City of Seaside

Identity Theft Prevention Program

Amended July 2, 2015

I. PROGRAM ADOPTION

The City of Seaside ("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 ("FACTA"). 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the City Council. After consideration of the size and complexity of the City's operations and account systems, and the nature and scope of the City's activities, the City Council determined that this Program was appropriate for the City of Seaside, and therefore approved this Program on March 19, 2009.

On July 2, 2015, the Program was amended by the City Council to incorporate the Red Flag Program Clarification Act of 2010 ("Clarification Act") and 16 C. F. R. § 682.3 of FACTA.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags and Disposal Rules

Red Flags Rule

Under the Red Flags 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.

Disposal Rule

Under the Disposal Rule, any government agency who maintains or otherwise possesses Consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

B. Definitions used in this Program

The Red Flags 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."

According to the Clarification Act, the City is a Creditor subject to the Rule requirements. 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."

Under the Rule, a "covered account" is:

1) Any account the City offers or maintains that involves or is designated 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, employees, or citizens or to the safety and soundness of the City from Identity Theft. This term is further defined in Section C below.

"Identifying information" is defined under the Rule 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, computer's Internet Protocol address, or routing code.

"Consumer information" is defined as "any record about an individual, whether in paper, electronic, or other form, that is a Consumer report or is derived from a Consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data."

Under the Disposal Rule, the term ''dispose,'' ''disposing,'' or ''disposal'' means:

1) The discarding or abandonment of Consumer information; or
2) The sale, donation, or transfer of any medium, including computer equipment, upon which Consumer information is stored.

C. Covered Accounts

The City is a Creditor for the purposes of FACTA and has determined that it maintains the following Covered Accounts:

1) Utility Accounts
2) Employee Housing Loans
3) Community Development Block Grant Housing Loans
4) Housing Successor (formerly Redevelopment Agency) Housing Loans
5) Miscellaneous Accounts Receivables

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the City considers 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;
4) Notice or report from a credit agency of an address discrepancy; and
5) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity, such as
    a) a recent significant increase in the number 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;
    d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or Creditor.

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);
4) Application for service that appears to have been altered or forged or gives the appearance of having been destroyed and reassembled;
5) Other information on the identification document that is not consist with information provided by the person opening a new account; and
6) Other information on the identification document that is not consistent with readily accessible information that is on file with the City.

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 consistent with 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 or nonpayment when there is no history of late or missed payments);
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 (example: presentation of a business card, business letterhead, or business license); and
4) Independently contact the affected customer if appropriate.

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 affected customer of suspected Identity Theft;
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) Ask the customer to appear in person with government issued identification;
9) Require a deposit to be paid before providing service;
10) Do not provide account information to anyone other than the account holder(s), or other individual authorized by the account holder(s);
11) Update all account information;
12) Deactivate payment method registered for automatic payments;
13) Connect or disconnect service;
14) Notify law enforcement; or
15) 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.

Response to Address Discrepancy notice

Upon receipt of notice of Address Discrepancy, City personnel will take steps to confirm that credit agency report relates to the person about whom it has requested the report. These steps will include:

1) Comparing the information in the credit agency report to the information that the City:
   a) has obtained to verify the person's identity;
   b) maintains in its own records, such as applications or change of address notifications;
   c) obtains from third party; or
2) Verifying the information in the credit agency report with the person to whom the report relates.

Response to Identity Theft

The City will notify the affected customer(s) of any Identity Theft, suspected or actual, of which it becomes aware. The following information will be included in the notice:

1) The type of identifying information involved;
2) The telephone number that the customer can call for further information and assistance, including:
   a) Local law enforcement;
   b) Federal Trade Commission;
   c) Credit Reporting Agencies, including Equifax, Experian, and Trans Union.

Proper disposal of Consumer information

The City will take reasonable measures to protect against unauthorized access to or use of Consumer information. The following steps will be taken:

1) Require City personnel or reputable destruction service provider to burn, pulverize, or shred papers containing Consumer information so that the information cannot practicably be read or reconstructed;
2) Require City personnel or reputable destruction service provider to destruct or erase electronic media containing Consumer information so that the information cannot practicably be read or reconstructed.
3) Prohibit City personnel or service provider from selling, donating, or transferring any medium, including computer equipment, upon which Consumer information is stored.

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. In doing so, 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 update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

The City's Identity Theft Prevention Program was approved by the City Council and began May 1, 2009. Responsibility for developing, implementing and updating this Program lies with the Program Administrator who may be the head of the City or his or her appointee. 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 in connection with City accounts, 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, the responsive steps to be taken when a Red Flag is detected, and proper disposal methods of Consumer information.

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 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 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.