

FINANCE MEMORANDUM
#10-19

DATE: July 8, 2010

TO: Honorable Mayor Joyce Downing and City Council Members

FROM: Bill Simmons, City Manager *WAS*
Shawn Cordsen, Finance Director *SC*

SUBJECT: CR-107 – Red Flag Rules

BACKGROUND:

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations, known as red flag rules, which require financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) act of 2003. Under the Rules, a financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer. Transaction accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

Under the Red Flags Rules, the City must develop a written program that identifies and detects the relevant warning signs – or “red flags” – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The Red Flags Rules provide the City with the opportunity to design and implement a program that is appropriate for its size and complexity, as well as the nature of ongoing operations.

UPDATE:

In conjunction with the City Attorney, staff has drafted the attached proposed policy document and approving resolution. In many cases, city staff has already put in place many of the activities outlined in the policy document, thus it would entail very few procedural changes should Council choose to approve the resolution and policy. The policy document will also serve as a future reference and training tool for employees and provide clear direction to those staff members involved in the maintenance and administration of customer transaction accounts.

STAFF REFERENCE:

If Councilmembers have any comments or questions, you may contact Shawn Cordsen at scordsen@northglenn.org or at 303-450-8719.

SPONSORED BY: MAYOR DOWNING

COUNCILMAN'S RESOLUTION

RESOLUTION NO.

No. CR-107
Series of 2010

Series of 2010

A RESOLUTION COMPLYING WITH THE FEDERAL TRADE COMMISSION'S RED FLAG RULES, AND ADOPTING THE CITY'S IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, as part of the Fair Accurate Credit Transactions Act of 2003, the Federal Trade Commission ("FTC") issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs by July 1, 2010 ("Red Flag Rules"); and

WHEREAS, the City of Northglenn (the "City") is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears; and

WHEREAS, covered accounts offered to customers for the provision of City services include utility accounts and development review accounts; and

WHEREAS, the process of opening a new covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur; and

WHEREAS, to comply with the FTC's Red Flag Rules, the City desires to create and adopt an appropriate identity theft prevention policy.

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF NORTHGLENN, COLORADO, THAT:

Section 1. The City Council hereby adopts the City of Northglenn Identity Theft Prevention Program, effective July 1, 2010, attached hereto as **Exhibit A** and incorporated herein by reference.

DATED at Northglenn, Colorado, this ____ day of _____, 2010.

JOYCE DOWNING
Mayor

ATTEST:

JOHANNA SMALL, CMC
City Clerk

APPROVED AS TO FORM:

COREY Y. HOFFMANN
City Attorney

City of Northglenn CO
Identity Theft Prevention Program

Effective beginning July 1, 2010

I. PROGRAM ADOPTION

The City of Northglenn Colorado (“the City”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission's Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C.F.R. § 681.1.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Rule

Under the Rule, every financial institution and creditor is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. 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.

B. Definitions used in the Program

The Rule defines “Identity Theft” as “fraud committed using the identifying information of another person” and a “Red Flag” as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

The Rule defines creditors “to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. *Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.*” [Emphasis added.]

The Rule applies to creditors only in regard to “covered accounts.” Under the Rule an “account” means continuing relationship established by a person with the City 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. Under the Rule, a “covered account” is:

1. Any account the City offers or maintains primarily for personal, family or household purposes of the person for whom the account is being offered or maintained, that involves or is designed to permit multiple payments or transactions; and

2. Any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from Identity Theft, including financial, operational, compliance, reputation or litigation risks.

Identifying information is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, a computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City will consider the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The City identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

- 1) Report of fraud accompanying a credit report;
- 2) Notice or report from a credit agency of a credit freeze on a customer or applicant;
- 3) Notice or report from a credit agency of an active duty alert for an applicant; and
- 4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is suggestive of fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the City that a customer is not receiving mail sent by the City;
6. Notice to the City that an account has unauthorized activity;
7. Breach in the City's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the City from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, City personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;

8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for City purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from identity theft. At least every year, the Program Administrator will consider the City's experiences with identity theft situation, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the Governmental Operations Committee of the City Board of Commissioners with his or her recommended changes and the Committee will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for implementing and recommending updates to this Program lies with the City Risk Manager, who is designated as the Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of City staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of

prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

City staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of identity theft prevention programs, the Rule envisions a degree of confidentiality regarding the City's specific practices relating to identity theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Program Administrator and those employees who need to know them for purposes of preventing identity theft. Because this Program is to be adopted by a public body and thus be publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices are listed in this document.