Templeton Municipal Light and Water Plant

RED FLAG POLICY

1. POLICY

   It is the policy of the Templeton Municipal Light and Water Plant (TMLWP) that information compiled on all customers and employees is to be vigorously defended against Identity Theft.

2. INTRODUCTION

   This policy has been developed in accordance with the Fair and Accurate Transactions Act of 2003 (FACT Act) implemented under Section 114 of the Act to provide "Red Flag" Guidelines as well as Section 315 which provides guidance to financial institutions for responding to address discrepancy notices sent by a consumer reporting agency. It has been designed to detect, prevent, and mitigate identity theft in connection with existing customer accounts, the opening of new customer accounts, and information held on employees.

3. COVERAGE: Any account opened by a customer and/or any file opened on a full- or part-time employee.

4. TREATMENT OF SENSITIVE DATA

   A. COLLECTION OF INFORMATION:

      i. Employees collecting sensitive data on new customers will verify the identity of the customer for whom the account is being established by requiring the Positive Photo Identification, such as a valid current driver's license or current passport.

      ii. Employees making changes to an account of an existing customer will verify the identity of the caller as the existing customer by requiring at least one of the following:

         a. Positive Photo Identification, such as a valid current driver's license or current passport,

b. Identifying activity on the account such as last payment date and amount, and/or

c. Social Security #.

iii. No customer account will be established or changed based upon the presentation of suspicious documents.

iv. Employees collecting sensitive data on new employees will require the following:

a. Positive Photo Identification, such as a valid current driver's license or current passport.

b. Proof of Residency.

c. Authorization to conduct a criminal history check.

d. Completion of Form I-9, Employment Eligibility Verification.

B. RELEASE OF INFORMATION:

i. No employee will release information on a customer or employee to anyone other than the identified customer, employee, authorized third party contracted with TMLWP, or to a third party who has received the expressed authorization from the customer or employee. Such information may include but is not limited to:

a. Personal information such as phone listings, mailing addresses, service addresses, marital status or medical records.

b. Financial information such as payment records, financial account data, and wages.

ii. At no time will banking or social security information be released to anyone other than a third party contracted with the Department.

iii. All contractors of the Department who come into contact with customer or employee information must provide the Department with the following:

a. A written Red Flag Policy where required or the written equivalent, and

b. An agreement to notify the Department immediately in the event of a security breach regarding the employees or customers of the Department.

C. STORAGE OF INFORMATION: Employees who handle sensitive data will take steps to ensure that it is not compromised with such actions that may include but are not limited to:

i. Locked files with limited access.

ii. Shredding all unused and/or outdated documents containing sensitive data.

iii. Password-protected computers.

D. IDENTIFICATION OF INFORMATION: To facilitate response in the event of an identity breach emergency, the Department will store in a locked file a master list of sensitive information including, but not limited to:

i. Type of sensitive information stored in the Department's files.

ii. Location of the stored sensitive information.

iii. List of personnel with authorized access to information.

iv. List of companies contracted with the Department who have access to sensitive information and their Written Red Flag policy or equivalent.

5. PROCEDURE FOR "RED FLAGS"

E. Accounts that are subjected to alerts, notifications, or other warnings from consumer reporting agencies or service providers such as fraud detection services, law enforcement authorities or other persons regarding possible identity theft will be flagged and investigated.

i. When the identity of the Customer of Record is at issue:

a. The customer will be required to show proof of identity or the account will be terminated.

b. Any person whose identity was fraudulently used to establish an account will not be considered liable for the charges rendered on the account.

c. Every attempt will be made to ascertain and assess the true identity of the person who signed for the account.

ii. When the identity of the Customer of Record is not at issue but has been reported stolen in non-Department related events, the account will be flagged and no changes will be made to the account without photo identification.

F. Suspicious activity related to a covered account will immediately be reported to The General Manager and Office Manager for investigation, and the account will be flagged.

6. REPORTING OF EVENTS

G. Annual Reports:

i. The Office Manager will maintain a record of suspicious events and flagged accounts with regard to customer accounts. The Office Manager will keep a record of suspicious events with regards to employee files.

ii. An annual report of "significant events" will be made to the General Manager, including recommendations for program changes as risks and methods of identity theft evolve.

H. Incident Reports:

i. Security breaches will immediately be reported to the General Manager.

ii. Security breaches that could result in harm to a person or business will be immediately reported to the police or responsible authority.

iii. Security breaches that impact financial accounts held by financial institutions and credit card companies will be reported to these institutions so that the accounts can be monitored.

iv. Security breaches will be promptly reported to the customer or employee.

7. TRAINING

I. All Department employees will receive copies of the Red Flag Policy and will be educated on how to identify and respond to the risk of identity theft. On-going

training sessions will be held in response to changes in risks and methods of identity theft.

Adopted: November 04, 2008

Municipal Light Board: _____
Dana Blais, Chairman

_____
Gregg Edwards, Clerk

_____
Gerald Skelton, Member