Red Flag Rule
Considerations in Developing an Identity Theft Prevention Program

In November 2007, the Federal Trade Commission (FTC) issued regulations (the Red Flags Rule) requiring financial institutions and creditors to develop and implement a written Identity Theft Prevention Program, as required by the Fair and Accurate Credit Transactions (FACT) Act of 2003.¹ Health centers that regularly extend, renew, or continue credit² to patients and that offer covered accounts³ (including billing accounts) are considered “creditors” and must comply with the rule.

The components of the Identity Theft Prevention Program include procedures for detecting, preventing and mitigating patterns, practices, or specific activities—known as “Red Flags” – that could indicate identity theft. The Identity Theft Program must be approved by the health center’s board of directors and be in place by May 1, 2009.

NACHC has prepared this Issue Brief to assist health centers develop and implement an Identity Theft Prevention Program (the “Program”). It is important to note that the Program should be appropriate to the size and complexity of the health center, the nature and scope of its activities, and the level of risk of identity theft from those activities. In other words, the scope and content of a health center’s Program should reflect the unique attributes of the particular health center.

Health centers should review NACHC’s February, 2009 Issue Brief, Complying with the FTC’s Red Flag Rules, for background on the Red Flags Rule and for information about which health centers must comply.⁴ The FTC Red Flags Rule, located at page 63771 of the Federal Register notice, is included in Exhibit A.⁵ Guidelines on how to develop a Program are included on pages 63773 through 63774.

How to Develop an Identity Theft Prevention Program Overview

As discussed below, health centers should complete the following steps to develop and implement a comprehensive and compliant Program:

Step 1: identify covered accounts

¹ The FTC defines “identity theft” as “a fraud committed or attempted using the identity of another person without authority.” 16 C.F.R. § 603.2(e).
² “Credit” is “the right granted… to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.” 15 U.S.C. § 1691a(d).
³ Covered account is any “account that a … creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions … and [a]ny other account that the … creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the … creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” 16 C.F.R. § 681.2(b)(3).
⁴ “Complying with the FTC’s Red Flag Rules” is available on-line at www.nachc.org/regulatory-issues.cfm.
⁵ The complete Red Flags Rule is available on-line by browsing the November 9, 2007 issue of the Federal Register at www.gpoaccess.gov/fr/index.html.
Step 2: identify Red Flags
Step 3: detect Red Flags
Step 4: prevent and mitigate identity theft
Step 5: update the program
Step 6: train relevant health center staff
Step 7: implement the Program

Developing a Program should not be a daunting task for a health center in part because the health center may incorporate provisions of its existing policies and procedures that are designed to protect patient identity, such as its Health Insurance Portability and Accountability Act (HIPAA) privacy and security programs. For example, HIPAA security policy addressing the confidentiality of patients’ electronic protected health information likely already contains procedures that mitigate the dangers of identity theft.

Step 1. Identify Covered Accounts

As an initial step, the health center must determine whether it has any “covered accounts.” Health centers should describe the types of covered accounts it offers and/or maintains in its Program.

An account is defined as a “continuing relationship established by a person … to obtain a product or service for personal, family [or] household … purposes.”

A covered account is defined as any “account that a … creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions … and [a]ny other account that the … creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the … creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.”

Requiring payment in full at the time of service (including full payment of insurance co-pays or discounted fees under a “sliding fee” scale) either in cash, with a credit card, or via a third party, such as Medicaid, Medicare or other third party payor, does not constitute the extending of credit. On the other hand, allowing patients to pay on a periodic basis—to defer full payments (with or without the imposition of any interest on carrying charges) —would be extending credit under the regulation and would be subject to the Red Flag Rule requirements if the health center regularly follows this practice. Deferment includes situations under which a patient is billed after the service is rendered.

The FTC takes the position that an account designed to permit multiple payments is also a covered account. For example, a billing account opened for a patient treated at the health center while on vacation would be considered a covered account if the billing

---

6 16 C.F.R. § 681.2(b)(1).
7 16 C.F.R. § 681.2(b)(3).
system would permit multiple payments, even though the patient paid in full for the services and there is no likelihood of a continuing relationship.

**Step 2. Identify Red Flags**

Next, a health center should analyze its covered accounts to identify potential Red Flags, and should list the Red Flags relevant to its operations in its Program.

The following factors should be considered in identifying Red Flags:

- **The types of covered accounts at the health center.** Health centers’ covered accounts will most likely be billing accounts that allow for deferred payment, as described above. However, a health center should examine its practices to determine if it offers or maintains other types of covered accounts.

- **The methods provided to open the health center’s covered accounts.** A health center should identify the Red Flags associated with its current processes for opening covered accounts. For example, health centers should examine what patient information is required to open a covered account, what steps are taken to verify that patient’s identity, and what gaps exist in the procedure that may undermine patient identity protection.

- **The methods available to access the health center’s covered accounts.** Health centers should consider both electronic access (e.g., network security measures, which are frequently addressed in HIPAA security policies to safeguard electronic protected health information) and non-electronic access (e.g., processes whereby health center staff require patients to verify their identity prior to disclosing personally identifiable information to them).

- **Any previous experience at the health center with identity theft.**

A Health center should also include relevant Red Flags from the categories below.\(^8\)

- **The documents associated with a covered account are suspicious.** Examples include, but are not limited to, the following:
  - The documents provided for the patient’s identification appear to have been altered or forged.
  - The patient’s photograph or physical description on their identification document (e.g., driver’s license) is inconsistent with the person presenting the document.
  - A patient has an insurance number but fails to provide an insurance card or other physical documentation of insurance (unless the health center can

---

\(^8\) A complete list of the example Red Flags is included in Exhibit A, 72 Fed. Reg. 63774, November 9, 2007.
confirm that there is a legitimate reason for the absence of such documentation).

- The patient’s signature appears forged, based on previous examples of the person’s signature on file.

- **The patient has presented suspicious personal identifying information.** Examples include, but are not limited to, the following:
  - Personal identifying information provided by the patient is inconsistent with other personal identifying information provided by the patient (e.g., there is a lack of correlation between the social security number range and the date of birth).
  - The social security number provided is the same as that submitted by another patient.
  - The insurance number provided is the same as that submitted by another patient.

- **There is unusual or suspicious activity related to a covered account.** Examples include, but are not limited to, the following:
  - Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient’s covered account.

- **Health center is notified by a patient, victim of identity theft, law enforcement official, or other persons that identity theft has, or will be, committed via the health center.**

- **Health center uses consumer reports as part of its billing and/or payment procedures and receives an alert, notification, or other warning from the consumer agency.** Examples include, but are not limited to, the following:
  - Report of fraud or other alert accompanying a credit or consumer report.
  - Notice of a credit freeze in response to a request for a consumer report.
  - Report from consumer reporting agency indicating an address discrepancy.
  - Consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient.

**Step 3. Detect Red Flags**

Once a health center has determined the Red Flags of identity theft that are pertinent to its operations, it must develop and describe procedures to detect these Red Flags. The examples of such procedures below are suggestions only. Other procedures may be more appropriate for a particular health center.

- **Covered Account.** Registration staff require that patients provide certain identifying information (e.g., name, date of birth, address, insurance card or
driver’s license) prior to creating a patient account that allows for deferred payment (i.e., creating a new covered account).

- **Access to Existing Accounts.** Registration staff, and other appropriate health center staff, take steps to monitor and protect patients’ existing covered accounts, in compliance with the health center’s HIPAA privacy policy, such as:
  
  o Verify the identification of a patient who presents at the health center for an appointment by requesting that the patient provide certain identification (such as a driver’s license, passport, or medical card). If the patient is unable to present such identification, registration staff request that the patient verify two types of identifying information (e.g., billing address, date of birth, etc.) without prompting from staff.
  
  o Verify the identification of a patient who requests patient-related information via the telephone by requiring that the patient verify two types of identifying information (e.g., billing address, date of birth, etc.) without prompting from staff.
  
  o Verify the validity of a change in address by requesting certain identifying information (e.g., lease forms, new driver’s license, etc.)
  
  o Verify changes in credit card or insurance information provided for the purposes of billing and payment by requesting certain identifying information (e.g., credit card, insurance card, etc.).

**Step 4. Prevent and Mitigate Identity Theft**

The health center should then describe how the health center will respond to Red Flags it identified. In determining appropriate responses, a health center should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a patient’s record.

Appropriate responses may include, but are not limited to, the following:

- Monitoring a covered account for evidence of identity theft
- Contacting the patient
- Changing any passwords, security codes, or other security devices that permit access to a covered account
- Reopening a covered account with a new account number
- Not opening a new covered account (e.g., when identification of new patient is in question)
- Closing an existing covered account
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement of possible instances of identity theft
Step 5. **Update the Program**

Given the frequent technology changes and evolving identity theft tactics, a health center must update its Program (including the list of Red Flags) periodically to reflect changes in identity theft risks to patients and to address the following factors:

- The health center’s experiences with identity theft
- Changes in the methods of identity theft
- Changes in the methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that the health center offers or maintains
- Changes in the health center’s business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements

Although the Red Flags Rule does not specify how frequently these updates should occur, it is advisable that they occur at least annually. Health centers should include a brief description of its periodic updates in its Program.

Step 6. **Train Relevant Health Center Staff**

A health center must train relevant staff, “as necessary,” to effectively implement the Program. Relevant staff may include compliance, intake, billing, medical records, and information technology staff, among others.

The training should address the Red Flags identified by the health center and should be appropriate to a health center’s individual circumstances. Relevant staff should also be trained regarding any Program updates.

Step 7. **Implement the Program**

The board of directors, an appropriate committee of the board, or a designated employee at the senior management level must be responsible for overseeing the Program. In order to satisfy this oversight requirement, the board should designate a Red Flag Compliance Officer charged with developing and monitoring the Program. This could be the health center’s Compliance Officer, although other employees familiar with the health center’s billing processes may be appropriate. The Red Flag Compliance Officer may wish to establish an Identity Theft Committee to assist in developing the Program. Participants may include the Chief Financial Officer and other applicable staff (i.e., compliance, billing, information technology, and other health center employees).

The designation of the Red Flag Compliance Officer should occur before May 1, 2009, and should be documented in the board’s meeting minutes.

The Red Flag Compliance Officer (or other designated individual(s)) should review the Program and provide a report of his/her findings to the board of directors at least...
annually. The report should examine the effectiveness of the Program in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts, significant incidents involving identity theft and management’s response, and service provider arrangements, as described below.

As part of identity theft oversight, the FTC also suggests considering identity theft risks that arise from contracts with organizations that perform services in connection with one or more covered accounts. For example, health centers may purchase billing services from an outside vendor. Health centers should take steps to ensure that the services provided by the contracting party are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a health center could include language in the contract requiring the contracting party to have policies and procedures to detect relevant Red Flags that may arise in the performance of its activities, and either report the Red Flags to the health center, or take appropriate steps to prevent or mitigate identity theft.

**Conclusion**

Following the above guidance on drafting an Identity Theft Prevention Program will assist health centers identify, mitigate, and respond to threats of patient identity theft, thereby satisfying the Red Flags Rule requirements.

The FTC expects to publish more detailed guidance on the Red Flag Rule, which may clarify the agency’s interpretation and requirements. The FTC has advised that specific questions about compliance may be addressed to RedFlags@ftc.gov.

For further information, contact Roger Schwartz at NACHC: (202) 296-0158 or rschwartz@nachc.com.
EXHIBIT A

FEDERAL TRADE COMMISSION

RED FLAG RULE

Federal Register / Vol. 72, No. 217 / Friday, November 9, 2007 / Rules and Regulations

with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address in accordance with the address confirmed by the consumer reporting agency that the user has previously confirmed is accurate to the consumer reporting agency as part of the information the user regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

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

(a) Scope. This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

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

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

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

(ii) A deposit account.

(2) The term board of directors includes:

(i) The board of directors of any other person that does not have a board of directors, a designated employee at the level of senior management.

(3) Covered account means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves the use or issuance of a card, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonable likelihood of consumer use or access, and that is processed by a financial institution or creditor or maintained by a nonfinancial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

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

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

(4) Train staff, as necessary, to effectively implement the Program and exercise appropriate and effective oversight of service provider arrangements.

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

§ 581.3 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in § 581.2(a) that issues a credit card that is subject to the requirements of this part.

(b) Definitions. For purposes of this section:

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

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

(c) Address validation requirements. A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address that requires 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 must receive a request for an additional or replacement card for the same account. Under these circumstances, the card issuer shall not issue an additional or replacement card, unless, in accordance with its reasonable policies and procedures, it reasonably verifies that the card is valid and that the card is not lost or stolen.

(3) Notification of the cardholder of the request:

(A) At the cardholder's former address;

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

(C) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and
(1) Provides to the cardholder a reasonable means of promptly reporting an incorrect address change; or
(2) Otherwise assesses the validity of the change of address to the cardholder, as appropriate, in accordance with the requirements under §631.2 of this part.
(3) Alternative address validation. A card issuer may satisfy the requirements of paragraphs (c)(1) through (c)(3) of this section in the event that it can establish to the satisfaction of the Federal Reserve or the appropriate Federal banking agency that it has taken reasonable steps to validate the address change under paragraph (c)(1) of this section upon the methods and procedures in paragraph (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.
(4) Affirmative written or electronic notice that the card issuer provides under this paragraph must be clear, conspicuous, and separate from the cardholder correspondence with the cardholder.

Appendix A to Part 601—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 601.2 of this part requires each financial institution and creditor that offers a covered account or a consumer report, to provide written notice to the consumer of identity theft, in accordance with the requirements of §601.2 of this part.

I. The Program

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

II. Identifying Relevant Red Flags

(a) Risk Factors. A financial institution or creditor should consider the following factors as relevant red flags for the purposes of the Program:

(1) The types of accounts offered or maintained;
(2) The methods or procedures to open its accounts or to maintain accounts;
(3) The methods or procedures to access and use accounts;
(4) The procedures for renewing accounts; and
(5) The policies and procedures for identifying and assessing red flags.

(b) Sources of Red Flags. Financial institutions and creditors should consider relevant red flags from sources such as:

(1) Consumer reports;
(2) Credit report inquiries;
(3) Underwriting results;
(4) Fraud reports;
(5) Identity theft reports;
(6) Criminal records; and
(7) Other information sources.

(c) Financial institutions or creditors that identify, in writing, a relevant red flag from one or more sources, shall consider it in determining that no response is warranted under the particular circumstances.

V. Updating the Program

(a) Financial institutions and creditors that use the Program should update the Program periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

(b) Changes include:

(1) Changes in the types of accounts the financial institution or creditor offers or maintains;
(2) Changes in the types of red flags the financial institution or creditor recognizes; and
(3) Changes in the processes and procedures of the financial institution or creditor from identity theft.

VI. Methods for Administering the Program

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

(1) Understanding and assessing the Program's implementation;
(2) Reviewing reports prepared by staff regarding compliance with the Program requirements; and
(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) Reports. Reports to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Identification of material changes to the Program as necessary to address changing identity theft risks.

(c) Contents of reports. The reports should address material matters relating to the Program and events that affect the effectiveness of the Program.

(d) Records. The Program's policies and procedures should address the safeguards necessary to protect the Program's records and other information used in implementing the Program.

(e) Oversight of service provider arrangements. The Program's policies and procedures should address the safeguards necessary to protect the Program's records and other information used in implementing the Program.

(f) Determining that no response is warranted under the particular circumstances.
that may arise in the performance of the service provider’s activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

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

(a) For financial institutions and creditors that are subject to 51 U.S.C. § 3811(h), filing a Suspicious Activity Report in accordance with applicable laws and regulations,
(b) Implementing any requirements under 15 U.S.C. § 1681d-2 regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active identity theft,
(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. § 1681d-2, for example, to correct or update inaccurate or incomplete information, and to report information that the furnisher has reasonable cause to believe is inaccurate, and
(d) Complying with the provisions of 15 U.S.C. § 1681m on the safe, timely, and secured transfer and placement for collection of certain debts remaining from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the source recommended in section II.B of the Creditors in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combinations, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Credit or Reporting Agency

1. A fraud or active identity theft is included in a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address dispute, as defined in § 609(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   (a) A recent and significant increase in the volume of inquiries; or
   (b) An unusual number of recently established credit relationships.
5. A material change in the use of credit, especially with respect to recently established credit relationships.
6. An account that was closed for cause or identified for advance notice of account privileges by a financial institution or creditor.

Suspicious Documents

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

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
   (a) The address does not match any address in the consumer report; or
   (b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
   (a) The address on an application is the same as the address provided on a fraudulent application; or
   (b) The phone number on an application is the same as the number provided on a fraudulent application.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
   (a) An account that was closed for cause or identified for advance notice of account privileges by the financial institution or creditor.
14. The SSN is provided in a manner that is inconsistent with a pattern of usage.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information on file with the financial institution or creditor.

Suspicious Activity

18. Financial institutions and creditors that are subject to regulating questions, that person opening the covered account or the customer cannot provide satisfactory information beyond that which generally would be available from a voice or consumer report.

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

19. Shortly following the notice of the change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a call from or for the addition of authorized users on the account.
20. A new revolving credit account is opened in a manner commonly associated with new patterns of theft patterns. For example:
   (a) The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronic equipment or jewelry); or
   (b) The customer fails to make the first payment on the account.
21. A current account is used in a manner that is not consistent with established patterns of activity on the account. For example:
   (a) Non-payment when there is a 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 debit card account;
   (e) A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for an unusually lengthy period of time is used with little or no notice; the account is opened in a manner commonly associated with a pattern of usage and other relevant factors. For example:
   (a) The account is open a long period of time without notice; or
   (b) The account is open in a manner commonly associated with a pattern of usage and other relevant factors.
23. Mail sent to the customer is returned undelivered as undeliverable although transactions continue to be conducted in accordance with the customer’s covered account.
24. The financial institution or creditor notifies the customer that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized access transactions in connection with a customer’s covered account.

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

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

John C. Dugan,
Comptroller of the Currency.

Jennifer J. Johnson,
Secretary of the Record.

Dated at Washington, D.C., this 5th day of October, 2007.
By order of the Board of Directors.
Federal Deposit Insurance Corporation.
Robert E. Feldman,
Interim Secretary.

By the Office of Thrift Supervision.
John M. Reich,
Director.

By order of the National Credit Union Administration Board, October 15, 2007.
Mary Kapp,
Secretary of the Board.

By direction of the Commission,
Donald C. Clark,
Secretary.

[FR Doc. 07–5453 Filed 11–8–07; 8:40 am]