1/28/2009

The National Association of Community Health Centers, Inc.®

Issue Brief
on

Complying with the FTC's Red Flag Rules

February, 2009

Prepared for NACHC by:

Michael Glomb
Feldesman Tucker Leifer Fidell, LLP
2001 L Street, N.W.
Second Floor
Washington, DC 20036
202.466.8960

For more information please contact:

Roger Schwartz, J.D.
Associate Vice President of Executive Branch Liaison
National Association of Community Health Centers
Tel. 202.296.0158
e-mail. rshcwartz@nachc.com

National Association of Community Health Centers
7200 Wisconsin Avenue • Suite 210 • Bethesda, MD 20814
Tel. 301.347.0400 • Fax. 301.347.0459

This publication was supported by Grant/Cooperative Agreement Number U3OCS00209 from the Health Resources Services Administration, Bureau of Primary Health Care (HRSA/BPHC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of HRSA/BPHC.

Complying With the "Red Flag" Rules

NACHC has prepared this Issue Brief to assist health centers in complying with the so-called "Red Flag" rules issued by the Federal Trade Commission (FTC).[1] The Red Flag rules require covered entities to implement certain measures to detect, prevent, and mitigate identity theft. Although the compliance date for the rules was November 1, 2008, the FTC has delayed its enforcement until May 1, 2009 to allow covered entities additional time to develop and implement policies and procedures, *i.e.*, a compliance program, in accordance with the rules. The program must be in writing and must be approved by the board of directors. Therefore, **health centers that determine that they are covered by the Red Flag rules should act promptly to meet the May 1, 2009 deadline.**

Background

The Fair and Accurate Credit Transactions Act of 2003 ("the Act"), which amended the Fair Credit Reporting Act, required the FTC (and federal banking industry regulatory agencies) to issue regulations regarding the detection, prevention, and mitigation of identity theft.[2] The regulations are designed to protect consumers by requiring, among other things, that businesses that extend credit and maintain covered accounts (as defined in the Red Flag rules) to customers develop a written program, approved by its board of directors, that identifies warning signs and suspicious activity (that is, "red flags") of possible identity theft.[3] The program must include measures to prevent identity theft and to mitigate damages from instances of identity theft, as well as provisions for staff training and periodic program updates, as needed.

It is likely that most health centers are covered by the Red Flag rules on account of the broad scope of "creditors" and "covered accounts" subject to the regulations. **However, whether an individual health center is covered by the Red Flag rules depends entirely on its specific billing and collection practices**. Accordingly, health centers are well advised to review the Red Flag rules to determine if they are covered and, if so, the actions necessary to comply with them.

Penalties and Enforcement

The FTC may impose civil money penalties (up to $2,500 per violation) where there is a pattern and practice of knowing violations of the rules.[4] In addition, state Attorneys General have

---

[1] The rules can be found at http://www.ftc.gov/os/fedreg/2007/november/0711090redflags.pdf. The FTC Red Flag rules are at page 63771 of the *Federal Register* notice.

[2] 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).

[3] Health centers should be aware of another provision of the Red Flag rules that requires users of a consumer report to develop reasonable policies and procedures to follow when they receive notice of an address discrepancy from a consumer reporting agency. This provision would be applicable to health centers that use consumer credit reports as part of their background checks on prospective employees or if they use credit reports in determining whether to extend credit to patients. *See* 16 C.F.R. § 681.1.

[4] While, the FTC does not have general jurisdiction over nonprofit organizations, such as health centers, the Fair Credit Reporting Act, under which the Red Flag rules were promulgated, authorizes the FTC to bring enforcement actions irrespective of any other jurisdictional tests. Moreover, in a June 2008 *FTC Business Alert*, the FTC stated: "where non-profit and government entities defer payment for goods or services, they too are to be considered creditors." *See* www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.pdf.

authority to enforce the rules and may recover damages of up to $1,000 for each willful or negligent violation, plus reasonable attorney fees. The Act does not authorize private individuals to bring an action to enforce the Red Flag rules. **However, a person harmed by identity theft may be able to bring an action against a health center under available state law**.

It is important to note that penalties under the Red Flag rules arise from violations of the guidelines (*e.g.*, failure to establish an identity theft prevention program consistent with the guidelines in the rules), not from individual instances of identity theft involving a patient or customer. In fact, identity theft may occur despite the implementation of a compliant identity theft prevention program.

Health centers should also be aware that it is unlikely that the FTC will initiate random compliance audits of health centers. Nevertheless, if there is an instance of identity theft or other event that results in a complaint to the FTC or the appropriate state agency, the health center will be at risk of an enforcement action and penalties if it does not have a compliant program.

A health center should consider the risks of an enforcement action in light of the fact that identity theft can cause substantial financial harm to the health center and patients, as well as severely damage the health center's reputation. Health centers, like all other health care providers, already are required under the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules to prevent unauthorized disclosure of protected health information. Preventing unauthorized access to and/or disclosure of patient information is critical to protect patients from identity theft, although strict adherence to HIPAA privacy and security measures alone is insufficient to comply with the Red Flag rules. Therefore, health centers would be well advised to implement identity theft protection measures as required by the Red Flag rules.

Covered Entities

The Red Flag rules apply to entities that regularly extend, renew, or continue *credit* and that offer or maintain *covered accounts*. These terms are defined in the regulations and are explained more fully below.

Extending Credit

The threshold question for a health center to determine if it must comply with the Red Flag rules is whether it extends credit. Credit is defined for purposes of the regulations as "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."[5] A health center that allows patients to pay on a periodic basis – to defer full payments (with or without the imposition of any interest or carrying charges) – is extending credit under the regulations and would be subject to the regulations.[6]

---

[5] 15 U.S.C. § 1691a(d).

[6] One must extend credit "regularly" in order to be a "creditor." 16 U.S.C. § 1691a(e). The term "regularly" is not defined in the regulations, but a reasonable conclusion may be drawn that deferring payment on an infrequent and intermittent basis would not be sufficient for a health center to be subject to the "Red Flag" rules.

Note that the FTC takes a very expansive view of what constitutes a deferral of payment. According to the FTC, a deferral of payment – and therefore the extension of credit – takes place any time a customer/patient leaves the premises without having paid in full for the goods/services provided. Thus, billing a patient for services **after the service is rendered** with the expectation that the patient will pay in full upon receipt of the bill is considered extending credit to the patient**.**

Conversely, requiring payment in full **at the time of service** (including 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 extension of credit. Note, however, that if the patient remains responsible for any part of the cost of the service provided (such as an insurance deductible or co-pay) that is not collected at the time of service, the transaction is considered to be a credit transaction.

Maintaining a Covered Account

Even if a health center is a creditor (as defined in the regulations), it is not covered by the Red Flag rules unless it maintains *covered accounts*.

The regulations define an *account* as a "continuing relationship established by a person ... to obtain a product or service for personal, family [or] household ... purposes."[7]

A *covered account* is defined as:

> An 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.[8]

Thus, a billing account maintained for a patient who has a continuing relationship with the health center almost certainly would be a covered account. However, the FTC takes the position that an account that is *designed to permit multiple payments* also is 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 system would permit multiple payments even though the patient paid in full for the services and there is no likelihood of a continuing relationship.

Moreover, given the definition of "account" in terms of a continuing relationship, patient medical records may well fall within the second prong of the definition of *covered accounts*, that is, records for which there is a reasonably foreseeable risk to patients or the health center from identity theft. In short, health centers would be well advised to assess the risk of identity theft with respect to all of its accounts, *i.e.*, patient relationships

[7] 16 C.F.R. § 681.2(b)(1).
[8] 16 C.F.R. § 681.2(b)(3).

Key Features of the Red Flag Rules

The Red Flag rules have many features typical of a compliance program. Importantly, the rules permit a health center to structure an identity theft protection program appropriate to the health center's activities and the complexity of the covered accounts it maintains. Moreover, a health center may incorporate provisions of its existing policies and procedures that are designed to protect patient identity, such as its HIPAA privacy and security programs. As with most compliance programs, the Red Flag rules have both substantive and procedural features. Nevertheless, it should not be difficult for a health center to implement a compliant identity theft protection program.

Developing an Identity Theft Prevention Program

The Red Flag rules require a health center to include certain elements in its identity theft prevention and detection program. However, the program should be appropriate to the size and complexity of the health center and the covered accounts that it maintains. The required elements, **which must be reflected in written policies and procedures, as applicable**, are as follows:

- **Assess Risk.** A health center must periodically determine whether it maintains covered accounts and, in particular, whether it offers or maintains accounts for which there is a reasonable foreseeable risk to the patients or to the health center of identity theft, taking into account the methods it provides to open or access accounts and any previous experiences with identity theft.

- **Identify Red Flags.** A health center must identify what signals of potential identity theft (*i.e.*, Red Flags) are relevant to its covered accounts and include them in its program. Specifically, the rules require covered entities to consider, and incorporate as appropriate, guidelines for an identity theft program that the FTC published as Appendix A to the Red Flag rules. (A copy of Appendix A is included with this Bulletin.)

  Appendix A provides that an identity theft program should include "Red Flags" from the following categories:

  - Alerts, notifications, or other warnings from consumer agencies or service providers. (Note that the Red Flag rules do not require a health center to seek a consumer credit report before extending credit to a patient, but it should include possible "Red Flags" provided by those agencies in its identity theft prevention program if it does so.)
  - Suspicious documents, *e.g.*, evidence of forgery or alteration; information that is not consistent with existing information on file.
  - Suspicious personnel identifying information, *e.g.*, photograph or physical description inconsistent with actual appearance; fictitious address; duplicate Social Security number.

- Unusual or suspicious activity in a covered account, *e.g.*, failure to make payments; late or missed payment with no prior history of nonpayment.
- Notice from patients, victims of identity theft, law enforcement officials, or other persons regarding possible identity theft.

- **Detect Red Flags.** Once a health center has identified Red Flags of possible identity theft that are relevant to its operations, it must develop written policies and procedures to detect instances of those Red Flags occurring in connection with the opening of new covered accounts and with existing covered accounts. This would include, for example, obtaining identifying information about and verifying the identity of patients for new accounts and authenticating patients, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

- **Respond Appropriately.** A health center must have written polices and procedures that provide for an appropriate response to Red Flags that are detected, commensurate with the degree of risk posed. In determining the appropriate response, the rules provide that a covered entity must consider "aggravating factors" that may increase the risk of identity theft, such as a data security breach that results in unauthorized access to a patient's account records or notice of fraudulent conduct on the part of a patient. The rule indicates that an appropriate response may include:

  - Monitoring a covered account for identity theft
  - Contacting the patient
  - Changing passwords or security codes that permit access to a covered account
  - Not opening a new covered account
  - Reopening a covered account with a new security account, or closing a covered account
  - Notifying law enforcement
  - Determining that no response is warranted under the circumstances

  Note that these are merely examples of appropriate responses. A health center could reasonably determine that other responses are appropriate. Further, appropriate responses to data breaches are likely to be included in a health center's HIPAA security and privacy polices and would not have to be developed for purposes of compliance with the Red Flag rules. **They should, however, be incorporated into the health center's identity theft prevention and detection program.**

- **Periodically Update Program.** A health center's identity theft prevention program must be updated periodically (including the identification of relevant Red Flags to reflect changes in risks to patients and to the health center from identity theft). A health center should take into account such factors as:

  - The health center's experience with identity theft
  - Changes in the methods of identity theft and in the methods to detect, prevent, and mitigate identity theft
  - Changes in the types of accounts that the health center maintains

- Changes in the business arrangements of the health center, including service provider arrangements

Administering an Identity Theft Prevention Program

While health centers have substantial flexibility in establishing an identity theft prevention program, the Red Flag rules impose certain administrative requirements that must be followed in order to have a compliant program. These requirements are as follows:

- **Board Approval.** A health center's initial identity theft program must be approved by its board of directors. (A health center may delegate approval to an appropriate board committee if its bylaws permit.)

- **Ongoing Oversight.** The program must provide for ongoing oversight of the operation of the program, including at least an annual report on compliance addressing the effectiveness of the health center's policies and procedures in addressing the risk of identity theft and recommendations for any material changes in the program. Under the Red Flag rules, the board may delegate its oversight responsibility to a committee of the board or to specifically designated members of the health center's senior management. In any case, the board should assign specific responsibility for the program's implementation, provide for review of compliance reports by the appropriate authority (board or designee), and assign authority for approving material modifications to the program that address changing identity theft risks.

- **Staff Training.** Staff must be trained, "as necessary," to effectively implement the program. Training should address risks of identity theft that the health center has identified and should be appropriate to the health center's individual circumstances.

- **Oversight of Service Providers.** The health center must exercise appropriate and effective oversight of vendors providing services in connection with a covered account, *e.g.*, billing and collection services, to ensure that the activity is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. This might include, for example, contract provisions requiring the service provider to follow the health center's Red Flag policies and procedures or to implement similar policies and procedures to detect relevant Red Flags and either report them to the health center or take appropriate steps to prevent or mitigate identity theft.

The FTC expects to publish more detailed guidance on the Red Flag rules, which may clarify the agency's interpretation of these and other issues. 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.

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

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 681.2 of this part.

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

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

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

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

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

II. Identifying Relevant Red Flags

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

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

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

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

(4) Its previous experiences with identity theft.

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

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

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

(3) Applicable supervisory guidance.

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

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

(2) The presentation of suspicious documents;

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

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

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

III. Detecting Red Flags

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

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

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

IV. Preventing and Mitigating Identity Theft

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

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

(b) Contacting the customer;

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

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

(e) Not opening a new covered account;

(f) Closing an existing covered account;

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

(h) Notifying law enforcement; or

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

V. Updating the Program

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

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

(b) Changes in methods of identity theft;

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

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

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

VI. Methods for Administering the Program

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

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

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and

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

(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.

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

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

that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

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

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

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

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

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

Supplement A to Appendix A

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

Alerts, Notifications or Warnings from a Consumer Reporting Agency

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

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

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.

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

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

b. An unusual number of recently established credit relationships;

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

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

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

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

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

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

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

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

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

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

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

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

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

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

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

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

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

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

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

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

c. A material change in purchasing or spending patterns;

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

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

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

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

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

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

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

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

Dated: October 5, 2007.

John C. Dugan,

Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System, October 29, 2007.

Jennifer J. Johnson,

Secretary of the Board.

Dated at Washington, DC, this 16th day of October, 2007.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

Dated: October 24, 2007.

By the Office of Thrift Supervision.

John M. Reich,

Director.

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

Mary Rupp,

Secretary of the Board.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 07–5453 Filed 11–8–07; 8:45 am]

BILLING CODE 4810–33–P; 6210–01–P; 6714–01–P; 6720–01–P; 7535–01–P; 6750–01–P