

INFORMATION MUNICIPAL CLERKS NEED TO KNOW ABOUT IDENTITY THEFT: RED FLAG REGULATIONS AND GUIDELINES

By Dan Bolin

Ancel, Glink, Diamond, Bush, DiCianni & Krafthefer, P.C.

The Fair and Accurate Credit Transactions Act of 2008 (FACT Act) creates some new obligations for municipalities related to identity theft. 15 U.S.C. 1681 *et seq.* Specifically, those municipalities providing a service involving a deferred payment must adopt an Identity Theft Prevention Program by November 1, 2008. This includes accounts for utility services. 16 C.F.R. 681 *et seq.* This memo summarizes your obligations under this new law.

Introduction to the FACT Act

The FACT Act requires Federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission to establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and to prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines. Final rules implementing these “Red Flag Regulations and Guidelines” were published in November 2007.¹

The FACT Act seeks to prevent identity theft by requiring creditors to identify and respond to “Red Flags” in covered accounts. A creditor includes any person who regularly extends, renews, or continues credit. A person is defined to include government entities. A Red Flag is pattern, practice, or specific activity that indicates the possible existence of identity theft. An account includes the provision of a service by a creditor for personal, family, household or business purposes, with a deferred payment. A covered account includes cell phone accounts, utility accounts or any other account where there is a reasonably foreseeable risk of identity theft.

1. Overview of Red Flag Regulations. A creditor is required to periodically ascertain whether they have covered accounts. In doing so, the creditor must consider the methods it provides to open or access their accounts and any previous experiences with identity theft. By November 1, 2008, any creditor that has a covered account must establish a written Identity Theft Prevention Program, designed to detect, prevent, and mitigate identity theft. The requirements for a satisfactory program are intended to be flexible and appropriate to the size and complexity of the creditor and the nature and scope of its activities.

The Program must identify Red Flags for the covered accounts maintained by the creditor. Once identified, policies and procedures must be developed to respond to Red Flags as they are detected. The Program must be updated periodically, in response to changing risks for identity theft. The creditor’s board of directors must approve the initial program and remain involved in its oversight, development, implementation and administration. Staff must be trained in the program and there must be effective oversight of other people providing services to the creditor.

¹ Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718-01 (Nov. 9, 2007)

2. Overview of Red Flag Guidelines. Program guidelines and examples of Red Flags are included in the administrative rules. The guidelines specifically note that existing policies, procedures, and other arrangements that control reasonably foreseeable risks of identity theft may be included in the Program. In order to identify Red Flags, it is necessary to consider past incidents and future risks of identity theft. Red Flags may be classified in the following possible categories:

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

The presentation of suspicious documents;

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

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

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. Possible Red Flags to be included in a Program are available are listed below.

In order to detect Red Flags, the guidelines suggest obtaining identifying information about, and verifying the identity of, a person opening a covered account. Additionally, creditors should be authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts. The guidelines also offer possible responses to the detection of a Red Flag or an incident of identity theft, including:

monitoring a covered account for evidence of identity theft;

contacting the customer;

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;

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; or

determining that no response is warranted under the particular circumstances.

The Program should be updated periodically, considering factors such as:

the experiences of the financial institution or creditor with identity theft;

changes in methods of identity theft;

changes in methods to detect, prevent, and mitigate identity theft;

changes in the types of accounts that the financial institution or creditor offers or maintains; and

changes in the business arrangements of the creditor.

In administering the Program, the board of directors should specifically designate responsibility for the implementation of the program and adopt any material changes that become necessary. Staff should also prepare an annual report for the board of directors, reviewing the Program's compliance with the federal regulations.

3. Conclusion. In conclusion, when a local government does business as a "creditor," it must take the necessary steps to determine whether it has any "covered accounts." A government entity with covered accounts must develop a written Identity Theft Prevention Program, as described in the implementing regulations to the FACT Act. The following is an illustrative, non-exclusive list of Red Flags published as examples in the administrative rules pursuant to the Fair and Accurate Credit Transactions Act of 2003. They are classified by the five categories of Red Flags described in the guidelines.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

- A. A fraud or active duty alert is included with a consumer report.
- B. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- C. A consumer reporting agency provides a notice of address discrepancy, as defined in 16 C.F.R. 681.1(b).
- D. 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 recent and significant increase in the volume of inquiries;
An unusual number of recently established credit relationships;
A material change in the use of credit, especially with respect to recently established credit relationships; or
An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- E. Documents provided for identification appear to have been altered or forged.
- F. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- G. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- H. 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.
- I. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

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

The address does not match any address in the consumer report; or
The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

- K. 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.
- L. 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:

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

- M. 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:

The address on an application is fictitious, a mail drop, or a prison; or
The phone number is invalid, or is associated with a pager or answering service.

- N. The SSN provided is the same as that submitted by other persons opening an account or other customers.
- O. 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.
- P. 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.
- Q. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- R. 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

- S. 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.

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

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

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

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

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

A material increase in the use of available credit;

A material change in purchasing or spending patterns;

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

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

- V. 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).

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

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

- Y. 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

- Z. 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.