Published on *MTAS* (http://www.mtas.tennessee.edu) July 05, 2020

Identity Theft Policy

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

Identity Theft Policy

Reference Number: MTAS-1255

Employers who offer of maintain at least one covered account must develop and implement a written attached Identity Theft Program that is designed to detect, prevent and mitigate identity theft. The program should identify relevant red flags (risk factors and sources of red flags), address the detection of red flags, prevent and mitigate identity theft, be updated and indicate the methods for administering the program.

Following is a section-by-section breakdown of the model policy.

Section one of the policy states broadly that only a concerted effort of every affected employee can mount an effective defense against the threat of identity theft.

Section two lays out the intent of the policy, which is to define sensitive information, describe the relevant security of data, and to protect this data, thus placing the municipality in compliance with federal law.

Section three speaks to coverage, stating that all employees, contractors, consultants, temporary workers, and other workers at the municipality are covered.

The general policy is provided in **section four**. First, sensitive information is defined, and examples are provided. Generally, any personally identifying financial or medical information is deemed sensitive under the rules and thus subject to protections. Whether in hard copy or electronic form, sensitive information must be protected by the reasonable, common sense measures provided.

Section five provides detailed definitions of covered accounts and red flags.

The federal rules define a covered account as an “account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.”

Section 681.2 (3). This policy incorporates that definition and charges the municipality with monitoring any such account for which there is a reasonably foreseeable risk of identity theft.

This foreseeable risk of identity theft is assessed by the numerous red flags provided for in Section 5.B. Red flags are indicators of fraud and include, but are not limited to the following:

- On alert, notification or warning from a consumer reporting agency;
- A credit freeze imposed by a consumer reporting agency;
- Address discrepancy notice from a consumer reporting agency;
- Irregular or suspicious account activity;
- Suspicious documents;
- Personal identifying information inconsistent with external information used for verification; and
- Personal identifying information associated with prior fraud.

Further examples of these red flags are provided in the policy.

Upon detecting a red flag, a municipality must, under section six, take specific actions to quash or mitigate the threat. The first step is to gather all related documentation and prepare a brief description of the situation. This initial investigation must be immediately forwarded to the preparing employee’s supervisor. The supervisor must then determine the merits of the potential red flag.

If the supervisor determines that the transaction is fraudulent, further action must be taken. These actions may include:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Determining the extent of liability to municipality; and
- Notifying the actual customer that fraud has been attempted.

As technology and nefarious scheming create new methods for attempting identity theft, this policy must be reviewed periodically to incorporate new red flags and new responses. This policy does not mandate the time frame for periodic update, leaving that decision to those responsible for managing the program. It is recommended, however, that the policy be updated as often as needed to stay current with any new threat or response. At a minimum, the policy should be reviewed for needed updates.

While identity theft is the responsibility of the entire municipal staff and requires board adoption, direct administration should be designated to a single person. Logical choices for administrator are city recorder, finance director or IT director. This designee must be noted in section 8.A.3 of the policy.

The chosen director is also responsible for identity theft training as provided for in section 8.B. Training in all sections of the policy is mandated for all employees, officials and contractors who may come into contact with covered accounts. In assessing which employees to include in these trainings, MTAS recommends to err on the side of inclusion.

While MTAS does not currently endorse any specific training, a growing number of public and private entities are offering identity theft training at a wide array of costs. In assessing your training needs consider the scope of your program and number of affected employees. Investigate a number of potential candidates before making your selection.

In addition to in-house employee training, municipalities are required to ensure that external service providers are in compliance with the provisions of this policy. However, if the external service provider has adopted and implemented its own identity theft policy, this will suffice. It is advisable for municipalities using external service providers to either obtain a copy of the provider's policy or a statement from the provider stating the existence of the policy and a promise of due diligence.
