

Clinton, Tennessee

RESOLUTION NO. 629

A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, required rules regarding identity theft protection to be promulgated; and

WHEREAS, Those rules become effective November 1, 2008, and require municipal utilities and other departments to implement an identity theft program and policy, and

WHEREAS, The City of Clinton has determined that the following policy is in the best interest of the municipality and its citizens. NOW, THEREFORE,

BE IT RESOLVED by the City of Clinton that the following is hereby approved:

IDENTITY THEFT POLICY

SECTION 1: BACKGROUND

The risk to the municipality, its employees and customers from data loss and identity theft is of significant concern to the municipality and can be reduced only through the combined efforts of every employee and contractor.

SECTION 2: PURPOSE

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

This policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the municipality in compliance with state and federal law regarding identity theft protection.

This policy enables the municipality to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the municipality from fraudulent new accounts. The program will help the municipality:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

SECTION 3: SCOPE

This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers at the municipality, including all personnel affiliated with third parties.

SECTION 4: POLICY

4.A: Sensitive Information Policy

4.A.1: Definition of Sensitive Information

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

4.A.1.a: Credit card information, including any of the following:

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address

4.A.1.b: Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

4.A.1.c: Payroll information, including, among other information:

1. Paychecks
2. Pay stubs

4.A.1.d: Cafeteria plan check requests and associated paperwork

4.A.1.e: Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

4.A.1.f: Other personal information belonging to any customer, employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number

4.A.1.g: Municipal personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Tennessee Public Records Act and the municipality's open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. In the event that the municipality cannot resolve a conflict between this policy and the Tennessee Public Records Act, the municipality will contact the Tennessee Office of Open Records.

4.A.2: Hard Copy Distribution

Each employee and contractor performing work for the municipality will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

3. 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.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" Municipal records, however, may only be destroyed in accordance with the city's records retention policy.

4.A.3: Electronic Distribution

Each employee and contractor performing work for the municipality will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved municipal e-mail. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM

5.A: Suspicious documents

5.A.1: Documents provided for identification that appear to have been altered or forged.

5.A.2: The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

5.A.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.A.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.A.5: An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.B: Suspicious personal identifying information

5.B.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.B.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.B.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.

SECTION 6: RESPONDING TO RED FLAGS

6.A: Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the municipality from damages and loss.

6.A.1: Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

6.A.2: The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the municipality; and

4. Notifying the actual customer that fraud has been attempted.

SECTION 7: PERIODIC UPDATES TO PLAN

7.A: At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

7.B: As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

7.C: Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the municipality and its customers.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Involvement of management

1. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. The Identity Theft Prevention Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.
3. Operational responsibility of the program is delegated to the City Manager

8.B: Staff training

1. Staff training shall be conducted for all employees, officials and contractors 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 municipality or its customers.
2. Police Department is responsible for ensuring identity theft training for all requisite employees and contractors.
3. Employees must receive annual training in all elements of this policy.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

8.C: Oversight of service provider arrangements

1. It is the responsibility of the municipality to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

2. 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.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

This resolution will take effect immediately upon its passage, the public welfare requiring it.

Approved this 20th day of October, 2008

Mayor Winfred Shoopman

Attest: _____
Vickie Fagan, City Recorder