City of Chelsea
Identity Theft Red Flag Policy

Policy

The City of Chelsea will fulfill its obligations under the Fair and Accurate Credit and Transactions Act of 2003 (FACTA), Public Law 108-159 and the final rules established by the Federal Trade Commission (FTC) regarding identity theft red flags. This policy shall be executed in accordance with the guidance provided in the City's red flag procedure.

Procedure

Scope

This policy applies to covered accounts within the City and the City's obligation to identify, prevent and detect potential identity theft risks associated with those accounts based on certain, known red flag indicators. This procedure also identifies response steps the City will take in the event a red flag indicator is encountered. For the City of Chelsea, covered accounts refer to customer utility accounts.

Intent

The intent of this procedure is to:

1. Identify personally identifiable information for City utility customers.
2. Describe the physical security controls over this information when it is printed on paper and in the City's possession.
3. Describe the electronic security controls over this information when it is stored within the City's utility billing system.
4. Place the City in compliance with Federal red flag rules regarding identity theft protection.

Coverage

This procedure applies to all City employees, contractors, consultants, temporary workers and others employed by the City with access to utility customer account information (hereafter referred to simply as employees).

General Policy

Prevention

1. Most personally identifiable information (PII) should only be used to identify an account holder. Limited PII is stored by the City—that is, account holder name, telephone number, and bank account number if they use automatic payment options. The City uses additional PII only for use in confirming identity to open an account, make changes to an existing account, or close an account. The Federal Trade Commission defines identifying information as "*any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any–*

a. *Name, social security number, date of birth, official State or government issued driver's license or identification number, government passport number, employer or taxpayer identification number;*

b. *Unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation;*

c. *Unique electronic identification number, address, or routing code; or*

d. *Telecommunication identifying information or access device*"

2. With the implementation of this procedure, the City will require persons opening utility accounts to complete the process in person at the City Offices so that a City employee can confirm personal identification with physical appearance. The City will require persons opening an account for a business to present appropriate identification. The person requesting to open the business account will be required to show personal identification to confirm authorization and business affiliation.

3. Requests to change or close an account can be made over the phone if the caller is the account holder and can confirm this by providing their name, address or account number. This can also be completed by submitting a notarized, written request through the mail. If an account holder does not choose to submit a notarized request, they must make the request in person so that identification can be verified.

4. To change an account to a new property owner or tenant, the new property owner or tenant must appear in person. If the former account holder does not call to end their service, the City will call the former account holder at the number on record and leave a message to confirm the service end date. If the former account holder is initiating the request to end service and transfer service to a new property owner or tenant, the former account holder must follow the add/change steps noted in item 4 above.

5. The City will continue to store all hard copies of automatic payment information containing account holder bank information in the City vault. Such information stored within the City utility system is not accessible outside the City offices. City office computers are not accessible to the public.

Detection

Red flags that might be encountered by City employees working with covered accounts include:

Suspicious Documents

- Documents provided for identification that appear to have been altered or forged
- A photograph or physical description on identification that is not consistent with the appearance of the applicant or customer presenting the identification
- Other information on the identification that is not consistent with readily accessible information that is on file with the municipality (such as the signature on an automated withdrawal application)

Personal Identifying Information

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the municipality (such as the local bank or police department)

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the municipality (for example, the address is fictitious, a mail drop or prison)
- The identification number provided is the same as that of another person with an account
- The person requesting the account fails to provide all required information or in response to notification that the application is incomplete
- Personal identifying information provided upon a change or close request is not consistent with personal identifying information already on file with the City

Unusual use of, or suspicious activity related to a covered account

- A covered account is used in a manner that is not consistent with established patterns of activity on the account (for example, nonpayment when there is no history of late or missed
- A covered account that has been inactive for a reasonably lengthy period of time is used
- A new account is used in a manner commonly associated with known patterns of fraud (for example, the customer fails to make the first payment or makes an initial payment but no subsequent payments)
- Mail sent to the customer is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The City is notified of unauthorized charges or changes made to a customer's covered account.
- The City receives notice from a customer, 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.
- The City receives 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 City.

Response Steps

The City Office staff will take the appropriate action from the following possible responses depending upon the nature of the red flag:

1. Monitor a covered account for evidence of identity theft
2. Contact the property owner and the account holder
3. Close the existing covered account
4. Notify law enforcement
5. Determine if no response is warranted

For any red flag identified the City Office staff will document the incident, including the date of occurrence, the covered account impacted, a description of the red flag, and the responsive actions taken. The incident will be recorded by the Administrative Director in a Red Flag Incident Log and the documentation will be filled in the manual customer file.

Oversight

The Administrative Director will provide a written annual report will be made and presented to City Council on compliance with the Program and any incidents experienced for the year. The report will include:

- The effectiveness of the defined policies and procedures in addressing the risk of identity theft
- Significant incidents that have occurred and management's response
- Recommendations for changing the Program

Definitions

The FTC Red Flag Rules defines certain key terms as follows.

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."

A ***covered account*** is 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."

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

The City of Chelsea defines certain key terms as follows:

Property owner is the owner on record in the City tax database, maintained by the City Assesors and available online at www.city-chelsea.org.

Account holder is the person, persons or business currently paying the utility account charges.