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

Documentary Identification

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

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

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

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

Personal Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Address Changes

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

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

Anomalous Use of the Account

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

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

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

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

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

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

c. A material change in purchasing or spending patterns;

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

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

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

Notice from Customers or Others Regarding Customer Accounts

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

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

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

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

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

Other Red Flags

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

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

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

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

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

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

Part 364 – STANDARDS FOR SAFETY AND SOUNDNESS

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

The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in sections 334.90, 334.91, and Appendix J of part 334.

Department of the Treasury

Office of Thrift Supervision

12 CFR Chapter V

Authority and Issuance

For the reasons discussed in the joint preamble, the Office of Thrift Supervision proposes to amend chapter V of title 12 of the Code of Federal Regulations by amending 12 CFR part 571 as follows:

PART 571 – FAIR CREDIT REPORTING

1. The authority citation for part 571 is revised to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, and 1881-1884; 15 U.S.C. 1681b, 1681c, 1681m, 1681s, and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

Subpart A – General Provisions

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

§ 571.1 Purpose and Scope.

* * * * *

(b) *Scope.*

* * * * *

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

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

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

571.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

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

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

5. Add § 571.82 to read as follows:

§ 571.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that receive notices of address discrepancies from credit reporting agencies (referred to as "users"), and that are either savings associations whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, federal savings association operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

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

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

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

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

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

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

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

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

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

(iv) Using other reasonable means.

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

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

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

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

Subpart J – Identity Theft Red Flags

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

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

Act (FCRA). It applies to financial institutions and creditors that are either savings associations whose deposits are insured by the Federal Deposit Insurance Corporation or, in accordance with § 559.3(h)(1) of this chapter, federal savings association operating subsidiaries that are not functionally regulated within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

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

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

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

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

(2) The term board of directors includes:

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

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

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

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

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

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

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

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

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

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

(A) Appendix J;

(B) Applicable supervisory guidance;

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) Contacting the customer;

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

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

(E) Not opening a new account;

(F) Closing an existing account;

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

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

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

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

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

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

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

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

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

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

§ 571.91 Duties of card issuers regarding changes of address.

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

(b) Definitions. For purposes of this section:

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

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

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

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

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

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

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

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

7. Add and reserve appendices B–I.

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

APPENDIX J TO PART 571 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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

Information from a Consumer Reporting Agency

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

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

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

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

b. An unusual number of recently established credit relationships.

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

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

Documentary Identification

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

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

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

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

Personal Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Address Changes

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

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

Anomalous Use of the Account

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

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

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

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

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

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

c. A material change in purchasing or spending patterns;

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

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

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

Notice from Customers or Others Regarding Customer Accounts

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

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

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

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

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

Other Red Flags

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

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

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

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

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

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

National Credit Union Administration

12 CFR part 717

Authority and Issuance

For the reasons discussed in the joint preamble, the National Credit Union Administration proposes to amend chapter VII of title 12 of the Code of Federal Regulations by amending 12 CFR part 717 as follows:

PART 717 – FAIR CREDIT REPORTING

1. The authority citation for part 717 is revised to read as follows:

Authority: 15 U.S.C. 1681a, 1681c, 1681m, 1681s, 1681w, 6801 and 6805.

Subpart A – General Provisions

2. Amend § 717.3 by revising the introductory text to read as follows:

§ 717.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

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 § 717.82 to read as follows:

§ 717.82 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 Federal credit unions.

(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 717 to read as follows:

Subpart J – Identity Theft Red Flags

717.90 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 Federal credit unions.

(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.

§ 717.91 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 717.90(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 717.90.

(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 717 to read as follows:

APPENDIX J TO PART 717 – 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 Trade Commission

16 CFR Part 681

For the reasons discussed in the joint preamble, the Commission proposes to add part 681 of title 16 of the Code of Federal Regulations as follows:

PART 681 – IDENTITY THEFT RULES

Sec.

681.1 Duties of users of consumer reports regarding address discrepancies.

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

681.3 Duties of card issuers regarding changes of address.

Appendix A to Part 681 Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Authority: Pub. L. 108-159, sec 114 and sec 315; 15 U.S.C. 1681m(e) and 15 U.S.C. 1681c(h).

§ 681.1 - Duties of users of consumer reports regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1) (referred to as "users").

(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.

§ 681.2 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 subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) Definitions. For purposes of this section, 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 A;

(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.

§ 681.3 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 681.2(a) that issues a debit or credit card.

(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 this section.

(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.

APPENDIX A TO PART 681 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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

Information from a Consumer Reporting Agency

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

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

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

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

   b. An unusual number of recently established credit relationships.

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

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

Documentary Identification

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

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

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

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

Personal Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Address Changes

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

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

Anomalous Use of the Account

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

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

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

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

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

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

c. A material change in purchasing or spending patterns;

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

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

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

Notice from Customers or Others Regarding Customer Accounts

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

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

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

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

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

Other Red Flags

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

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

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

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

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

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

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

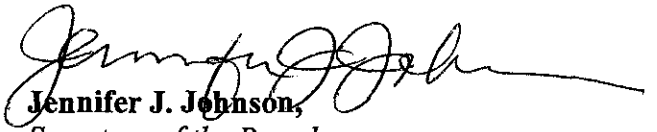
Dated: May 8, 2006.

John C. Dugan,
Comptroller of the Currency.

MHP

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

By Order of the Board of Governors of the Federal Reserve System, July 5, 2006.



Jennifer J. Johnson,
Secretary of the Board.

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

By order of the Board of Directors.

Dated at Washington, DC, the 9th day of May, 2006. Federal Deposit Insurance Corporation.

Robert E. Feldman
Executive Secretary

074296

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

Dated: April 10, 2006

By the Office of Thrift Supervision,

John M. Reich,
Director.

MHP 7-10-06

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

By the National Credit Union Administration Board on June 15, 2006.

Mary Rupp

Mary Rupp,
Secretary of the Board.

147 154

NHM
7-10-06

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

By direction of the Commission.

Donald S. Clark
Secretary

142 155

7-10-06