

September 4, 2008

TO: Managers, Administrators, Clerks, Attorneys, Finance Officers

FROM: Andrew L. Romanet, Jr., General Counsel  
John M. Phelps, II, Senior Assistant General Counsel

RE: Identity Theft Prevention Programs/Red Flag Rules

**Important Information on New Federal Requirements for Municipalities**

**IMMEDIATE ACTION NECESSARY**

This Memorandum explains new Federal Trade Commission (FTC) requirements concerning the adoption of identity theft prevention programs. Immediate action is required because programs must be in place by November 1, 2008.

The FTC rules apply to all municipalities that have utility accounts, even those that do not use computerized accounting systems. Why utility accounts? According to an article published in the July-August 2008 edition of *TVPPA News*, utilities are collectively number three on the list of favorite places for identity thieves to hunt for information. Utilities rank behind credit card companies and cell phone companies.

By November 1, you will need to have in place written procedures that help protect consumer identity and fight theft of customer account information. The procedures must identify, detect and respond to possible signals of identity theft known as Red Flags.

The *TVPPA News* points out that there may be significant consequences for noncompliance including civil penalties, damages, and attorneys' fees. It also reports that the FTC is likely to demand copies of Programs from randomly selected utilities immediately after the November 1 deadline.

The League has investigated possible sources to help you develop, implement and oversee identity theft prevention programs. We have found a product that is both educational and practical, and believe it to be affordable and readily available. Information on how to obtain the product is found below.

## **Background**

Identity theft is a serious problem in the United States today. To combat the problem, as part of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act), the FTC and several other federal agencies have issued rules requiring creditors (including municipalities under certain circumstances) to develop, adopt and implement written Identity Theft Prevention Programs (“Programs”). The Programs must be in place by November 1, 2008. The rules are often referred to the “Red Flag” requirements and also apply to financial institutions. In addition, the provisions place certain duties relating to address discrepancies upon the users of consumer reports. The address discrepancy rules may also apply to your municipality.

The FTC requirements associated with the adoption of the Programs and the address discrepancy provisions for users of consumer reports may be found in the Federal Register at 72 Fed. Reg. 63771 (codified at 16 C.F.R. Part 681). A copy of the pages of the Federal Register containing Part 681 is attached to this memorandum and cited herein as the “Rules.” The full rules may be found at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

## **Municipalities as Creditors**

The new Rules apply to all municipal utility and other operations that provide a service for which payment is deferred until a future date. For example, when water, sewer or electricity is provided by a city and then paid for by the consumer at the end of a billing cycle, the city has extended credit for the purpose of the Rules. The definition of “creditor” in the Rules specifically includes “utility companies” and a “covered account” (those accounts to which the Rules apply) is defined to include 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, such as a . . . utility account.” Note that “covered accounts” also include “any 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.”

## **Red Flags**

The central objective in the development of a Program is the identification, detection and response to “Red Flags.” Under the Rules, Red Flags “means a pattern, practice or specific activity that indicates the possible existence of identity theft.” In other words, Red Flags are warnings of identity theft. The Rules set out examples of Red Flags. Examples include such events as the receipt of warnings from consumer reporting agencies, the presentation to a creditor of suspicious documents, the presentation to a creditor of suspicious personal identifying information, and the unusual use of a covered account. Please note Supplement A to Appendix A found on the last page of the excerpts from the Federal Register attached that lists 26 illustrative examples of Red Flags.

## **Establishment of a Program**

16 C.F.R. Part 681 (attached) provides that each creditor that offers or maintains covered accounts must develop and implement a written Program “that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.” It is important to note that the Program must be appropriate to the size and

complexity of the creditor and the nature and scope of its activities. Therefore, it is crucial in the Program establishment process for each municipality to individually and methodically follow the steps set out in the Rules as it develops and adopts a Program. Each municipality, for example, should review its covered accounts and how those accounts are opened and accessed, evaluate its previous experiences with identity theft, and tailor its policies to prevent and mitigate identity theft accordingly.

Introductory portions of the Rules, (not included with this memorandum) summarize the elements of a Program as follows:

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

Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;

Detect Red Flags that have been incorporated into the Program;

Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and,

Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the . . . creditor from identity theft.

72 Fed. Reg. 63720.

### **Program Administration**

The initial written Programs must be approved by the governing body of the creditor (municipality) or an appropriate committee of that body, if applicable. Thereafter the governing body, or an appropriate committee of the body, or a designated employee at the level of senior management must be involved in the oversight, implementation and administration of a Program. Training must be provided to the staff so as to effectively implement the Program, and appropriate and effective oversight must be exercised with regard to service provider arrangements.

### **Address Discrepancies**

The FACT Act requires several federal agencies (including the FTC) to issue rules to provide guidance to a user of a consumer report when the user receives a notice of address discrepancy from a consumer reporting agency. The rules regarding address discrepancies apply to a municipality if it is a user of a consumer report. For example, the Rules would apply to your municipality if you request a report from a consumer reporting agency and that agency finds a substantial difference between the address you provided to the agency and the address the agency has in the consumer’s file. The agency would then provide a “notice of address discrepancy” to you reporting the inconsistency between the two addresses.

The guidelines are to describe reasonable policies and procedures that a user of a consumer report should employ (if it receives a notice of address discrepancy) to determine if it knows the identity of the consumer for whom the report applies, and reconcile the address of the consumer with the credit reporting agency if the user has a continuing relationship with the consumer and in the regular course of business furnishes information to the agency. 72 Fed. Reg. 63735.

16 C.F.R. § 681.1 (attached) provides the guidelines required by the FACT Act regarding duties of users regarding address discrepancies.

### **Additional Information and Support**

This memorandum is designed to alert our membership to the Red Flag requirements and to provide basic information about them. As mentioned above, the FTC has mandated that Identity Theft Prevention Programs be tailored to each municipality based on its size and complexity and the nature and scope of its activities. Further, the process of developing the Program is a significant part of meeting the FTC requirements. Recognizing that a “one size fits all” solution will not satisfy the Rules, the League investigated the existence of educational tools that would be beneficial from the “hands-on” perspective. We believe that we have found such a tool. It is the same set of materials identified by Electricities in its recent memo on the FACT Act.

The Tennessee Valley Public Power Association (“TVPPA”) has conducted several workshops and created associated materials that assist utilities in the development of Identity Theft Prevention Programs. The TVPPA has modified the materials for a non-classroom environment and will sell them to individual municipalities for \$350.00. The materials consist of a notebook (topics include: needs assessments, case studies, policy and procedure development, and program checklist), a compact disc, and a user manual. We understand that either a conference call or Webinar may be available to further explain the materials. If you would like to purchase the materials, you may contact Danette Scudder at [dscudder@tvppa.com](mailto:dscudder@tvppa.com) or by phone at 423-648-2464. Please be sure to include your name, municipality, and billing and other contact information. We understand that TVPPA accepts credit cards.

Additional information may also be obtained through the website of the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov) or you may contact [RedFlags@ftc.gov](mailto:RedFlags@ftc.gov).



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

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

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

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

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

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

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

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

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

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the federal credit union.

18. For federal credit unions that use challenge questions, the person opening the covered account or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

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

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

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

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

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

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

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

c. A material change in purchasing or spending patterns;

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

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

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

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

24. The federal credit union is notified that the member is not receiving paper account statements.

25. The federal credit union is notified of unauthorized charges or transactions in connection with a member's covered account.

#### *Notice From Members, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Federal Credit Union*

26. The federal credit union is notified by a member, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

### FEDERAL TRADE COMMISSION

16 CFR Part 681

#### Authority and Issuance

■ For the reasons discussed in the joint preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

#### PART 681—IDENTITY THEFT RULES

Sec.

681.1 Duties of users of consumer reports regarding address discrepancies.

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

681.3 Duties of card issuers regarding changes of address.

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

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

#### § 681.1 Duties of users regarding address discrepancies.

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

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

report and the address(es) in the agency's file for the consumer.

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

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

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

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

(C) Obtains from third-party sources; or

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

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

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

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

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

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

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

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

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

(iv) Using other reasonable means.

(3) *Timing.* The policies and procedures developed in accordance

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

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

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

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

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

- (i) An extension of credit, such as the purchase of property or services involving a deferred payment; and
- (ii) A deposit account.

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

- (i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and
- (ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

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

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

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

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

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

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

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

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

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

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

- (1) The methods it provides to open its accounts;
- (2) The methods it provides to access its accounts; and
- (3) Its previous experiences with identity theft.

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

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

- (i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
- (ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
- (iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and
- (iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor

that is required to implement a Program must provide for the continued administration of the Program and must:

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

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

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

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

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

**§ 681.3 Duties of card issuers regarding changes of address.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

##### I. The Program

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

##### II. Identifying Relevant Red Flags

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

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

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

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

(3) Applicable supervisory guidance.

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

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

(2) The presentation of suspicious documents;

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

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

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

##### III. Detecting Red Flags

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

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

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

##### IV. Preventing and Mitigating Identity Theft

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

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or

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

##### V. Updating the Program

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

- (a) The experiences of the financial institution or creditor with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

##### VI. Methods for Administering the Program

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

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

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

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

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

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

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

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

#### VII. Other Applicable Legal Requirements

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

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

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

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

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

#### *Supplement A to Appendix A*

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

#### *Alerts, Notifications or Warnings from a Consumer Reporting Agency*

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - a. A recent and significant increase in the volume of inquiries;
  - b. An unusual number of recently established credit relationships;
  - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
  - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

#### *Suspicious Documents*

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

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

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

#### *Suspicious Personal Identifying Information*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for

a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

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

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

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

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

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

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

c. A material change in purchasing or spending patterns;

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

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

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

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

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

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

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

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

Dated: October 5, 2007.

**John C. Dugan,**  
*Comptroller of the Currency.*

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

**Jennifer J. Johnson,**  
*Secretary of the Board.*

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

By order of the Board of Directors,  
Federal Deposit Insurance Corporation.

**Robert E. Feldman,**  
*Executive Secretary.*

Dated: October 24, 2007.