Identity Theft Prevention Program

Approved September 13, 2011

Requirement:

All utilities are required to comply with this regulation. The Red Flag Rule requires any entity where there is a risk of identity theft, to develop and implement an Identity Theft Prevention Program. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The rule was issued by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The policy has been designed to comply with the Federal Trade Commission's (FTC) Identity Theft Red Flag Rule. The rule requires utilities to develop an "Identity Theft Prevention Program." The program consists of selecting methods to detect red flags when accounts are fraudulent, procedures to prevent the establishment of false accounts, procedures to ensure existing accounts are not being manipulated, and procedures to respond to identity theft. All utilities are required to comply with the FTC's "Identity Theft Red Flag Rule" even if only nominal information such as name, phone number and address are collected.

The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts are not being manipulated. This regulation does not address or require utilities to adopt measures that will protect consumer information and prevent unauthorized access. However, implementation of good management practices to protect personal consumer data can prevent identity theft.

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

The Red Flag Rule implements portions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Section 111 of FACTA defines "Identity Theft" as "fraud committed using the identifying information of another person."

Under the Red Flag Rule, every financial institution and "creditor" (defined below) is required to establish an Identity Theft Prevention Program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

- Identify relevant Red Flags for new and existing "covered accounts"
- Establish procedures to prevent the establishment of false accounts
- Establish procedures to assure existing accounts are not being manipulated
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- 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.

The Rule requires the Program to be approved by "a designated employee at the level of senior management."

Definitions Related to Municipal Utilities:

Municipal Utility: According to the Rule, a municipal utility is a creditor subject to the Rule requirements. Accounts maintained by a municipal utility that are covered by the Rule are all the individual utility service accounts held by customers of the utility whether residential, commercial or industrial.

Creditors: 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."~~any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and also regularly in the ordinary course of business:

- Obtains or uses consumer reports directly or indirectly in connection with a credit transaction; or
- Furnishes information to consumer reporting agencies in connection with a credit transaction; or
- Advances funds to or on behalf of a person based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.

The definition of creditors does not include an entity that allows for payment of services after the service has been provided.

The definition of creditors any other person whom the Federal Trade Commission determines offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.

Covered Account: Under the Rule, a "covered account" is:

- Any account th~~e~~at ~~Utility~~ 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 credit card account, utility account, checking account, or savings account; and
- Any other account the ~~Utility~~ financial institution or creditor offers or

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.5"

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.18", Hanging: 0.25"

maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the ~~Utility~~financial institution or creditor from from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

Identifying Information: "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." It specifically includes all of the items listed below:

- 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
- Routing code

Risk Assessment:

The City of Stacy Utility has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the utility was able to identify red flags that were appropriate to prevent identity theft:

- New accounts opened In Person without identification
- New accounts opened via Telephone
- New accounts opened via Fax
- New accounts opened via Web
- Account information accessed In Person
- Account information accessed via Telephone (Person)

Established Red Flags:

The City of Stacy Utility adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary:

- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Customer fails to provide all information requested
- Personal information provided is inconsistent with information on file for a customer
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

The tables on the following two pages are tools to assist in identifying specific Red Flags and procedures in the utility for incorporation into the utility employee training and incorporated into the Identity Theft Prevention Program.

"IDENTITY THEFT" (FRAUD) TYPE 1 – NEW ACCOUNTS

Establishing utility service using another person's identity

Why would someone do it?

- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his/her own name.
- The perpetrator intends to establish fraudulent proof of residency in order to commit fraud elsewhere.

Red flag:	**Detect whether fraud is being attempted or committed:**	**Prevent or mitigate detected fraud:**
ID picture doesn't match person	Request additional ID	Do not open account
ID information doesn't match person	Request additional ID	Do not open account
ID does not look authentic	Request additional ID	Do not open account
ID looks doctored	Request additional ID	Do not open account
Using a suspicious name	Request additional ID	Do not open account
Applicant requests that bill be sent to address different from where service is received	Verify that customer is connected to billing address (But be aware of the state's "Safe at Home" program)	Do not open account
Account for a residential address established under business name (to avoid using own bad name)	Obtain credit report on the individual	Do not open account
Bill payment made under name other than that on utility account	Request proof of residence (other bills, etc.)	Close account

"IDENTITY THEFT" (FRAUD) TYPE 2 – EXISTING ACCOUNTS

Continuing utility service under a another customer's name after he or she moves out

Why would someone do it?

- The perpetrator wants to avoid paying for service.
- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his/her own name.

Red flag:	**Detect whether fraud is being committed:**	**Mitigate detected fraud:**
Non-payment of previously current account	Call customer phone number on file	Discontinue service; close account
Utility service utilized after known move-out with no change of customer notice received by utility	Call customer phone number on file	Discontinue service; close account
Bill payment made under a name other than name on utility account	Call customer phone number on file	Discontinue service; close account

Suspect of Fraud Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the City Clerk:

- Ask applicant for additional documentation
- Notify City Clerk or Utility Billing Clerk of suspected fraud
- Notify law enforcement if warranted
- Do not open the account
- Close the account
- Do not attempt to collect against the account but notify authorities

Personal Information Security Procedures:

The following is a list of other security procedures that the city will follow to assure data is secure:

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.
2. Only specially identified employees with a legitimate need will have keys to the files.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employee will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employee store files when leaving their work areas
6. Employee log off their computers when leaving their work areas
7. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
8. No visitor will be given any entry codes or allowed unescorted access to the office.
9. Password-activated screen savers will be used to lock employee computers after a period of five minutes of inactivity.
10. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
11. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
12. When sensitive data is received or transmitted, secure connections will be used
13. Computer passwords will be required.
14. User names and passwords will be different.
15. The use of laptops is restricted to those employees who need them to perform their jobs.
16. Laptops are stored in a secure place.

17. Laptop users will not store sensitive information on their laptops.
18. Laptops which contain sensitive data will be encrypted
19. The computer network will have a firewall where your network connects to the Internet.
20. Check references or do background checks before hiring employees who will have access to sensitive data.
21. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
22. Access to customer's personal identity information is limited to employees with a "need to know."
23. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
24. Implement a regular schedule of employee training.
25. Employees are required to notify the City Clerk immediately if there is a potential security breach, such as a lost or stolen laptop.
26. Employees who violate security policy are subjected to discipline.
27. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
28. Sensitive Paper records will be shredded before being placed into the trash.
29. Paper shredders will be available at each office.
30. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Contact Information:

The Senior Management Person responsible for this program is:

Name:	Sharon Payne
Title:	City Clerk
Phone number:	651-462-4486

The Governing Body Members of the Utility are:

Mayor:	Mark Utecht
Council:	Tony Olivolo
	Dennis Thieling
	Mark Ness
	Paul Authier

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the City Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

This plan was approved by the City Council on September 13, 2011; revised on _____.

_____ _____

Mark Utecht, Mayor Sharon MT Payne, City Clerk