Financial Services Policy

SUBJECT: Identity Theft Detection and Prevention for Utility Customer Accounts **NO: UBO 1.16**

EFFECTIVE: November 1, 2008
REVISED: August 4, 2009
August 10, 2015

APPROVED: Constance P. Sanchez
Constance P. Sanchez
Director of Financial Services

PROGRAM ADOPTION:

The City of Corpus Christi ("Utility") developed an 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 of2003. 16 C.F.R. § 681.2. This program was approved by the Corpus Christi City Council on October 21, 2008 via Resolution Number 027910. This policy replaces Finance policy F-5.3.

PURPOSE:

A. Fulfilling requirements of the 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.

DEFINITIONS:

1. 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."

2. According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobiledealers, 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."

3. All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

   a. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

   b. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

4. "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.

IDENTIFICATION OF RED FLAGS:

In order to identify relevant Red Flags, the Utility 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 Utility identifies the following red flags, in each of the listed categories:

A. **Notifications and Warnings received from consumer reporting agencies or other consumer information service providers**

1. Report of fraud accompanying a consumer report;

2. Notice or report of a credit freeze on a customer or applicant.

B. Suspicious Identifying Information

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 a social security number or driver's license number that is the same as another utility customer);

5. An address presented that is the same as that of another person;

6. 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

7. A person's identifying information is not consistent with the information that is on file for the customer.

C. Suspicious Documents

I. Identification document or card that appears to be forged, altered or not authentic;

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 or is not consistent with readily accessible consumer information; and

4. Altered lease documents, or altered divorce decrees or altered marriage certificates.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name;

2. Mail sent to the account holder is repeatedly returned as undeliverable;

3. Notice to the Utility that an account has unauthorized activity;

4. Breach in the Utility's computer system security; and

5. Unauthorized access to or use of customer account information.

E. Alerts from Others

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

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 staff will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential and business address, principal place of business for an entity, driver's license or other government-issued identification.

2. Upon receipt of identifying information, staff person taking the initial application will run a consumer credit report or public data report to confirm information provided.

3. Do not open the account, and take steps to mitigate possibility of identity theft as described in Section V below, if the reports indicate fraud, or indicate discrepancy with identifying information.

B. Existing Accounts

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

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email); and update as necessary.

PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility 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. For new accounts, do not open the account until customer has brought in proof of identifying information.

2. For existing account, contact the customer and require the customer to bring in proof of identifying information within 30 days. Tum off the utilities if the customer does not provide the information by the time requested.

3. Notify law enforcement and the customer if the consumer reports indicate report of identity theft or fraud when identifying information cannot be independently identified.

PROGRAM UPDATES

This Policy will be periodically reviewed and updated at least every year by the Identity Theft Committee (described below) to reflect changes in identity theft risks to customers of the Utility. The Committee is jointly headed by the Utilities Business Office Manager and Call Center Manager and consists of the Assistant Director of Financial Services, the Director of Financial Services, attorney assigned to the Financial Services Department, and the Resolutions Supervisor. At least once a year, the Identity Theft Committee will meet to consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the Identity Theft Committee will determine whether changes to the Policy are warranted. If warranted, the recommended changes will be presented to City Council for their consideration. The determination to make changes to this policy will be made after careful consideration of the following:

A. Past experience(s) with identity theft.
B. Changes in methods of identity theft.
C. Changes in methods to detect, prevent, and mitigate identity theft.
D. Changes in the types of accounts the Utility offers.

PROGRAM ADMINISTRATION

A. Oversight

The Supervisor of the department responsible for utility applications (i.e., the Program Administrator) will be responsible to ensure appropriate training of utility application staff on the Program, for reviewing any reports regarding the detection of Red Flags, and determining which steps of prevention and mitigation should be taken in particular circumstances.

B. Staff Training and Reports

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 Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility 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 provider's review the Utility's Program and report any Red Flags to the Program Administrator.

D. Customer Address Discrepancies

1. When Utility receives notice from any consumer reporting agency that a substantial difference exists between the address for the consumer that Utility provided and the address(es) in the consumer reporting agency's file for that particular consumer, the Utility will verify the information in the consumer report provided by the consumer reporting agency with the consumer.

2. Once the address is confirmed, the Utility shall furnish the confirmed address to the consumer reporting agency as part of the information it regularly furnishes for the reporting period.

QUESTIONS ON THIS POLICY:

Questions on this Policy may be referred to the Director of Financial Services.

APPENDIX A

RESOLUTION APPROVING A POLICY REGARDING IDENTITY THEFT DETECTION AND PREVENTION FOR UTILITY CUSTOMER ACCOUNTS

Whereas, the Fair & Accurate Credit Transactions Act of 2003 ("Act") was signed into law to amend the Fair Credit Reporting Act, to improve accuracy of consumer reports and help prevent identity theft in covered accounts;

Whereas, under the rules adopted pursuant to the Act, covered accounts includes municipal utility accounts;

Whereas, under the rules adopted pursuant to the Act, municipal utilities are required to implement a written program for the detection, prevention and mitigation of identity theft as related to utility accounts;

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF CORPUS CHRISTI, TEXAS:

Section 1. The City Council approves the attached policy to detect and prevent identity theft related to utility customer accounts.

INTRODUCED AND PASSED by the City Council of the City of Corpus Christi, Texas, on the 21st day of October, 2008.

ATTEST:

Armando Chapa, City Secretary

CITY OF CORPUS CHRISTI

Henry Garrett, Mayor

Approved: Oct. 10, 2008

Lisa Aguilar
Assistant City Attorney
for City Attorney

027910

City of Corpus Christi

City Policies

SUBJECT: **Identity Theft Detection and Prevention for Utility Customer Accounts** **NO:** F-5.3 **EFFECTIVE:** 11/01/08

APPROVED: _____ **DATE:** _____

'Angel Escobar
Interim City Manager

I. PROGRAM ADOPTION

The City of Corpus Christi ("Utility") 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. § 681.2. This program was approved by Corpus Christi City Council on October 21, 2008.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the 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.

B. Definitions

This Policy incorporates the following definitions:

1. 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."

2. According to the Rule, a municipal utility 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."

3. All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

   a. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

   b. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

4. "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.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Utility 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 Utility identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings received from consumer reporting agencies or other consumer information service providers

1. Report of fraud accompanying a consumer report;

2. Notice or report of a credit freeze on a customer or applicant.

B. Suspicious Identifying Information

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 a social security number or driver's license number that is the same as another utility customer);

5. An address presented that is the same as that of another person;

6. 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

7. A person's identifying information is not consistent with the information that is on file for the customer.

C. Suspicious Documents

1. Identification document or card that appears to be forged, altered or not authentic;

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 or is not consistent with readily accessible consumer information; and

4. Altered lease documents, or altered divorce decrees or altered marriage certificates.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name;

2. Mail sent to the account holder is repeatedly returned as undeliverable;

3. Notice to the Utility that an account has unauthorized activity;

4. Breach in the Utility's computer system security; and

5. Unauthorized access to or use of customer account information.

E. Alerts from Others

1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that the Utility 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 staff will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential and business address, principal place of business for an entity, driver's license or other government-issued identification.

2. Upon receipt of identifying information, staff person taking the initial application will run a consumer credit report or public data report to confirm information provided.

3. Do not open the account, and take steps to mitigate possibility of identity theft as described in Section V below, if the reports indicate fraud, or indicate discrepancy with identifying information.

B. Existing Accounts

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

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email); and update as necessary.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility 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. For new accounts, do not open the account until customer has brought in proof of identifying information.

2. For existing account, contact the customer and require the customer to bring in proof of identifying information within 30 days. Turn off the utilities if the customer does not provide the information by the time requested.

3. Notify law enforcement and the customer if the consumer reports indicate report of identity theft or fraud when identifying information cannot be independently identified.

VI. PROGRAM UPDATES

This Policy will be periodically reviewed and updated at least every year by the Identity Theft Committee (described below) to reflect changes in identity theft risks to customers of the Utility. The Committee is jointly headed by the Utilities Business Office Manager and Call Center Manager and consists of the Assistant Director of Financial Services, the Director of Financial Services, attorney assigned to the Financial Services Department, and the Resolutions Supervisor. At least once a year, the Identity Theft Committee will meet to consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the Identity Theft Committee will determine whether changes to the Policy are warranted. If warranted, the recommended changes will be presented to City Council for their consideration. The determination to make changes to this policy will be made after careful consideration of the following:

A. Past experience(s) with identity theft.
B. Changes in methods of identity theft.
C. Changes in methods to detect, prevent, and mitigate identity theft.
D. Changes in the types of accounts the Utility offers.

VII. PROGRAM ADMINISTRATION

A. Oversight

The Supervisor of the department responsible for utility applications (i.e., the Program Administrator) will be responsible to ensure appropriate training of utility application staff on the Program, for reviewing any reports regarding the detection of Red Flags, and determining which steps of prevention and mitigation should be taken in particular circumstances.

B. Staff Training and Reports

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 Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility 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 Utility's Program and report any Red Flags to the Program Administrator.

D. Customer Address Discrepancies

1. When Utility receives notice from any consumer reporting agency that a substantial difference exists between the address for the consumer that Utility provided and the address(es) in the consumer reporting agency's file for that particular consumer, the Utility will verify the information in the consumer report provided by the consumer reporting agency with the consumer.

2. Once the address is confirmed, the Utility shall furnish the confirmed address to the consumer reporting agency as part of the information it regularly furnishes for the reporting period.

VIII. QUESTIONS REGARDING THIS POLICY

Questions regarding this Policy shall be directed to the Director of Financial Services or designee, who may be contacted at (361) 826-3613.

Corpus Christi, Texas

21st of October, 2008

The above resolution was passed by the following vote:

Henry Garrett	Aye
Melody Cooper	Aye
Larry Elizondo, Sr.	Absent
Mike Hummell	Aye
Bill Kelly	Aye
Priscilla G. Leal	Aye
John E. Marez	Aye
Nelda Martinez	Aye
Michael McCutchon	Aye

027910