CITY OF OSSEO WATER UTILITY

Identity Theft Prevention Program

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 compliance date is May 1, 2009 and includes all U.S. utilities.

Identity Theft Prevention Program
For
City of Osseo Water Utility
13712 – 8th Street, P O Box 308
Osseo, Wisconsin 54758
January 9th, 2024

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.

Contact Information:

The Senior Management Person responsible for this program is:

Name: Steven Durham

Title: Director of Public Works

Phone number: (715) 597-2207

The Governing Body Members of the Utility are:

Council Members:

1. Mayor Joshua R. Pettis
2. Council President Timothy Johnson
3. Councilman Jim Cialdini
4. Councilperson Jerilyn Mulcahy
5. Councilman Stuart Dodge
6. Councilman Greg Eisberner
7. Councilman Rodney Anderson

Risk Assessment

The **City of Osseo Water 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
- ❑ New accounts opened via Telephone
- ❑ New accounts opened via Fax
- ❑ Account information accessed In Person
- ❑ Account information accessed via Telephone (Person)

Detection (Red Flags):

The **City of Osseo Water 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.

- ❑ Fraud or active duty alerts included with consumer reports
- ❑ Notice of credit freeze provided by consumer reporting agency
- ❑ Notice of address discrepancy provided by consumer reporting agency
- ❑ Inconsistent activity patterns indicated by consumer report such as:
    - Recent and significant increase in volume of inquiries
    - Unusual number of recent credit applications
    - A material change in use of credit
    - Accounts closed for cause or abuse
- ❑ 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.
- ❑ Application appears altered or destroyed and reassembled
- ❑ Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- ❑ Lack of correlation between the SS# range and date of birth
- ❑ Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- ❑ Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- ❑ Address or telephone # is the same as that of other customer at utility

- ❑ 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

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 senior management official.

- ❑ Ask applicant for additional documentation
- ❑ Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the City Clerk or Public Works Director.
- ❑ Notify law enforcement: The utility will notify the Chief of Police of the Osseo Police Department at (715) 597-2481 of any attempted or actual identity theft.
- ❑ Do not open the account
- ❑ Close the account
- ❑ Do not attempt to collect against the account but notify authorities

---

Personal Information Security Procedures:

The **City of Osseo Water Utility** adopts the following security procedures:

1. Paper documents, file, and electronic media containing secure information will be stored in locked file cabinets in a locked room.
2. Only identified employees with a legitimate need will have access to customer's personal information or keys to the room and cabinets.
3. Files containing personally identifiable information are kept in locked file cabinets except when working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. When leaving their work areas, employees shall: store files, log off computers, lock file cabinets and lock file room doors.
6. Any visitors entering the area where sensitive files are kept must be escorted by an employee of the utility. Visitors will not be given any entry codes or be allowed

unescorted access to the office.

7. Employees shall protect sensitive information by using "strong" passwords. Passwords shall contain a mix of letters, numbers, and characters and shall not be shared or posted near workstations. Usernames and passwords will be different with passwords being changed at least monthly.
8. Password activated screen savers will be used to lock employee computers after a period of inactivity.
9. When installing new software, vendor-supplied default passwords shall be changed immediately.
10. Anti-virus programs will be run on individual computers and on servers daily.
11. The computer network will have a firewall where your network connects to the Internet.
12. Any wireless network in use is secured.
13. Conduct background checks before hiring employees who will have access to sensitive data.
14. New employees must sign the city's Confidentiality Agreement.
15. Procedures exist for making sure that employees who leave the city's employment, no longer have access to sensitive information.
16. Implement a regular schedule of employee training.
17. Employees are required to notify the Public Works Director immediately if there is a potential security breach.
18. Employees who violate security policy are subject to discipline, up to, and including, dismissal.
19. Paper records will be shredded before being placed into the trash.

Identity Theft Prevention Program Review and Approval

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

Signatures:

1. Joshua R. Pettis Date 3-5-24
2. [signature] Date 3-11-24
3. Stuart Dodge Date 3-11-24
4. Rod Anderson Date 3/11/24
5. [signature] Date 3/11/24
6. Jerilyn Mulcahy Date 3/11/24
7. Greg Esbenn Date 3/11/2024

A report will be prepared annually and submitted to the above named senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.