Consent Agenda
Item I-G

DES MOINES WATER WORKS
Board of Water Works Trustees

Des Moines Water Works
Water You Can Trust for Life

2201 George Flagg Parkway | Des Moines, Iowa 50321-1190 | (515) 283-8700 | www.dmww.com

MEMORANDUM

DATE: January 15, 2019

TO: William Stowe, CEO and General Manager

FROM: Amy Kahler, Director of Customer Service

SUBJECT: Identity Theft Prevention Policy

Effective May 1, 2009, Des Moines Water Works (DMWW) implemented an Identity Theft Prevention Policy in response to "red flag" rules in the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). These rules require certain companies, including Des Moines Water Works, identify and respond to account activities that may indicate identity theft.

Attached is the Identity Theft Prevention Policy for Des Moines Water Works. The policy defines and addresses the handling of sensitive information and how to identify, detect, and respond to theft red flags. DMWW customer service and employee focused processes have been structured to adhere to this policy. Customer Service staff is (re)trained on this policy annually during team meetings.

Section VIII of the policy outlines the Board will review and reaffirm the policy annually in order to reflect changing risks to Des Moines Water Works, employees, and customers. No change is recommended to the policy at this time.

Attachment

DES MOINES WATER WORKS
Board of Water Works Trustees

2201 George Flagg Parkway | Des Moines, Iowa 50321-1190 | (515) 283-8700 | www.dmww.com

Identity Theft Prevention Policy

I. Background

This policy shall be known as Des Moines Water Works' ("Utility") Identity Theft Prevention Policy. The risk to the Utility, its employees and customers from data loss and identity theft is of significant concern to the Utility and can be reduced only through the combined efforts of every employee.

This policy applies to new or existing business, personal, and household accounts for which there is a reasonably foreseeable risk of identity theft, or for which there is a reasonably foreseeable risk to the safety or soundness of the utility from identity theft, including financial, operational, compliance, reputation, or litigation risks.

II. Purpose

The Utility adopts this sensitive information policy to help protect employees, customers, contractors, and the Utility from damages related to the loss or misuse of sensitive information.

This policy will:

a. Define sensitive information and outline policies for the security of sensitive information;
b. Identify relevant red flags to prevent identify theft;
c. Outline procedures to be followed when identity red theft flags are detected; and
d. Assist the Utility in complying with state and federal law regarding identity theft protection.

III. Sensitive Information

A. Sensitive Information Definition

Sensitive information includes the following items whether stored in electronic or printed format:

1. Credit card information, including
    i. Credit card number (in part or whole)
    ii. Credit card expiration date
    iii. Credit card CVV code
    iv. Cardholder name

v. Cardholder address

2. Tax identification numbers, including:
    i. Social security number
    ii. Business identification number
    iii. Employer identification number

3. Paychecks and paystubs

4. Cafeteria plan check requests and associated paperwork

5. Medical information for any employee or customer, including but not limited to:
    i. Doctor names and claims
    ii. Insurance claims
    iii. Prescriptions
    iv. Any related personal medical information

B. Sensitive Information Policies

1. Customer social security numbers will not be collected by the utility as a requirement to receive water service.

2. When appropriate or requested by a customer, the Utility will designate a password that must be provided in order to verbally transact business related to the protected account.

3. Each employee and contractor performing work for the Utility will comply with the following policies:
    i. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
    ii. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday, or when unsupervised.
    iii. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
    iv. Whiteboards, dry-erase boards, writing tablets, etc. containing sensitive information in common shared work areas will be erased, removed, or shredded when not in use.
    v. When documents containing sensitive information are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut shredding device.
    vi. Credit card information must be encrypted when stored in electronic format.

IV. Identifying Relevant Red Flags to Prevent Identity Theft

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag is apparent, it should be investigated for verification.

1. Alerts, notifications, or warnings from a consumer reporting agency.
2. A fraud or active duty alert included with a consumer report.
3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report.
4. A notice of address discrepancy from a consumer reporting agency.
5. Notice of credit card chargeback from customer's financial institution.
6. Mail sent to the customer is returned repeatedly as undeliverable, although water service continues to be provided at the service address in connection with the customer's covered account.
7. The utility 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 utility.
8. Suspicious documents, including but not limited to:
    a. Documents provided for identification that appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.
    b. A photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
    c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

V. Detection of Identity Theft Red Flags

In addition to the policies outlined in Section IIIB, the following procedures are aimed at detecting identity theft red flags:

1. All credit card transactions will require the use of the 3 digit CVV code and the cardholder's zip code.
2. The Utility may require photo identification and/or a lease agreement when opening an account or finaling or closing an account with an outstanding past due balance.
3. The Des Moines Water Works website will require a user login and password in order for customers to gain access to online account information.

VI. Response to Identity Theft Red Flags

Once potentially fraudulent activity is detected, an employee must act quickly, as a rapid appropriate response can protect customers and the Utility from damages and loss. Appropriate responses may include, but are not limited to:

1. Not processing or canceling the payment.
2. Not opening a new account.
3. Closing an existing account.
4. Monitoring the account for evidence of identity theft.
5. Not attempting to collect on an account, either directly, through special assessment, or through a 3rd party debt collection agency.
6. Notifying and cooperating with appropriate law enforcement
7. Notifying the actual customer that fraud has been attempted.
8. Determining that, under the circumstances, no response is warranted.

VII. Policy Updates

This policy and the procedures associated with its implementation, shall be updated as necessary, but at least annually, to reflect changes in risks to customers or to the Utility from identity theft, based on factors such as the Utility's experiences with identity theft, changes in methods of identity theft, changes in methods of detection, prevention, and mitigation of identity theft, changes in the types of accounts offered by the Utility, and changes in the Utility's business arrangements, including third party service provider arrangements. Information relating to such factors shall be collected by the Customer Service Department and shall be furnished to the Board of Trustees as part of the review provided for in Section VIII below.

VIII. Policy Administration.

This policy shall be approved by the Des Moines Water Works Board of Trustees and reviewed by the Board of Trustees annually.

Staff training shall be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the Utility or its customers. The Customer Service Department shall conduct training for appropriate members of staff on at least an annual basis and shall administer this policy.

The Utility shall ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the "red flag" rules and validated by appropriate due diligence, may be considered to be meeting these requirements.