

NCUA: You may submit comments by any of the following methods (Please send comments by one method only):

Federal eRulemaking Portal: *http://www.regulations.gov*.

Follow the instructions for submitting comments.

NCUA Web site: *http://www.ncua.gov/RegulationsOpinionsLaws/proposedregs/proposedregs.html*.

Follow the instructions for submitting comments.

E-mail: Address to *regcomments@ncua.gov*. Include ''[Your name] Comments on -,'' in the e-mail subject line.

Fax: (703) 518–6319. Use the subject line described above for e-mail.

Mail: Address to Mary F. Rupp, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314–3428.

Hand Delivery/Courier: Same as mail address.

Additionally, commenters may send a copy of their comments to the OMB desk officer for the OCC, Board, FDIC, OTS, and NCUA by mail to the Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street, NW., Washington, DC 20503, or by fax to (202) 395–6974.

FTC: Comments should refer to ''The Red Flags Rule: Project No. R611019,'' and may be submitted by any of the following methods. However, if the comment contains any material for which confidential treatment is requested, it must be filed in paper form, and the first page of the document

[65] The cost is derived from a mid-range among the reported 2006 Bureau of Labor Statistics rates for likely positions within the professional technical and managerial categories. See June 2006 Bureau of Labor Statistics National Compensation Survey for occupational wages in the United States at *http://www.bls.gov/ncs/ocs/sp/ncbl0910.pdf* (''June 2006 BLS NCS Survey'').

[66] This hourly wage is a conservative inflation-adjusted updating of hourly mean wages ($14.86) shown for administrative support personnel in the June 2006 BLS NCS Survey.

must be clearly labeled ''Confidential.'' [67]

E-mail: Comments filed in electronic form should be submitted by clicking on the following Web link: *https://secure.commentworks.com/ftc-redflags* and following the instructions on the Web-based form. To ensure that the Commission considers an electronic comment, you must file it on the Web-based form at *https://secure.commentworks.com/ftc-redflags*.

Federal eRulemaking Portal: If this notice appears at *http://www.regulations.gov*, you may also file an electronic comment through that Web site. The Commission will consider all comments that regulations.gov forwards to it.

Mail or Hand Delivery: A comment filed in paper form should include ''The Red Flags Rule, Project No. R611019,'' both in the text and on the envelope and should be mailed or delivered, with two complete copies, to the following address: Federal Trade Commission/Office of the Secretary, Room H–135 (Annex M), 600 Pennsylvania Avenue, NW., Washington, DC 20580. Because paper mail in the Washington area and at the Commission is subject to delay, please consider submitting your comments in electronic form, as prescribed above. The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible.

Comments on any proposed filing, recordkeeping, or disclosure requirements that are subject to paperwork burden review under the Paperwork Reduction Act should additionally be submitted to: Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission. Comments should be submitted via facsimile to (202) 395–6974 because U.S. Postal Mail is subject to lengthy delays due to heightened security precautions.

The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. All timely and responsive public comments, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC Web site, to the extent practicable, at *http://www.ftc.gov/os/publiccomments.htm*. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm*.

Members of the public also can request additional information or a copy of the collection from:

OCC: Mary Gottlieb, OCC Clearance Officer, (202) 874–5090, Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, 250 E Street, SW., Washington, DC 20219.

Board: Michelle Shore, Clearance Officer, Division of Research and Statistics (202) 452–3829.

FDIC: Steven F. Hanft, Clearance Officer, Legal Division, (202–898–3907).

OTS: Ira L. Mills, OTS Clearance Officer, Litigation Division, Chief Counsel's Office, at *Ira.Mills@ots.treas.gov*, (202) 906–6531, or facsimile number (202) 906–6518.

NCUA: Regina M. Metz, Staff Attorney, Office of General Counsel, (703) 518–6540.

FTC: See **FOR FURTHER INFORMATION CONTACT** above.

B. Regulatory Flexibility Act

OCC: Under section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), the OCC must either publish a Final Regulatory Flexibility Analysis (FRFA) for a final rule or certify, along with a statement providing the factual basis for such certification, the rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration has defined ''small entities'' for banking purposes as a bank or savings institution with assets of $165 million or less. *See* 13 CFR 121.201.

Based on its analysis and for the reasons stated below, the OCC certifies that this final rulemaking will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 114

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

In connection with the proposed rulemaking, the OCC concluded that the proposed regulations implementing section 114, if adopted as proposed, would not impose undue costs on national banks and would not have a substantial economic impact on a substantial number of small national banks. The OCC noted that national banks already employ a variety of measures that satisfy the requirements of the rulemaking because (1) such measures are a good business practice and generally are a part of a bank's efforts to reduce losses due to fraud, and (2) national banks already comply with other regulations and guidance that relate to information security, authentication, identity theft, and response programs. For example, national banks are already subject to CIP rules requiring them to verify the identity of a person opening a new account [68] and already have various systems in place to detect certain patterns, practices and specific activities that indicate the possible existence of identity theft in connection with the opening of new accounts. Similarly, national banks complying with the ''Interagency Guidelines Establishing Information Security Standards'' [69] and guidance recently issued by the FFIEC titled ''Authentication in an Internet Banking Environment'' [70] already have policies and procedures in place to detect attempted and actual intrusions into customer information systems and to detect patterns, practices and specific activities that indicate the possible existence of identity theft in connection with existing accounts. Banks complying with the OCC's ''Guidance on Identity Theft and Pretext Calling'' [71] already have policies and procedures to verify the validity of change of address requests on existing accounts.

Nonetheless, the OCC specifically requested comment and specific data on the size of the incremental burden creating an identity theft prevention program would have on small national banks, given banks'' current practices and compliance with existing requirements. The OCC also requested comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Commenters confirmed that the proposed regulations implementing section 114 of the FACT Act are consistent with banks'' usual and customary business practices used to minimize losses due to fraud in connection with new and existing

[67] Commission Rule 4.2(d), 16 CFR 4.2(d). The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. See Commission Rule 4.9(c), 16 CFR 4.9(c).

[68] 31 CFR 103.121; 12 CFR 21.21 (national banks).

[69] 12 CFR part 30, app. B (national banks).

[70] OCC Bulletin 2005–35 (Oct. 12, 2005).

[71] OCC AL 2001–4 (April 30, 2001).

accounts. They also confirmed that banks have implemented measures to address many of the proposed requirements as a result of having to comply with existing regulations and guidance. However, commenters also asserted that the Agencies had underestimated the incremental burden imposed by the proposed rules. They highlighted aspects of the proposal that they maintained would have required banks to alter their current practices and implement duplicative policies and procedures.

Only a few commenters provided estimates of additional burden that would result from the proposed rules. Many of these comments stemmed from a misreading of the requirements of the proposed rules. Further, many commenters confused the Agencies' PRA estimates with the Agencies' overall conclusions regarding regulatory burden.[72]

The OCC believes that the final rules substantially address the concerns of the commenters as follows:

- The final rules allow a covered entity to tailor its Program to its size, complexity and nature of its operations. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.
- The final rules list the four elements that must be a part of a Program, and the steps that a covered entity must take to administer the Program. The rules provide covered entities with greater discretion to determine how to implement these mandates.
- Additional requirements previously in the proposed rules are now in guidelines that are located in Appendix J. The guidelines describe various policies and procedures that a financial institution or creditor must consider and include in its Program, where appropriate, to satisfy the requirements of the final rules. The preamble to the rules explains that an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program as long as its Program contains reasonable policies and procedures to meet the specific requirements of the final rules.
- The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program.
- The final rules clarify that a Program (including the Red Flags determined to be relevant) may be periodically, rather than continually, updated to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
- The rules focus on consumer accounts, and require a Program to include only other accounts ''for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.''
- The definition of ''Red Flags'' no longer includes reference to the ''possible risk'' of identity theft and no longer incorporates precursors to identity theft.
- The final rules clarify that the Red Flags in Supplement A are examples rather than a mandatory checklist.
- Supplement A includes a Red Flag for activity on an inactive account in place of a separate guideline.
- The final rules clarify that the Board of Directors or a committee thereof must approve only the initial written Program. The rules provide a covered entity with the discretion to determine whether the Board or management will approve changes to the Program and the extent of Board involvement in oversight of the Program.
- The final rules clarify that only relevant staff must be trained to implement the Program, as necessary.
- Card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers' existing procedures.
- Covered entities need not comply with the final rules until November 1, 2008.

The Agencies did consider whether it would be appropriate to extend different treatment or exempt small covered entities from the requirements of this section of the final rulemaking. The Agencies note that identity theft can occur in small entities as well as large ones. The Agencies do not believe that an exemption for small entities is appropriate given the flexibility built into the final rules and guidelines and the importance of the statutory goals and mandate of section 114.

As a result of the changes and clarifications noted above, this section of the final rule is far more flexible and less burdensome than that in the proposed rules while still fulfilling the statutory mandates enumerated in section 114. Moreover, the OCC has concluded that the incremental cost of these final rules and guidelines will not impose undue costs and will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 315

The proposed regulations implementing section 315 required a user of consumer reports to have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. The proposed rules also required the user to furnish to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the user: (1) Is able to form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained; (2) establishes *or* maintains a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained.

In connection with the proposed rulemaking the OCC noted that the FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. The OCC stated that with respect to new accounts, a national bank already is required by the CIP rules to ensure that it knows the identity of a person opening a new account and to keep a record describing the resolution of any substantive discrepancy discovered during the verification process. The OCC also stated that as a matter of good business practice, most national banks currently have policies and procedures in place to respond to notices of address discrepancy when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the bank has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy.

The OCC specifically requested comment on whether the proposed requirements differ from small banks' current practices and whether the proposed requirements on users of consumer reports to have policies and procedures to respond to the receipt of an address discrepancy could be altered

[72] The PRA focuses more narrowly on the time, effort, and financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency. *See* 44 U.S.C. 3501 *et seq.*

to minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Many suggestions received in response to this solicitation for comment would have required a statutory change. However, many commenters noted that section 315 does not require the reporting of a confirmed address to a CRA for a notice of address discrepancy received for an existing account. These commenters stated that the level of regulatory burden imposed by this requirement would be significant and would force users to reconcile and verify addresses millions of times a year in connection with routine account maintenance. Commenters maintained that this would result in enormous costs that provide relatively little benefit to consumers. The final rules address these comments and accordingly, under the rules implementing section 315, a user is not obligated to furnish a confirmed address for the consumer to the CRA in connection with existing accounts.

Although, a bank will likely have to modify its existing procedures to add a new procedure for promptly reporting to CRAs the reconciled address for new deposit accounts, the OCC has concluded that the final rules implementing section 315 will not impose undue costs on national banks and will have not have a significant economic impact on a substantial number of small entities. Finally, as mentioned earlier, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

Board: The Board prepared an initial regulatory flexibility analysis as required by the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 *et seq.*) in connection with the July 18, 2006 proposed rule. The Board received one comment on its regulatory flexibility analysis.

Under Section 605(b) of the RFA, 5 U.S.C. 605(b), the regulatory flexibility analysis otherwise required under Section 604 of the RFA is not required if an agency certifies, along with a statement providing the factual basis for such certification, that the rule will not have a significant economic impact on a substantial number of small entities. Based on its analysis and for the reasons stated below, the Board certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

1. *Statement of the need for, and objectives of, the final rule.*

The FACT Act amends the FCRA and was enacted, in part, for the purpose of helping to reduce identity theft. Section 114 of the FACT Act amends section 615 of the FCRA and directs the Board, together with the other Agencies, to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances. Section 315 of the FACT Act adds section 605(h)(2) to the FCRA and requires the Agencies to issue joint regulations that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy. The Board received no comments on the reasons for the proposed rule. The Board is adopting the final rule to implement sections 114 and 315 of the FACT Act. The **SUPPLEMENTARY INFORMATION** above contains information on the objectives of the final rule.

2. *Summary of issues raised by comments in response to the initial regulatory flexibility analysis.*

In accordance with Section 3(a) of the RFA, the Board conducted an initial regulatory flexibility analysis in connection with the proposed rule. One commenter, the Mortgage Bankers Association (MBA), responded to the initial regulatory flexibility analysis and stated that contrary to the Agencies' belief, the proposed rule would have a significant economic impact on a substantial number of affected small entities. The MBA stated that commercial and multifamily mortgage lenders should not be subject to the proposed rule because it would constitute useless regulatory burden. Three commenters (Independent Community Bankers of America, The Financial Services Roundtable and BITS, and KeyCorp) believed that the Board and the other Agencies had underestimated the costs of compliance. The issues raised by these commenters did not apply uniquely to small entities and are described in the Paperwork Reduction Act section above.

Some small financial institutions expressed concern about the flexibility granted by the proposal. As stated in the Overview of Proposal and Comments Received, these commenters preferred to have more structured guidance that describes how to develop and implement a Program and what they would need to do to achieve compliance. In addition, one commenter expressed concern that smaller institutions would be particularly burdened by the proposal's requirement that the Program be designed to address changing identity risks ''as they arise.''

3. *Description and estimate of small entities affected by the final rule.*

The final rule applies to all banks that are members of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and Agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*). The Board's rule will apply to the following institutions (numbers approximate): State member banks (881), operating subsidiaries that are not functionally regulated with in the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (877), U.S. branches and agencies of foreign banks (219), commercial lending companies owned or controlled by foreign banks (3), and Edge and agreement corporations (64), for a total of approximately 2,044 institutions. The Board estimates that more than 1,448 of these institutions could be considered small entities with assets of $165 million or less.

4. *Recordkeeping, reporting, and other compliance requirements.*

Section 114 requires the Board to prescribe regulations that require financial institutions and creditors to establish reasonable policies and procedures to implement guidelines established by the Board and other federal agencies that address identity theft with respect to account holders and customers. This would be implemented by requiring a covered financial institution or creditor to create an Identity Theft Prevention Program that detects, prevents and mitigates the risk of identity theft applicable to its accounts.

Section 114 also requires the Board to adopt regulations applicable to credit and debit card issuers to implement policies and procedures to assess the validity of change of address requests. The final rule implements this by requiring credit and debit card issuers to establish reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the issuer receives a request for an additional or replacement card for the same account.

Section 315 requires the Board to prescribe regulations that provide guidance regarding the reasonable policies and procedures that a user of

consumers' reports should employ to verify the identity of a consumer when a consumer reporting agency provides a notice of address discrepancy with the consumer reporting agency in certain circumstances. The final rule requires users of consumer reports to develop and implement reasonable policies and procedures for verifying the identity of a consumer for whom it has obtained a consumer report and for whom it receives a notice of address discrepancy and to reconcile an address discrepancy with the appropriate consumer reporting agency in certain circumstances.

5. *Steps taken to minimize the economic impact on small entities.*

The Board and the other Agencies have attempted to minimize the economic impact on small entities by providing more flexibility in developing a Program and moving certain detail contained in the proposed regulations to the guidelines. In addition, to allow small entities and creditors to tailor their Programs to their operations, the final rules provide that the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. The Board has also eliminated the requirement for institutions to update their Program in response to changing identity theft risks ''as they arise.'' The final rule instead requires ''periodic'' updating.

FDIC: The FDIC prepared an initial regulatory flexibility analysis as required by the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 et seq.) in connection with the July 18, 2006 proposed rule. Under Section 605(b) of the RFA, 5 U.S.C. 605(b), the regulatory flexibility analysis otherwise required under Section 604 of the RFA is not required if an agency certifies, along with a statement providing the factual basis for such certification, that the rule will not have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include banks with less than $165 in assets). Based on its analysis and for the reasons stated below, the FDIC certifies that this final rule will not have a significant economic impact on a substantial number of small entities

Under the final rule implementing FACT Act Section 114, financial institutions and creditors must have a written program that includes controls to address the identity theft risks they have identified. Credit and debit card issuers must also have additional policies and procedures to assess the validity of change of address requests.

The final rule would apply to all FDIC-insured state nonmember banks, approximately 3,260 of which are small entities. The rule is drafted in a flexible manner that allows institutions to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.

The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program. The FDIC believes that many institutions have already implemented a significant portion of the detection and mitigation efforts required by the rule.

With respect to the portion of the rule covering card issuers, those entities may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers'' existing procedures.

Under the final rule implementing FACT Act Section 315, a user of consumer reports (which constitutes most, if not all, FDIC-insured state nonmember banks) must have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. Although, a bank will likely have to modify its existing procedures to add a new procedure for promptly reporting to consumer reporting agencies the reconciled address for new deposit accounts, the FDIC has concluded that the final rules implementing section 315—which only obligates a user to furnish a confirmed address for the consumer to the consumer reporting agency in connection with new, and not existing, accounts—will not impose undue costs on banks and will not have a significant economic impact on a substantial number of small entities.

Moreover, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

OTS: Under section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), OTS must either publish a Final Regulatory Flexibility Analysis (FRFA) for a final rule or certify, along with a statement providing the factual basis for such certification, the rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration has defined ''small entities'' to include savings associations with total assets of $165 million or less. 13 CFR 121.201.

The rule will implement section 114 and 315 of the FACT Act and will apply to all savings associations (and federal savings associations operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act), 424 of which have assets of less than or equal to $165 million. Based on its analysis and for the reasons stated below, OTS certifies that this final rulemaking will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 114

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

In connection with the proposed rulemaking, OTS concluded that the proposed regulations implementing section 114, if adopted as proposed, would not impose undue costs on savings associations and would not have a substantial economic impact on a substantial number of small savings associations. OTS noted that savings associations already employ a variety of measures that satisfy the requirements of the rulemaking because (1) such measures are a good business practice and generally are a part of a thrift's efforts to reduce losses due to fraud, and (2) savings associations already comply with other regulations and guidance that relate to information security, authentication, identity theft, and response programs. For example, savings associations are already subject to CIP rules requiring them to verify the identity of a person opening a new account [73] and already have various systems in place to detect certain patterns, practices and specific activities that indicate the possible existence of identity theft in connection with the opening of new accounts. Similarly, savings associations complying with the ''Interagency Guidelines Establishing

[73] 31 CFR 103.121; 12 CFR 563.177 (savings associations).

Information Security Standards'' [74] and guidance recently issued by the FFIEC titled ''Authentication in an Internet Banking Environment'' [75] already have policies and procedures in place to detect attempted and actual intrusions into customer information systems and to detect patterns, practices and specific activities that indicate the possible existence of identity theft in connection with existing accounts. Savings associations complying with OTS's guidance on ''Identity Theft and Pretext Calling'' [76] already have policies and procedures to verify the validity of change of address requests on existing accounts.

Nonetheless, OTS specifically requested comment and specific data on the size of the incremental burden creating an identity theft prevention program would have on small saving associations, given their current practices and compliance with existing requirements. OTS also requested comment on how the final regulations might minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Commenters confirmed that the proposed regulations implementing section 114 of the FACT Act are consistent with savings associations' usual and customary business practices used to minimize losses due to fraud in connection with new and existing accounts. They also confirmed that savings associations have implemented measures to address many of the proposed requirements as a result of having to comply with existing regulations and guidance. However, commenters also asserted that the Agencies had underestimated the incremental burden imposed by the proposed rules. They highlighted aspects of the proposal that they maintained would have required savings associations to alter their current practices and implement duplicative policies and procedures.

Only a few commenters provided estimates of additional burden that would result from the proposed rules. Many of these comments stemmed from a misreading of the requirements of the proposed rules. Further, many commenters confused the Agencies' PRA estimates with the Agencies' overall conclusions regarding regulatory burden.[77]

OTS believes that the final rules substantially address the concerns of the commenters as follows:

- The final rules allow a covered entity to tailor its Program to its size, complexity and nature of its operations. The final rules and guidelines do not require the use of any specific technology, systems, processes or methodology.
- The final rules list the four elements that must be a part of a Program, and the steps that a covered entity must take to administer the Program. The rules provide covered entities with greater discretion to determine how to implement these mandates.
- Additional requirements previously in the proposed rules are now in guidelines that are located in Appendix J. The guidelines describe various policies and procedures that a financial institution or creditor must consider and include in its Program, where appropriate, to satisfy the requirements of the final rules. The preamble to the rules explains that an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program as long as its Program contains reasonable policies and procedures to meet the specific requirements of the final rules.
- The guidelines clarify that a covered entity need not create duplicate policies and procedures and may incorporate into its Program, as appropriate, its existing processes that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, such as those already developed in connection with the entity's fraud prevention program.
- The final rules clarify that a Program (including the Red Flags determined to be relevant) may be periodically, rather than continually, updated to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
- The rules focus on consumer accounts, and require a Program to include only other accounts ''for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.''
- The definition of ''Red Flags'' no longer includes reference to the ''possible risk'' of identity theft and no longer incorporates precursors to identity theft.
- The final rules clarify that the Red Flags in Supplement A are examples rather than a mandatory checklist.
- Supplement A includes a Red Flag for activity on an inactive account in place of a separate guideline.
- The final rules clarify that the Board of Directors or a committee thereof must approve only the initial written Program. The rules provide a covered entity with the discretion to determine whether the Board or management will approve changes to the Program and the extent of Board involvement in oversight of the Program.
- The final rules clarify that only relevant staff must be trained to implement the Program, as necessary.
- Card issuers may satisfy the requirements of this section by verifying the address at the time the address change notification is received, whether or not the notification is linked to a request for an additional or replacement card—building on issuers' existing procedures.
- Covered entities need not comply with the final rules until November 1, 2008.

The Agencies did consider whether it would be appropriate to extend different treatment or exempt small covered entities from the requirements of this section of the final rulemaking. The Agencies note that identity theft can occur in small entities as well as large ones. The Agencies do not believe that an exemption for small entities is appropriate given the flexibility built into the final rules and guidelines and the importance of the statutory goals and mandate of section 114.

As a result of the changes and clarifications noted above, this section of the final rule is far more flexible and less burdensome than that in the proposed rules while still fulfilling the statutory mandates enumerated in section 114. Moreover, OTS has concluded that the incremental cost of these final rules and guidelines will not impose undue costs and will not have a significant economic impact on a substantial number of small entities.

Rules Implementing Section 315

The proposed regulations implementing section 315 required a user of consumer reports to have policies and procedures to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report. The proposed rules also required the user to furnish to the CRA from whom it received the notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the user: (1) Is able to form a reasonable belief that it knows the identity of the consumer

[74] 12 CFR part 570, app. B (savings associations).

[75] OTS CEO Letter 228 (Oct. 12, 2005).

[76] OTS CEO Letter 139 (May 4, 2001).

[77] The PRA focuses more narrowly on the time, effort, and financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency. *See* 44 U.S.C. 3501 *et seq.*

for whom the consumer report was obtained; (2) establishes *or* maintains a continuing relationship with the consumer; and (3) regularly and in the ordinary course of business furnishes information to the CRA from which a notice of address discrepancy pertaining to the consumer was obtained.

In connection with the proposed rulemaking OTS noted that the FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. OTS stated that with respect to new accounts, a savings association already is required by the CIP rules to ensure that it knows the identity of a person opening a new account and to keep a record describing the resolution of any substantive discrepancy discovered during the verification process. OTS also stated that as a matter of good business practice, most savings associations currently have policies and procedures in place to respond to notices of address discrepancy when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the association has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy.

OTS specifically requested comment on whether the proposed requirements differ from small savings associations' current practices and whether the proposed requirements on users of consumer reports to have policies and procedures to respond to the receipt of an address discrepancy could be altered to minimize any burden imposed to the extent consistent with the requirements of the FACT Act.

Many suggestions received in response to this solicitation for comment would have required a statutory change. However, many commenters noted that section 315 does not require the reporting of a confirmed address to a CRA for a notice of address discrepancy received for an existing account. These commenters stated that the level of regulatory burden imposed by this requirement would be significant and would force users to reconcile and verify addresses millions of times a year in connection with routine account maintenance. Commenters maintained that this would result in enormous costs that provide relatively little benefit to consumers. The final rules address these comments and, accordingly, under the rules implementing section 315, a user is not obligated to furnish a confirmed address for the consumer to the CRA in connection with existing accounts.

Although, a savings association will likely have to modify its existing procedures to add a new procedure for promptly reporting to CRAs the reconciled address for new deposit accounts, OTS has concluded that the final rules implementing section 315 will not impose undue costs on savings associations and will have not have a significant economic impact on a substantial number of small entities. Finally, as mentioned earlier, the final rules provide a transition period and do not require covered entities to fully comply with these requirements until November 1, 2008.

FTC: The Regulatory Flexibility Act (''RFA''), 5 U.S.C. 601–612, requires that the Commission provide an Initial Regulatory Flexibility Analysis (''IRFA'') with a proposed rule and a Final Regulatory Flexibility Analysis (''FRFA''), if any, with the final rule, unless the Commission certifies that the rule will not have a significant economic impact on a substantial number of small entities. *See* 5 U.S.C. 603–605.

The Commission hereby certifies that the final regulations will not have a significant economic impact on a substantial number of small business entities. The Commission recognizes that the final regulations will affect a substantial number of small businesses. We do not expect, however, that the final regulations will have a significant economic impact on these small entities.

The Commission continues to believe that a precise estimate of the number of small entities that fall under the final regulations is not currently feasible. Based on changes made to the final regulations in response to comments received, however, and the Commission's own experience and knowledge of industry practices, the Commission also continues to believe that the cost and burden to small business entities of complying with the final regulations are minimal. Accordingly, this document serves as notice to the Small Business Administration of the agency's certification of no effect. Nonetheless, the Commission has decided to publish a FRFA with these final regulations. Therefore, the Commission has prepared the following analysis:

1. Need for and Objectives of the Rule

The FTC is charged with enforcing the requirements of sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) (15 U.S.C. §§ 1681m(e) and 1681c(h)(2)), which require the FTC to establish guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft, and regulations requiring each financial institution and creditor to establish policies and procedures for implementing the guidelines. In addition, section 114 requires credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. Section 315 requires the FTC to develop policies and procedures that a user of consumer reports must employ when such a user receives a notice of address discrepancy from a consumer reporting agency described in section 603(p) of the FCRA. In this action, the FTC promulgates final rules that would implement these requirements of the FACT Act.

2. Significant Issues Received by Public Comment

The Commission received a number of comments on the effect of the proposed regulations. Some of the comments addressed the effect of the proposed regulations on businesses generally, and did not identify small businesses as a particular category. The FTC staff, therefore, has included all comments in this FRFA that raised potentially significant compliance issues for small businesses, regardless of whether the commenter identified small businesses as being an affected category.

In drafting its PRA analysis for the proposed regulations, FTC staff believed that because motor vehicle dealers' loans typically are financed by financial institutions also subject to those regulations, the dealers were likely to use the latter's programs as a basis to develop their own. Therefore, although subject to a high risk of identity theft, their burden would be less than other high-risk entities. Commenters, however, noted among other concerns that some motor vehicle dealers finance their own loans. Thus, FTC staff no longer is considering motor vehicle dealers separately from other high-risk entities.

As noted in the PRA analysis, the Agencies continue to believe that many of the high-risk entities, as part of their usual and customary business practices, already take steps to minimize losses due to fraud. The final rulemaking clarifies that only relevant staff need be trained to implement the Program, as necessary—meaning, for example, that staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be re-trained except as incrementally needed. Notwithstanding this clarification, in response to comments received, the Agencies are increasing the burden estimates attributable to training from two to four hours, as is the FTC for high-risk entities in their initial year of

implementing the Program, but FTC staff continues to believe that one hour of recurring annual training remains a reasonable estimate.

A few commenters believed that FTC staff had underestimated the amount of time it would take low-risk entities to comply with the proposed regulations. These commenters estimated that the amount of time would range from 6 to 20 hours to create a program and 1 hour each to train employees and draft the annual report. The FTC staff believes these estimates were based on a misunderstanding of the requirements of the proposed regulations, including that the list of 31 Red Flags in the proposed guidelines was intended to be a checklist. The final regulations clarify that the list of Red Flags is illustrative only. Moreover, the emphasis of the written Program, as required under the final regulations, is to identify risks of identity theft. To the extent that entities with consumer accounts determine that they have a minimal risk of identity theft, they would be tasked only with developing a streamlined Program. Therefore, FTC staff does not believe that it would take such an entity 6 to 20 hours to develop a Program, 1 hour to train employees, and 1 hour to draft an annual report on risks of identity theft which are minimal or non-existent. Nonetheless, FTC staff believes that it may have underestimated the time low-risk entities may need to initially apply the final rule to develop a Program. Thus, FTC staff has increased from 20 minutes to 1 hour its previously stated estimate for this activity.

In addition, the final regulations have been revised from the proposed regulations to alleviate the burden of creating a written Program for entities that determine that they do not have any covered accounts. The FTC staff believes that entities subject to a low risk of identity theft, but not having consumer accounts, will likely determine that they do not have covered accounts. Such entities would not be required to develop a written Program. The FTC staff estimates that approximately 9,191,496 [78] of the 10,813,525 low-risk entities subject to the requirement to create a written Program under the proposed regulations will not have covered accounts under the final rule. Therefore, although these 9,191,496 low-risk entities will have to conduct a periodic risk assessment to determine if they covered accounts, they will not be required to develop a written Program, thereby substantially reducing the original burden estimate in the NPRM for low-risk entities.

The FTC received additional comments on its IRFA requesting that the FTC delay implementation of the final rules for small businesses by a minimum of six months, consider creating a certification form for low-risk entities, and develop a small business compliance guide. The Agencies have set a mandatory compliance deadline of November 1, 2008, thereby providing all entities with well over six months in which to implement the final regulations. The FTC staff will be developing a small business compliance guide prior to the mandatory compliance deadline of November 1, 2008. The FTC staff will consider whether to include any model forms in such guide.

The FTC did not receive any comments on its IRFA for the proposed regulations implementing section 114 requiring credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request, including notifying the cardholder or using another means of assessing the validity of the change of address. The FTC staff does not believe that the changes made to the final regulation have altered its original burden estimates.

The FTC did not receive any comments on its IRFA relating to the proposed regulations under section 315.

3. Small Entities to Which the Final Rule Will Apply

The final regulations apply to a wide variety of business categories under the Small Business Size Standards. Generally, the final regulations would apply to financial institutions, creditors, and users of consumer reports. In particular, entities under FTC's jurisdiction covered by section 114 include State-chartered credit unions, non-bank lenders, mortgage brokers, automobile dealers, utility companies, telecommunications companies, and any other person that regularly participates in a credit decision, including setting the terms of credit. The section 315 requirements apply to State-chartered credit unions, non-bank lenders, insurers, landlords, employers, mortgage brokers, automobile dealers, collection agencies, and any other person who requests a consumer report from a consumer reporting agency described in section 603(p) of the FCRA.

Given the coverage of the final rules, a very large number of small entities across almost every industry could be subject to the final rules. For the majority of these entities, a small business is defined by the Small Business Administration as one whose average annual receipts do not exceed $6.5 million or who have fewer than 500 employees.[79]

Section 114: As discussed in the PRA section of this Notice, given the broad scope of section 114's requirements, it is difficult to determine with precision the number of financial institutions and creditors that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the final regulations implementing section 114 will affect over 3500 financial institutions and over 11 million creditors [80] subject to the FTC's jurisdiction, for a combined total of approximately 11.1 million affected entities. Of this total, the FTC staff expects that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors).

One commenter acknowledged that the FTC's estimates as to the number of small entities that will be affected were accurate, but did not provide precise numbers.

The final regulations implementing section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. Indeed, the final regulations require credit and debit card issuers to notify the cardholder or to use another means of assessing the validity of the change of address. FTC staff believes that there may be as many as 3,764 credit or debit card issuers that fall under the jurisdiction of the FTC and that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial

[78] This estimate is derived from an analysis of a database of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers or other businesses, net of the number of creditors subject to the FTC's jurisdiction, an estimated subset of which comprise anticipated low-risk entities not having covered accounts under the final rule.

[79] These numbers represent the size standards for most retail and service industries ($6.5 million total receipts) and manufacturing industries (500 employees). A list of the SBA's size standards for all industries can be found at *http://www.sba.gov/size/summary-whatis.html*.

[80] This estimate is derived from census data of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers and businesses. 2003 County Business Patterns, U.S. Census Bureau *(http://censtats.census.gov/cgi- bin/cbpnaic/cbpsel.pl)*; and 2002 Economic Census, Bureau *(http://www.census.gov/econ/census02/)*.

institutions and $6.5 million in sales for many creditors).

The Commission did not receive any comments to the IRFA on the latter credit or debit card issuers that would allow it to determine the precise number of small entities that will be affected.

Section 315: As discussed in the PRA section of this Notice, given the broad scope of section 315's requirements, it is difficult to determine with precision the number of users of consumer reports that are subject to the FTC's jurisdiction. There are numerous small businesses under the FTC's jurisdiction and there is no formal way to track them; moreover, as a whole, the entities under the FTC's jurisdiction are so varied that there are no general sources that provide a record of their existence. Nonetheless, FTC staff estimates that the final regulations implementing section 315 will affect approximately 1.6 million users of consumer reports subject to the FTC's jurisdiction [81] and that well over 90% of these firms qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors).

The Commission did not receive any comments to the IRFA on the proposed regulations under Section 315 that would allow it to determine the precise number of small entities that will be affected.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The final requirements will involve some increased costs for affected parties. Most of these costs will be incurred by those required to conduct periodic risk assessments, and draft identity theft Programs and annual reports. There will also be costs associated with training, and for credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. In addition, there will be costs related to developing reasonable policies and procedures that a user of consumer reports must employ when a user receives a notice of address discrepancy from a consumer reporting agency, and for furnishing an address that the user has reasonably confirmed is accurate. The Commission does not expect, however, that the increased costs associated with the final regulations will be significant as explained below.

Section 114: The FTC staff estimates that there may be as many as 90% of the businesses affected by the proposed rules under section 114 that are subject to a high risk of identity theft that qualify as small businesses. It is likely that many such entities already engage in various activities to minimize losses due to fraud as part of their usual and customary business practices. Accordingly, the impact of the proposed requirements would be merely incremental and not significant. In particular, the rule will direct many of these entities to consolidate their existing policies and procedures into a written Program and may require some additional staff training.

The FTC expects that well over 90% of the businesses affected by the proposed rules under section 114 that are subject to a low risk of identity theft qualify as small businesses under existing size standards (*i.e.*, $165 million in assets for financial institutions and $6.5 million in sales for many creditors). The final requirements are drafted in a flexible manner that limits the burden on a substantial majority of low-risk entities to conducting periodic risk assessments for covered accounts, and allows the remaining minority of low-risk entities to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. As a result, the FTC staff expects that the burden on these low-risk entities will be minimal (*i.e.*, not significant). The final regulations would require low-risk entities that have covered accounts that have no existing identity theft procedures to state in writing their low-risk of identity theft, train staff to be attentive to future risks of identity theft, and, if appropriate, prepare an annual report. The FTC staff believes that, for the affected low-risk entities, such activities will be not be complex or resource-intensive tasks.

The final regulations implementing section 114 also require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. It is likely that most of the entities have automated the process of notifying the cardholder or using other means to assess the validity of the change of address such that implementation will pose no further burden. For those that do not, the FTC staff expects that a small number of such entities (100) will need to develop policies and procedures to assess the validity of a change of address request. The impacts on such entities should not be significant, however.

In calculating the costs, FTC staff assumes that for all entities, professional technical personnel and/or managerial personnel will conduct the periodic risk assessment, create and implement the Program, prepare the annual report, train employees, and assess the validity of a change of address request.

Section 315: The final regulations implementing section 315 provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a user receives a notice of address discrepancy from a consumer reporting agency. The final regulations also require a user of consumer reports to furnish an address that the user has reasonably confirmed is accurate to the consumer reporting agency from which it receives a notice of address discrepancy, but only to the extent that such user regularly and in the ordinary course of business furnishes information to such consumer reporting agency. The FTC staff believes that the impacts on users of consumer reports that are small businesses will not be significant. As discussed in the PRA section of the NPRM, the FTC staff believes that it will not take users of consumer reports under FTC jurisdiction a significant amount of time to develop policies and procedures that they will employ when they receive a notice of address discrepancy. FTC staff believes that only 10,000 of such users of consumer reports furnish information to consumer reporting agencies as part of their usual and customary business practices and that approximately 20% of these entities qualify as small businesses. Therefore, the staff estimates that 2,000 small businesses will be affected by this portion of the final regulation that requires furnishing the correct address. As discussed in the PRA section of this NPRM, FTC staff estimates that it will not take such users of consumer reports a significant amount of time to develop the policies and procedures for furnishing the correct address to the consumer reporting agencies pursuant to the final regulations for implementing section 315. The FTC staff estimates that the costs associated with these impacts will not be significant.

In calculating these costs, FTC staff assumes that the policies and procedures for notice of address discrepancy and furnishing the correct address will be set up by administrative support personnel.

[81] This estimate is derived from census data of U.S. businesses based on NAICS codes for businesses that market goods or services to consumers and businesses. 2003 County Business Patterns, U.S. Census Bureau *(http://censtats.census.gov/cgi-bin/cbpnaic/cbpsel.pl);* and 2002 Economic Census, Bureau *(http://www.census.gov/econ/census02/).*

5. Steps Taken To Minimize Significant Economic Impact of the Rule on Small Entities

The Commission considered whether any significant alternatives, consistent with the purposes of the FACT Act, could further minimize the final regulations' impact on small entities. The FTC asked for comment on this issue. The final requirements are drafted in a flexible manner that limits the burden on a substantial majority of low-risk entities to conducting periodic risk assessments for covered accounts and allows the remaining minority of low-risk entities to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. In addition, a commenter requested that the FTC delay implementation of the final rules for small businesses by a minimum of six months, produce a shortened Red Flags list, consider creating a certification form for low-risk entities, and develop a small business compliance guide. The Agencies have set a mandatory compliance deadline of November 1, 2008, thereby providing all entities with well over six months in which to implement the final regulations. As discussed in the PRA analysis *infra*, the Agencies have clarified that the Red Flags Supplement is illustrative only, and is not intended to be used as a checklist. Therefore, the Agencies did not consider it necessary to alter the Red Flags listed. The FTC staff will be developing a small business compliance guide prior to the mandatory compliance deadline of November 1, 2008. The FTC staff will consider whether to include any model forms in such guide.

C. OCC and OTS Executive Order 12866 Determination

The OCC and the OTS each have independently determined that the final rule is not a ''significant regulatory action'' as defined in Executive Order 12866 because the annual effect on the economy is less than $100 million. Accordingly, a regulatory assessment is not required.

D. OCC and OTS Executive Order 13132 Determination

The OCC and the OTS each has determined that these final rules do not have any federalism implications for purposes of Executive Order 13132.

E. NCUA Executive Order 13132 Determination

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on State and local interests. In adherence to fundamental federalism principles, the NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5) voluntarily complies with the Executive Order. These final rules apply only to federally chartered credit unions and would not have substantial direct effects on the States, on the connection between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. The NCUA has determined that these final rules do not constitute a policy that has federalism implications for purposes of the Executive Order.

F. OCC and OTS Unfunded Mandates Reform Act of 1995 Determination

Section 202 of the Unfunded Mandates Reform Act of 1995, Public Law 104–4 (Unfunded Mandates Act) requests that an agency prepare a budgetary impact statement before promulgating a rule that includes a federal mandate that may result in expenditure by State, local, and tribal governments, in the aggregate, or by the private section, of $100 million or more in any one year. If a budgetary impact statement is required, section 205, of the Unfunded Mandates Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule.

The OCC and OTS each has determined that this rule will not result in expenditures by State, local, and tribal governments, or by the private sector, of $100 million or more. National banks and savings associations already employ a variety of measures that satisfy the requirements of the final rulemaking because, as described earlier, these are usual and customary business practices to minimize losses due to fraud, or because, as described earlier, they already comply with other existing regulations and guidance that relate to information security, authentication, identity theft, and response programs. Accordingly, neither the OCC not the OTS has prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

G. NCUA: The Treasury and General Government Appropriations Act, 1999—Assessment of Federal Regulations and Policies on Families

The NCUA has determined that these final rules will not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105–277, 112 Stat. 2681 (1998).

H. NCUA: Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) Determination

A SBREFA (Pub. L. 104–121) reporting requirement is triggered in instances where NCUA issues a final rule as defined by section 551 of the Administrative Procedure Act, 5 U.S.C. 551. NCUA has determined this final rule is not a major rule for purposes of SBREFA and the Office of Management and Budget (OMB) has concurred.

I. Plain Language

Section 722 of the Gramm-Leach-Bliley Act (12 U.S.C. 4809) requires the Federal banking agencies and the NCUA to use ''plain language'' in all proposed and final rules published in the **Federal Register**. The Agencies received no comments on how to make the rules easier to understand, and believe the final rules are presented in a clear and straightforward manner.

List of Subjects

12 CFR Part 41

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

12 CFR Part 222

Banks, banking, Holding companies, state member banks.

12 CFR Part 334

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and soundness.

12 CFR Part 364

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 571

Consumer protection, Credit, Fair Credit Reporting Act, Privacy, Reporting and recordkeeping requirements, Savings associations.

12 CFR Part 717

Consumer protection, Credit unions, Fair credit reporting, Privacy, Reporting and recordkeeping requirements.

16 CFR Part 681

Fair Credit Reporting Act, Consumer reports, Consumer report users, Consumer reporting agencies, Credit, Creditors, Information furnishers, Identity theft, Trade practices.

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Office of the Comptroller of the Currency amends Part 41 of title 12, chapter I, of the Code of Federal Regulations as follows:

PART 41—FAIR CREDIT REPORTING

■ 1. The authority citation for part 41 continues to read as follows:

Authority: 12 U.S.C. 1 *et seq.,* 24 (Seventh), 93a, 481, 484, and 1818; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–3, 1681t, 1681w, Sec. 214, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Section 41.1 is added to read as follows:

§ 41.1 Purpose.

(a) *Purpose.* The purpose of this part is to establish standards for national banks regarding consumer report information. In addition, the purpose of this part is to specify the extent to which national banks may obtain, use, or share certain information. This part also contains a number of measures national banks must take to combat consumer fraud and related crimes, including identity theft.

(b) [Reserved]

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

§ 41.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 4. Revise the heading for Subpart I to read as follows:

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

■ 5. Add § 41.82 to read as follows:

§ 41.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a national bank, Federal branch or agency of a foreign bank, or any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 6. Add Subpart J to part 41 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.
41.90 Duties regarding the detection, prevention, and mitigation of identity theft.
41.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

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

(a) *Scope.* This section applies to a financial institution or creditor that is a national bank, Federal branch or agency of a foreign bank, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell

phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

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

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 41.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a national bank, Federal branch or agency of a foreign bank, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 41.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendices D–I [Reserved]

■ 7. Add and reserve appendices D through I to part 41.

■ 8. Add Appendix J to part 41 to read as follows:

Appendix J to Part 41—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 41.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 41.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the

formulation and maintenance of a Program that satisfies the requirements of § 41.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

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

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 41.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 41.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 41.82(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
a. A recent and significant increase in the volume of inquiries;
b. An unusual number of recently established credit relationships;
c. A material change in the use of credit, especially with respect to recently established credit relationships; or
d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
a. The address does not match any address in the consumer report; or
b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
a. The address on an application is the same as the address provided on a fraudulent application; or
b. The phone number on an application is the same as the number provided on a fraudulent application.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
a. The address on an application is fictitious, a mail drop, or a prison; or
b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
a. Nonpayment when there is no history of late or missed payments;
b. A material increase in the use of available credit;
c. A material change in purchasing or spending patterns;
d. A material change in electronic fund transfer patterns in connection with a deposit account; or
e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Board of Governors of the Federal Reserve System

12 CFR Chapter II.

Authority and Issuance

■ For the reasons set forth in the joint preamble, part 222 of title 12, chapter II, of the Code of Federal Regulations is amended as follows:

PART 222—FAIR CREDIT REPORTING (REGULATION V)

■ 1. The authority citation for part 222 continues to read as follows:

Authority: 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–2, 1681s–3, 1681t, and 1681w; Secs. 3 and 214, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Section 222.3 is amended by revising the introductory text to read as follows:

§ 222.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. The heading for Subpart I is revised to read as follows:

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

■ 4. A new § 222.82 is added to read as follows:

§ 222.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a member bank of the Federal Reserve System (other than a national bank) and its respective operating subsidiaries, a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), commercial

lending company owned or controlled by a foreign bank, and an organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 5. A new Subpart J is added to part 222 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.
222.90 Duties regarding the detection, prevention, and mitigation of identity theft.
222.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

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

(a) *Scope.* This section applies to financial institutions and creditors that are member banks of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*).

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

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

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

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate

identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 222.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 222.90(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 222.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendices D–I [Reserved]

■ 6. Appendices D through I to part 222 are added and reserved.

■ 7. A new Appendix J is added to part 222 to read as follows:

Appendix J to Part 222—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 222.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 222.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 222.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

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

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules

implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 222.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 222.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 222.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

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

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Federal Deposit Insurance Corporation is amending 12 CFR parts 334 and 364 of title 12, Chapter III, of the Code of Federal Regulations as follows:

PART 334—FAIR CREDIT REPORTING

■ 1. The authority citation for part 334 is revised to read as follows:

Authority: 12 U.S.C. 1818, 1819 (Tenth) and 1831p–1; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–3, 1681t, 1681w, 6801 and 6805, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 334.3 by revising the introductory text to read as follows:

§ 334.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. Revise the heading for Subpart I as shown below.

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

■ 4. Add § 334.82 to read as follows:

§ 334.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency and that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

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

Subpart J—Identity Theft Red Flags

Sec.
334.90 Duties regarding the detection, prevention, and mitigation of identity theft.
334.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

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

(a) *Scope.* This section applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

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

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

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

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program*—(1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 334.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a

change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 334.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendices D–I [Reserved]

■ 6. Add and reserve appendices D through I to part 334.

■ 7. Add Appendix J to part 334 to read as follows:

Appendix J to Part 334—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 334.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 334.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 334.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

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

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. *Detecting Red Flags.*

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l)(31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. *Preventing and Mitigating Identity Theft.*

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. *Updating the Program.*

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 334.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the

financial institution or creditor with § 334.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

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

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

■ 8. The authority citation for part 364 is revised to read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth), 1831p–1; 15 U.S.C. 1681b, 1681s, 1681w, 6801(b), 6805(b)(1).

■ 9. Add the following sentence at the end of § 364.101(b):

§ 364.101 Standards for safety and soundness.

* * * * *

(b) * * * The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in §§ 334.90, 334.91, and Appendix J of part 334.

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Chapter V

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Office of Thrift Supervision is amending part 571 of title 12, chapter V, of the Code of Federal Regulations as follows:

PART 571—FAIR CREDIT REPORTING

■ 1. Revise the authority citation for part 571 to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, and 1881–1884; 15 U.S.C. 1681b, 1681c, 1681m, 1681s, 1681s–1, 1681t and 1681w; 15 U.S.C. 6801 and 6805; Sec. 214 Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 571.1 by revising paragraph (b)(9) and adding a new paragraph (b)(10) to read as follows:

§ 571.1 Purpose and Scope.

* * * * *

(b) *scope.*

* * * * *

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

(ii) The scope of § 571.83 of Subpart I of this part is stated in § 571.83(a) of this part.

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

(ii) The scope of § 571.91 of Subpart J of this part is stated in § 571.91(a) of this part.

■ 3. Amend § 571.3 by:

■ a. Removing paragraph (o); and

■ b. Revising the introductory text to read as follows:

§ 571.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 4. Revise the heading for Subpart I as shown below.

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

■ 5. Add § 571.82 to read as follows:

§ 571.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 6. Amend § 571.83 by:

■ a. Redesignating paragraphs (a) and (b) as paragraphs (b) and (c), respectively.

■ b. Adding a new paragraph (a) to read as follows:

§ 571.83 Disposal of consumer information.

(a) *Scope.* This section applies to savings associations whose deposits are

insured by the Federal Deposit Insurance Corporation and federal savings association operating subsidiaries in accordance with § 559.3(h)(1) of this chapter (defined as ''you'').

* * * * *

■ 7. Add Subpart J to part 571 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.
571.90 Duties regarding the detection, prevention, and mitigation of identity theft.
571.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

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

(a) *Scope.* This section applies to a financial institution or creditor that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

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

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 571.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a savings association whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, a federal savings association operating subsidiary that is not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a

change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 571.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendices D–I [Reserved]

■ 8. Add and reserve appendices D through I to part 571.

■ 9. Add Appendix J to part 571 to read as follows:

Appendix J to Part 571—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 571.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 571.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 571.90 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

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

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 571.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated

employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 571.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 571.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or

transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

National Credit Union Administration

12 CFR Chapter VII

Authority and Issuance

■ For the reasons discussed in the joint preamble, the National Credit Union Administration is amending part 717 of title 12, chapter VII, of the Code of Federal Regulations as follows:

PART 717—FAIR CREDIT REPORTING

■ 1. The authority citation for part 717 is revised to read as follows:

Authority: 12 U.S.C. 1751 *et seq.*; 15 U.S.C. 1681a, 1681b, 1681c, 1681m, 1681s, 1681s–1, 1681t, 1681w, 6801 and 6805, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend § 717.3 by revising the introductory text to read as follows:

§ 717.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

■ 3. Revise the heading for Subpart I as shown below.

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

■ 4. Add § 717.82 to read as follows:

§ 717.82 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is federal credit union.

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief*—(1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other member account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address*—(1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

■ 5. Add Subpart J to part 717 to read as follows:

Subpart J—Identity Theft Red Flags

Sec.
717.90 Duties regarding the detection, prevention, and mitigation of identity theft.
717.91 Duties of card issuers regarding changes of address.

Subpart J—Identity Theft Red Flags

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

(a) *Scope.* This section applies to a financial institution or creditor that is a federal credit union.

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

(1) *Account* means a continuing relationship established by a person with a federal credit union to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A share or deposit account.

(2) The term *board of directors* refers to a federal credit union's board of directors.

(3) *Covered account* means:

(i) An account that a federal credit union offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, checking account, or share account; and

(ii) Any other account that the federal credit union offers or maintains for which there is a reasonably foreseeable risk to members or to the safety and soundness of the federal credit union from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(6) *Customer* means a member that has a covered account with a federal credit union.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

(10) *Service provider* means a person that provides a service directly to the federal credit union.

(c) *Periodic Identification of Covered Accounts.* Each federal credit union must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a federal credit union must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each federal credit union that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the federal credit union and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the federal credit union offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the federal credit union;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to members and to the safety and soundness of the federal credit union from identity theft.

(e) *Administration of the Program.* Each federal credit union that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each federal credit union that is required to implement a Program must consider the guidelines in Appendix J of this part and include in its Program those guidelines that are appropriate.

§ 717.91 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to an issuer of a debit or credit card (card issuer) that is a federal credit union.

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a member who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a member's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 717.90 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendices D–I [Reserved]

■ 6. Add and reserve appendices D through I to part 717.

■ 7. Add Appendix J to part 717 to read as follows:

Appendix J to Part 717—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 717.90 of this part requires each federal credit union that offers or maintains one or more covered accounts, as defined in § 717.90(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist federal credit unions in the formulation and maintenance of a Program that satisfies the requirements of § 717.90 of this part.

I. The Program

In designing its Program, a federal credit union may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to members or to the safety and soundness of the federal credit union from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A federal credit union should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Federal credit unions should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the federal credit union has experienced;

(2) Methods of identity theft that the federal credit union has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix J.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the federal credit union.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating members, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the federal credit union has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a federal credit union should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a member's account records held by the federal credit union or a third party, or notice that a member has provided information related to a covered account held by the federal credit union to someone fraudulently claiming to represent the federal credit union or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the member;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Federal credit unions should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to members or to the safety and soundness of the federal credit union from identity theft, based on factors such as:

(a) The experiences of the federal credit union with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the federal credit union offers or maintains; and

(e) Changes in the business arrangements of the federal credit union, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the federal credit union with § 717.90 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the federal credit union responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the federal credit union with § 717.90 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the federal credit union in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a federal credit union engages a service provider to perform an activity in connection with one or more covered accounts the federal credit union should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a federal credit union could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the federal credit union, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Federal credit unions should be mindful of other related legal requirements that may be applicable, such as:

(a) Filing a Suspicious Activity Report under 31 U.S.C. 5318(g) and 12 CFR 748.1(c);

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the federal credit union detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each federal credit union may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings From a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 717.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or member presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the federal credit union, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the federal credit union. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the federal credit union. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the federal credit union. For example:

a. The address on an application is fictitious, a mail drop, or prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other members.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other members.

16. The person opening the covered account or the member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the federal credit union.

18. For federal credit unions that use challenge questions, the person opening the covered account or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The member fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account.

24. The federal credit union is notified that the member is not receiving paper account statements.

25. The federal credit union is notified of unauthorized charges or transactions in connection with a member's covered account.

Notice From Members, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Federal Credit Union

26. The federal credit union is notified by a member, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

FEDERAL TRADE COMMISSION

16 CFR Part 681

Authority and Issuance

■ For the reasons discussed in the joint preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

PART 681—IDENTITY THEFT RULES

Sec.
681.1 Duties of users of consumer reports regarding address discrepancies.
681.2 Duties regarding the detection, prevention, and mitigation of identity theft.
681.3 Duties of card issuers regarding changes of address.

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Authority: Pub. L. 108–159, sec. 114 and sec. 315; 15 U.S.C. 1681m(e) and 15 U.S.C. 1681c(h).

§ 681.1 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1) (users).

(b) *Definition.* For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(c) *Reasonable belief.* (1) *Requirement to form a reasonable belief.* A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:

(A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);

(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

(C) Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.* A user must develop and implement reasonable policies and procedures for furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

(ii) Establishes a continuing relationship with the consumer; and

(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;

(ii) Reviewing its own records to verify the address of the consumer;

(iii) Verifying the address through third-party sources; or

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance

with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

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

(a) *Scope.* This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

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

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

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

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

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

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate.

§ 681.3 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 681.2(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 681.2 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

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

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

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

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.* Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags

that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

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

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Dated: October 5, 2007.

John C. Dugan,

Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System, October 29, 2007.

Jennifer J. Johnson,

Secretary of the Board.

Dated at Washington, DC, this 16th day of October, 2007.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

Dated: October 24, 2007.

By the Office of Thrift Supervision.

John M. Reich,

Director.

By order of the National Credit Union Administration Board, October 15, 2007.

Mary Rupp,

Secretary of the Board.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 07–5453 Filed 11–8–07; 8:45 am]

BILLING CODE 4810–33–P; 6210–01–P; 6714–01–P; 6720–01–P; 7535–01–P; 6750–01–P