City of Caro
Identity Theft Prevention Policy

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account and to provide for continued administration of the Program in compliance with the Federal Trade Commission's Red Flags Rule (Part 681 of Title 16 of the Code of Federal Regulations) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Under the Red Flag 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 in to 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.

Definitions

Identifying information means any name or number that may be used, along 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, computer's Internet Protocol address, or routing code.

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A *covered account* means:

1. 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. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and
2. 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.

Adopted by Council: 10-20-08

Policy #08-019

A *red flag* means a pattern, practice or specific activity that indicates the possible existence of identify theft.

Policy

A. IDENTIFICATION OF RED FLAGS. The City identifies the following red flags, in each of the listed categories:

1. Suspicious Documents

i. Identification document or card that appears to be forged, altered or inauthentic;
ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
iii. Other document with information that is not consistent with existing customer; and
iv. Application for service that appears to have been altered or forged.

2. Suspicious Personal Identifying Information

i. Identifying information presented that is inconsistent with other information the customer provides;
ii. Identifying information presented that is inconsistent with other sources of information;
iii. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
iv. Identifying information presented that is consistent with fraudulent activity;
v. An address or phone number presented that is the same as that of another person;
vi. 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
vii. A person's identifying information is not consistent with the information that is on file for the customer.

3. Suspicious Account Activity or Unusual Use of Account

i. Change of address for an account followed by a request to change the account holder's name;
ii. Payments stop on an otherwise consistently up-to-date account;
iii. Mail sent to the account holder is repeatedly returned as undeliverable;

Adopted by Council: 10-20-08

Policy #08-019

iv. Notice to the City that a customer is not receiving mail sent by the City;
v. Notice to the City that an account has unauthorized activity;
vi. Breach in the City's computer system security; and
vii. Unauthorized access to or use of customer account information.

4. Alerts from Others
i. 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.

B. DETECTING RED FLAGS.

1. 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:
i. Require certain identifying information such as name, residential or business address, Homestead Exemption Affidavit or other identification;
ii. Verify the customer's identity (for instance, review a driver's license or other identification card);
iii. Review documentation showing the existence of a business entity; and/or
iv. Independently contact the customer.

2. 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:
i. Verify the validity of requests to change billing addresses; and
ii. Verify changes in banking information given for billing and payment purposes.

C. 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:

1. Prevent and Mitigate
i. Continue to monitor an account for evidence of Identity Theft;
ii. Contact the customer;
iii. Change any passwords or other security devices that permit access to accounts;
iv. Not open a new account;
v. Close an existing account;

vi. Reopen an account with a new number;
vii. Notify the City Treasurer for determination of the appropriate step(s) to take;
viii. Notify law enforcement; and/or
ix. Determine that no response is warranted under the particular circumstances.

2. **Protect customer identifying information**
   i. 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:
   ii. Ensure that its website is secure or provide clear notice that the website is not secure;
   iii. Ensure complete and secure destruction of paper documents and computer files containing customer information;
   iv. Ensure that office computers are password protected;
   v. Keep offices clear of papers containing customer information;
   vi. Ensure computer virus protection is up to date; and
   vii. Require and keep only the kinds of customer information that are necessary for utility purposes.

D. PROGRAM UPDATES. This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from Identify Theft. The City Treasurer 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 City Treasurer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the City Treasurer will present the City Council with his/her recommended changes and the Council will make a determination of whether to accept, modify or reject those changes to the Program.

E. PROGRAM ADMINISTRATION.

1. **Oversight.** Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the City. The Committee is headed by the City Treasurer, with the Manager and Deputy Treasurer comprising the remainder of the committee membership. The City Treasurer 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.

Adopted by Council: 10-20-08

Policy #08-019

2. **Staff Training and Reports.** City staff responsible for implementing the Program shall be trained either by or under the direction of the City Treasurer in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. City staff is required to provide reports to the Program Administrator on incidents of Identity Theft, the City's compliance with the Program and the effectiveness of the Program.

3. **Specific Program Elements and Confidentiality.** For the effectiveness of Identity Theft prevention Programs, the Red Flag 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 are to be limited to the Identity Theft Committee 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 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.

Authority & Revisions

This policy is enacted immediately upon approval of the City Council, as reflected in the regular meeting minutes dated October 20, 2008. Revisions to this policy shall only be enacted when approved by the City Council and reflected in the applicable meeting minutes. This policy shall be reviewed at least annually by the City Treasurer and updated as appropriate.

Adopted by Council: 10-20-08

Policy #08-019