North Attleborough Electric Department

Identity Theft Prevention Program

Implemented as of November 1, 2009

Adopted by the Board of Electric Commissioners, 10-28-09

FILE: POLICY – RED FLAGS..., 8-09

I. INTRODUCTION

The **North Attleborough Electric Department (**the "Department") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. 16 C. F. R. § 681.2 and consistent with the provisions of MGL Chapter 93H of 201 CMR Section 17.00. This Program is designed to detect, prevent and mitigate Identity Theft in connection with the opening and maintenance of certain Department accounts. For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The accounts addressed by the Program, (the "Accounts"), are defined as:

1. An account the Department offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Department offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Department from Identity Theft.

This Program was developed with oversight and approval of the North Attleborough Electric Commissioners and General Manager**.** After consideration of the size and complexity of the Department's operations and account systems, and the nature and scope of the Department's activities, the North Attleborough Electric Commissioners and the General Manager determined that this Program was appropriate for the North Attleborough Electric Department and therefore approved this Program on October 28, 2009.

II. IDENTIFICATION OF RED FLAGS.

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the Department considered 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 Department identifies the following Red Flags, in each of the listed categories:

A. Suspicious Documents.

1) Receiving documents that are provided for identification that appear to be forged or altered;
2) Receiving documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;
3) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4) Receiving an application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information.

1) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent SSNs or Driver License Numbers);
2) A person's identifying information is the same as shown on other applications found to be fraudulent;
3) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
4) A person's SSN or Driver License Number is the same as another customer's SSN or Driver License Number;
5) A person's address or phone number 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; and
7) A person's identifying information is not consistent with the information that is on file for the customer.

D. Unusual Use Of or Suspicious Activity Related to an Account.

1) A change of address for an Account followed by a request to change the Account holder's name;
2) An account being used in a way that is not consistent with prior use (such as late or no payments when the Account has been timely in the past);
3) Mail sent to the Account holder is repeatedly returned as undeliverable;
4) The Department receives notice that a customer is not receiving his paper statements; and

5) The Department receives notice that an Account has unauthorized activity.

E. Notice Regarding Possible Identity Theft.

1) The Department receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

III. DETECTION OF RED FLAGS.

In order to detect any of the Red Flags identified above with the opening of a new Account, Department personnel will take the following steps to obtain and verify the identity of the person opening the Account:

1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, SSN, driver's license or other identification;
2) Verifying the customer's identity, such as by copying and reviewing a driver's license or other identification card;
3) Reviewing documentation showing the existence of a business entity

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

1) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2) Verifying the validity of requests to change billing addresses; and
3) Verifying changes in banking information given for billing and payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT.

In the event Department 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) Continuing to monitor an Account for evidence of Identity Theft;
2) Contacting the customer;
3) Changing any passwords or other security devices that permit access to Accounts;
4) Reopening an Account with a new number;
5) Not opening a new Account;
6) Closing an existing Account;
7) Notifying law enforcement;
8) Determining that no response is warranted under the particular circumstances

Because a Department will not be able to predict particular circumstances that may arise, this section may be drafted to show a range of possible responses and identifying one or more persons who will be responsible within the Department for determining what response is appropriate in a circumstance. For example, if the Department receives notice that its system has been compromised such that a customer's personal information has become accessible, the Department would likely, at a minimum, notify the customer and change passwords. If the Department receives notice that a person has provided inaccurate identification information, the appropriate response may be to close the Account and contact law enforcement.

In order to further prevent the likelihood of identity theft occurring with respect to Department accounts, the Department will take the following steps with respect to its internal operating procedures:

1) Providing a secure website;
2) Ensuring complete and secure destruction of paper documents and computer files containing customer information;
3) Ensuring that office computers are password protected and that computer screens lock after a set period of time.

V. UPDATING THE PROGRAM AND THE RED FLAGS

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Department from Identity Theft. At least annually, the General Manager, will consider the Department'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 Department maintains and changes in the Department's business arrangements with other entities. After considering these factors, the General Manager will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the General Manager will present the Board of Electric Commissioners with his or her recommended changes and the Commissioners will make a determination of whether to accept, modify or reject those changes to the Program.

VI. PROGRAM ADMINISTRATION.

A. Oversight

The Department's Program will be overseen by a Program Administrator. The Program Administrator shall be: **Business Division Manager.**

The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of Department staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

B. Staff Training and Reports

Department 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 Department engages a service provider to perform an activity in connection with one or more Accounts, the Department 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) Requiring, by contract, that service providers have such policies and procedures in place;
2) Requiring, by contract, that service providers review the Department's Program and report any Red Flags to the Program Administrator.