Model Identity Theft Policy: Section 5

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Model Identity Theft Policy: Section 5

Reference Number:
MTAS-1258

If the municipality maintains certain covered accounts pursuant to federal legislation, the municipality may include the additional program details.

5.A: Covered accounts
A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:
1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the municipality from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5.B: Red flags
5.B.1: 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; or
4. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

5.B.2: Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
• A recent and significant increase in the volume of inquiries;
• An unusual number of recently established credit relationships;
• A material change in the use of credit, especially with respect to recently established credit relationships; or
• An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5.C: Suspicious documents
5.C.1: Documents provided for identification that appear to have been altered or forged.
5.C.2: The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
5.C.3: Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
5.C.4: Other information on the identification is not consistent with readily accessible information that is on file with the municipality, such as a signature card or a recent check.
5.C.5: An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.D: Suspicious personal identifying information
5.D.1: Personal identifying information provided is inconsistent when compared against external information sources used by the municipality. For example:
• The address does not match any address in the consumer report;
• The Social Security number (SSN) has not been issued or is listed on the Social Security Administration’s Death Master File; or
• Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

5.D.2: Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the municipality. For example, the address on an application is the same as the address provided on a fraudulent application.
5.D.3: Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the municipality. For example:
• The address on an application is fictitious, a mail drop, or a prison; or
• The phone number is invalid or is associated with a pager or answering service.

5.D.4: The SSN provided is the same as that submitted by other persons opening an account or other customers.
5.D.5: The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
5.D.6: The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

5.D.7: Personal identifying information provided is not consistent with personal identifying information that is on file with the municipality.
5.D.8: When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5.E: Unusual use of, or suspicious activity related to, the covered account
5.E.1: Shortly following the notice of a change of address for a covered account, the municipality receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
5.E.2: A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments
5.E.3: A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
• Nonpayment when there is no history of late or missed payments;
• A material change in purchasing or usage patterns

5.E.4: A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
5.E.5: Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
5.E.6: The municipality is notified that the customer is not receiving paper account statements.
5.E.7: The municipality is notified of unauthorized charges or transactions in connection with a customer's covered account.
5.E.8: The municipality 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 municipality
5.E.9: The municipality is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

MTAS