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 would apply to the following institutions (numbers approximate): State member banks (902), U.S. branches and agencies of foreign banks (206), commercial lending companies owned or controlled by foreign banks (3), and Edge and agreement corporations (71), for a total of approximately 1,182 institutions. The Board estimates that more than 550 of these institutions could be considered small institutions with assets less than $165 million.

D. Projected Reporting, Recordkeeping 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 identify 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 proposed rule would implement 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 (at least 30 days), 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 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 relating to that consumer and to reconcile the address discrepancy with the consumer reporting agency in certain circumstances. The proposed rule would require 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.

The Board seeks information and comment on any costs, compliance requirements, or changes in operating procedures arising from the application of the proposed rules in addition to or which may differ from those arising from the application of the statute generally.

E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules.

The Board is unable to identify any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed rule. The Board seeks comment regarding any statutes or regulations, including state or local statutes or regulations, that would duplicate, overlap, or conflict with the proposed rule, including particularly any statutes or regulations that address situations in which institutions must adopt specified policies and procedures to detect or prevent identity theft or mitigate identity theft that has occurred.

Section 222.90 of the Board's proposed rule would require financial institutions and creditors that are subject to the Board's rule to implement a written identity theft program that includes reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor. Many of these entities also are subject to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (see 12 C.F.R. Part 208, Appendix D-1) and rules of the Department of Treasury that require these entities to implement customer identification programs (see 31 C.F.R. 103.121).

Programs adopted pursuant to these requirements would include policies and procedures that would safeguard against the theft of customer information and would be considered complementary to the identity theft prevention program that would be required under section 222.90. For example, proposed section 222.90(d) would require that institutions adopt reasonable policies and procedures to, among other things, obtain identifying information about, and verify the identity of, persons opening an account. The proposed rule indicates that policies and procedures an institution has adopted under the Department of Treasury's rules on customer identification programs would satisfy this requirement.

F. Discussion of Significant Alternatives.

The proposed rules would require financial institutions and creditors to create an Identity Theft Prevention Program, maintain a record of the Program, and report to the board of directors, a committee of the board, or senior management at least annually on compliance with the regulations. Credit and debit card issuers would be required to assess the validity of a change of address request by notifying the cardholder or using other means to assess the validity of a change of address. Users of consumer reports would be required 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.

The Board welcomes comments on any significant alternatives, consistent with the mandates in section 114 and 315, that would minimize the impact of the proposed rules on small entities.

FDIC: In accordance with the Regulatory Flexibility Act (5 U.S.C. 601-612) (RFA), an agency must publish an initial regulatory flexibility analysis with its proposed rule, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include banks with less than $165 million in

assets). The FDIC hereby certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities.

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

The proposed rule would apply to all FDIC-insured state nonmember banks, approximately 3,400 of which are small entities. The proposed rule is drafted in a flexible manner that allows institutions to develop and implement different types of programs based upon their size, complexity, and the nature and scope of their activities. The proposed rule would also permit institutions to modify existing information security programs to address identity theft. The FDIC also believes that many institutions have already implemented a significant portion of the detection and mitigation efforts required by the proposed rule.

OTS: When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (RFA), requires the agency to publish an initial regulatory flexibility analysis unless the agency certifies that the rule will not have "a significant economic impact on a substantial number of small entities."[59] 5 U.S.C. 603, 605(b). OTS has reviewed the impact of the proposed regulations on small savings associations and certifies that that proposed regulations, if adopted as proposed, would not have a significant economic impact on a substantial number of small entities.

[59] Small Business Administration regulations define "small entities" to include savings associations with total assets of $165 million or less. 13 CFR 121.201.

The proposed rulemaking would implement sections 114 and 315 of the FACT Act and would apply to all savings associations (and federal savings association operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act),[60] 446 of which have assets of less than or equal to $165 million.

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

OTS believes that the proposed requirements implementing section 114 of the FACT Act would be consistent with savings associations' usual and customary business practices used to minimize losses due to fraud in connection with new and existing accounts. Savings associations also are likely to have implemented most of the proposed requirements as a result of having to comply with other existing regulations and guidance. For example, savings associations are already subject to CIP rules requiring them to verify the identity of a person opening a new account.[61] A covered entity may use the policies and procedures developed to comply with the CIP rules to satisfy the identity verification requirements in the proposed rules.

Savings associations complying with the "Interagency Guidelines Establishing Information Security Standards"[62] and guidance recently issued by the FFIEC titled "Authentication in an Internet Banking Environment"[63] already will have policies and procedures in place to detect attempted and actual intrusions into customer information systems. Savings associations complying with OTS's guidance on "Identity Theft and Pretext Calling"[64] already will have policies and procedures to verify the validity of change of address requests on existing accounts.

---

[60] For convenience, these entities are referred to as "savings associations."
[61] 31 CFR 103.121; 12 CFR 563.177 (savings associations).
[62] 12 CFR part 570, app. B (savings associations).
[63] OTS CEO Letter 228 (Oct. 12, 2005).
[64] "Identity Theft and Pretext Calling," OTS CEO Letter #139 (May 4, 2001).

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

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

The proposed regulations implementing section 315 would require users of consumer reports to have various policies and procedures to respond to the receipt of an address discrepancy. The FACT Act already requires CRAs to provide notices of address discrepancy to users of credit reports. OTS understands that as a matter of good business practice, most savings associations currently have policies and procedures in place to respond to these notices when they are provided in connection with both new and existing accounts, by furnishing an address for the consumer that the savings association has reasonably confirmed is accurate to the CRA from which it received the notice of address discrepancy. In addition, with respect to new accounts, a savings association already is required by the CIP rules to ensure that it knows the identity of a person opening a new account and to keep a record describing the resolution of any substantive discrepancy discovered during the verification process.

Given current practices of savings associations in responding to notices of address discrepancy from CRAs, and the existing requirements in the CIP rule, OTS believes that the

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

NCUA: The Regulatory Flexibility Act requires NCUA to prepare an analysis to describe any significant economic impact a regulation may have on a substantial number of small credit unions (primarily those under $10 million in assets). The NCUA certifies the proposed rule will not have a significant economic impact on a substantial number of small credit unions and therefore, a regulatory flexibility analysis is not required.

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 does not anticipate that the proposed regulations will have a significant economic impact on a substantial number of small entities. The Commission recognizes that the proposed regulations will affect a substantial number of small businesses. We do not expect, however, that the proposed requirements will have a significant economic impact on these small entities.

This document serves as notice to the Small Business Administration of the FTC's certification of no effect. To ensure the accuracy of this certification, however, the Commission requests comment on whether the proposed regulations will have a significant impact on a substantial number of small entities, including specific information on the number of entities that would be covered by the proposed regulations, the number of these companies that are "small

entities," and the average annual burden for each entity. Although the Commission certifies under the RFA that the regulations proposed in this notice would not, if promulgated, have a significant impact on a substantial number of small entities, the Commission has determined, nonetheless, that it is appropriate to publish an IRFA in order to inquire into the impact of the proposed regulations on small entities. Therefore, the Commission has prepared the following analysis:

1. Description of the Reasons That Action by the Agency Is Being Taken

The Federal Trade Commission 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) and1681c(h)(2)), which require the agency to issue these proposed regulations.

2. Statement of the Objectives of, and Legal Basis for, the Proposed Regulations

The objective of the proposed regulations is to establish guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. In addition, the proposed regulations require credit and debit card issuers to establish policies and procedures to assess the validity of a change of address request. They also set out requirements for 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. The legal basis for the proposed regulations is 15 U.S.C. §§ 1681m(e) and1681c(h)(2).

3. Small Entities to Which the Proposed Rule Will Apply

The proposed regulations apply to a wide variety of business categories under the Small Business Size Standards. Generally, the proposed 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 proposed rule, a very large number of small entities across almost every industry could be subject to the Rule. 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 million or who have fewer than 500 employees.[65]

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 proposed regulations implementing section 114 will affect over 3500 financial institutions and over 11 million creditors[66] 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), but requests comment on the number of small businesses that would be covered by the rule.

---

[65] These numbers represent the size standards for most retail and service industries ($6 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.

[66] 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/).

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. Indeed, the proposed 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 institutions and $6.5 million in sales for many creditors), but requests comment on the number of small businesses that would be covered by the rule.

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 proposed regulations implementing section 315 will affect approximately 1.6 million users of consumer reports subject to the FTC's jurisdiction[67] 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), but requests comment on the number of small businesses that would be covered by the rule.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The proposed requirements will involve some increased costs for affected parties. Most of these costs will be incurred by those required to draft identity theft Programs and annual reports.

---

[67] 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/).

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 proposed 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, but staff requests comment on the number of small businesses that would be affected. It is likely that 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), but the staff requests comment on the number of small businesses that would be covered by the rule. As discussed in the PRA section of this Notice, it is unlikely that such low-risk entities employ the measures to detect and address identity theft. Nevertheless, the proposed requirements are drafted in a flexible manner that allows 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 proposed regulations would require low-risk entities that

have no existing identity theft procedures to justify in writing their low-risk of identity theft, train staff to be attentive to future risks of identity theft, and prepare the annual report. The FTC staff believes that, for the affected low-risk entities, such activities will not be complex or resource-intensive tasks.

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. 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.

Section 315: The 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 proposed 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 this Notice, 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 proposed regulation that requires furnishing the correct address. As discussed in the PRA section of this Notice, 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 proposed regulations for implementing section 315. The FTC staff estimates that the costs associated with these impacts will not be significant.

The Commission does not expect that there will be any significant legal, professional, or training costs to comply with the Rule. Although it is not possible to estimate small businesses' compliance costs precisely, such costs are likely to be quite modest for most small entities. Nonetheless, because the Commission is concerned about the potential impact of the proposed Rule on small entities, it specifically invites comment on the costs of compliance for such parties. In particular, although the Commission does not expect that small entities will require legal assistance to meet the proposed Rule's requirements, the Commission requests comment on whether small entities believe that they will incur such costs and, if so, what they will be. In addition, the Commission requests comment on the costs, if any, of training relevant employees regarding the proposed requirements. The Commission invites comment and information on these issues.

5. Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has not identified any other federal statutes, rules, or policies that would duplicate, overlap, or conflict with the proposed Rule. The Commission invites comment and information on this issue.

6. Significant Alternatives to the Proposed Rule

The standards in the proposed Rule are flexible, and take into account a covered entity's size and sophistication, as well as the costs and benefits of alternative compliance methods. Nevertheless, the Commission seeks comment and information on the need, if any, for alternative

compliance methods that, consistent with the statutory requirements, would reduce the economic impact of the rule on such small entities, including the need, if any, to delay the rule's effective date to provide additional time for small business compliance.

If the comments filed in response to this notice identify small entities that are affected by the rule, as well as alternative methods of compliance that would reduce the economic impact of the rule on such entities, the Commission will consider the feasibility of such alternatives and determine whether they should be incorporated into the final rule.

C. OCC and OTS Executive Order 12866 Determination

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

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

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

review any comments and cost data provided carefully, and will revisit the cost aspects of the proposed rules in developing final rules.

D. OCC and OTS Executive Order 13132 Determination

The OCC and the OTS each has determined that this proposal does not have any federalism implications for purposes of Executive Order 13132.

E. NCUA Executive Order 13132 Determination

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

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

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

The OCC and OTS each believes that the financial institutions subject to their jurisdiction covered by the proposed rules already have identity theft prevention programs because it is a sound business practice. In addition, key elements of the proposed rules are elements in existing

regulations and guidance. Therefore, the OCC and OTS each has determined that this proposed rule will not result in expenditures by State, local, and tribal governments, or by the private sector, that exceed the expenditure threshold. Accordingly, neither the OCC nor OTS has prepared a budgetary impact statement or specifically addressed regulatory alternatives considered.

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

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

H. Community Bank Comment Request

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

IV. Solicitation of Comments on Use of Plain Language

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

- Have we organized the material to suit your needs? If not, how could this material be better organized?

- Are the requirements in the proposed guidelines and regulations clearly stated? If not, how could the guidelines and regulations be more clearly stated?

- Do the proposed guidelines and regulations contain language or jargon that is not clear? If so, which language requires clarification?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the guidelines and regulations easier to understand? If so, what changes to the format would make them easier to understand?
- What else could we do to make the guidelines and regulations easier to understand?

V. Communications by Outside Parties to FTC Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any FTC Commissioner or FTC Commissioner's advisor will be placed on the public record. See 16 C.F.R. 1.26(b)(5).

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

PART 41 – FAIR CREDIT REPORTING

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

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

Subpart A – General Provisions

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

§ 41.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

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

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

4. Add § 41.82 to read as follows:

§ 41.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as "users"), and that are national banks, Federal branches and agencies of foreign banks, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

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

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

(i) Can form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained;

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

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

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

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

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

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

(iv) Using other reasonable means.

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

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

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

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

Subpart J – Identity Theft Red Flags

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

(a) Purpose and scope. This section implements section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m, which amends section 615 of the Fair Credit Reporting

Act (FCRA). It applies to financial institutions and creditors that are national banks, Federal branches and agencies of foreign banks, and any of their operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

(1) Account means a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k). Account includes:

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

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

(2) The term board of directors includes:

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

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

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

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

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

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

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

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

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

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

(A) Appendix J;

(B) Applicable supervisory guidance;

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

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

(ii) Risk evaluation. In identifying which Red Flags are relevant, the financial institution or creditor must consider:

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

(B) The methods it provides to open these accounts;

(C) The methods it provides to access these accounts; and

(D) Its size, location, and customer base.

(2) Identity theft prevention and mitigation. The Program must include reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account, including policies and procedures to:

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

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

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

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

(A) Monitoring an account for evidence of identity theft;

(B) Contacting the customer;

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

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

(E) Not opening a new account;

(F) Closing an existing account;

(G) Notifying law enforcement and, for those that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

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

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

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

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

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

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

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

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

§ 41.91 Duties of card issuers regarding changes of address.

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

(b) Definitions. For purposes of this section:

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

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

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

(1) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

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

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

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

6. Add and reserve appendices B-I.

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

APPENDIX J TO PART 41 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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

Information from a Consumer Reporting Agency

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

2. A notice of address discrepancy is provided by a consumer reporting agency.

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, *such as*:

a. A recent and significant increase in the volume of inquiries.

b. An unusual number of recently established credit relationships.

c. A material change in the use of credit, especially with respect to recently established credit relationships.

d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification

4. Documents provided for identification appear to have been altered.

5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

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

Personal Information

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

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

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

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

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

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

a. The address on an application is fictitious, a mail drop, or prison.

b. The phone number is invalid, or is associated with a pager or answering service.

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

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

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

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

Address Changes

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

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

Anomalous Use of the Account

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

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

19. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, *for example:*

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

20. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

Notice from Customers or Others Regarding Customer Accounts

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

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

23. The financial institution or creditor is notified that the customer is not receiving account statements.

24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.

25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.

27. An employee has accessed or downloaded an unusually large number of customer account records.

28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.

29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.

30. There are unusually frequent and large check orders in connection with a customer's account.

31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

Board of Governors of the Federal Reserve System

12 CFR Chapter II

Authority and Issuance

For the reasons discussed in the joint preamble, the Board of Governors of the Federal Reserve System proposes to amend chapter II of title 12 of the Code of Federal Regulations by amending 12 CFR part 222 as follows:

PART 222 – FAIR CREDIT REPORTING (Regulation V)

1. The authority citation for part 222 is revised to read as follows:

Authority: 15 U.S.C. 1681b, 1681c, 1681m and 1681s; Secs. 3, 214, and 216, Pub. L. 108-159, 117 Stat. 1952.

2. Amend § 222.3 by revising the introductory text to read as follows:

Subpart A – General Provisions

* * * * *

§ 222.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

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

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

4. Add § 222.82 to read as follows:

§ 222.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as "users"), and that are 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) Definition. For purposes of this section, a notice of address discrepancy means a notice sent to a user of a consumer report by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

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

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

(i) Can form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained;

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

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

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

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

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

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

(iv) Using other reasonable means.

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

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

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

5. Add Subpart J to part 222 to read as follows:

Subpart J – Identity Theft Red Flags

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

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

(1) Account means a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k). Account includes:

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

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

(2) The term board of directors includes:

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

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

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

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

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

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

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

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

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

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

(A) Appendix J;

(B) Applicable supervisory guidance;

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

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

(ii) Risk evaluation. In identifying which Red Flags are relevant, the financial institution or creditor must consider:

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

(B) The methods it provides to open these accounts;

(C) The methods it provides to access these accounts; and

(D) Its size, location, and customer base.

(2) Identity theft prevention and mitigation. The Program must include reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account, including policies and procedures to:

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

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

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

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

(A) Monitoring an account for evidence of identity theft;

(B) Contacting the customer;

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

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

(E) Not opening a new account;

(F) Closing an existing account;

(G) Notifying law enforcement and, for those that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(H) Implementing any requirements regarding limitations on credit extensions under 15 U.S.C. 1681c-1(h), such as declining to issue an additional credit card when the financial

institution or creditor detects a fraud or active duty alert associated with the opening of an account, or an existing account; or

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

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

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

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

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

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

(B) Contents of report. The report must discuss material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of

accounts and with respect to existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes in the Program.

§ 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.

(b) Definitions. For purposes of this section:

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

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

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

(1) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

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

(3) Uses other means of assessing the validity of the change of address, in accordance with the policies and procedures the card issuer has established pursuant to section 222.90.

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

6. Add and reserve appendices B-I.

7. Add Appendix J to part 222 to read as follows:

APPENDIX J TO PART 222 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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

Information from a Consumer Reporting Agency

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

2. A notice of address discrepancy is provided by a consumer reporting agency.

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, *such as*:

a. A recent and significant increase in the volume of inquiries.

b. An unusual number of recently established credit relationships.

c. A material change in the use of credit, especially with respect to recently established credit relationships.

d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Documentary Identification

4. Documents provided for identification appear to have been altered.

5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

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

Personal Information

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

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

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

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

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

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

a. The address on an application is fictitious, a mail drop, or prison.

b. The phone number is invalid, or is associated with a pager or answering service.

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

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

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

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

Address Changes

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

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

Anomalous Use of the Account

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

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

19. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, *for example:*

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

20. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

Notice from Customers or Others Regarding Customer Accounts

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

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

23. The financial institution or creditor is notified that the customer is not receiving account statements.

24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.

25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.

27. An employee has accessed or downloaded an unusually large number of customer account records.

28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.

29. The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.

30. There are unusually frequent and large check orders in connection with a customer's account.

31. The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.

Federal Deposit Insurance Corporation

12 CFR Chapter III

Authority and Issuance

For the reasons set forth in the joint preamble, the Federal Deposit Insurance Corporation proposes to amend chapter III of title 12 of the Code of Federal Regulations by amending 12 CFR parts 334 and 364 as follows:

Part 334 – FAIR CREDIT REPORTING

1. The authority citation for part 334 is revised to read as follows:

Authority: 12 U.S.C. 1818 and 1819 (Tenth); 15 U.S.C. 1681b, 1681c, 1681m, 1681s, 1681w, 6801 and 6805.

Subpart A – General Provisions

2. Amend § 334.3 by revising the introductory text to read as follows:

334.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

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

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

4. Add § 334.82 to read as follows:

§ 334.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as "users"), and that are insured state nonmember banks, insured state licensed branches of foreign banks, or subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

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

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

(d) Consumer's address (1) Requirement to furnish consumer's address to a consumer reporting agency. A user must develop and implement reasonable policies and procedures for

furnishing an address for the consumer that the user has reasonably confirmed is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the user:

(i) Can form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained;

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

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

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

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

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

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

(iv) Using other reasonable means.

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

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

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

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

Subpart J – Identity Theft Red Flags

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

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

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

(1) Account means a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k). Account includes:

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

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

(2) The term board of directors includes:

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

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

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

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

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

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

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

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

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

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

(A) Appendix J;

(B) Applicable supervisory guidance;

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

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

(ii) Risk evaluation. In identifying which Red Flags are relevant, the financial institution or creditor must consider:

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

(B) The methods it provides to open these accounts;

(C) The methods it provides to access these accounts; and

(D) Its size, location, and customer base.

(2) Identity theft prevention and mitigation. The Program must include reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account, including policies and procedures to:

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

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

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

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

(A) Monitoring an account for evidence of identity theft;

(B) Contacting the customer;

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

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

(E) Not opening a new account;

(F) Closing an existing account;

(G) Notifying law enforcement and, for those that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

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

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

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

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

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

(ii) Oversight by board or senior management. The board of directors, an appropriate committee of the board, or senior management must oversee the development, implementation, and maintenance of the Program, including assigning specific responsibility for its

implementation, and reviewing annual reports prepared by staff regarding compliance by the financial institution or creditor with this section.

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

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

§ 334.91 Duties of card issuers regarding changes of address.

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

(b) Definitions. For purposes of this section:

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

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

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

reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

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

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

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

6. Add and reserve appendices B-I.

7. Add Appendix J to part 334 to read as follows:

APPENDIX J TO PART 334 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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

Information from a Consumer Reporting Agency

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

2. A notice of address discrepancy is provided by a consumer reporting agency.

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, *such as*:

a. A recent and significant increase in the volume of inquiries.

b. An unusual number of recently established credit relationships.

c. A material change in the use of credit, especially with respect to recently established credit relationships.