University of Tennessee, Knoxville
Trace: Tennessee Research and Creative Exchange

MTAS Publications: Full Publications | Municipal Technical Advisory Service (MTAS)

9-2008

Model Identity Theft Policy and FACTA Compliance

Josh Jones
Municipal Technical Advisory Service, jonesj@tennessee.edu

Follow this and additional works at: http://trace.tennessee.edu/utk_mtaspubs

Part of the Public Administration Commons

The MTAS publications provided on this website are archival documents intended for informational purposes only and should not be considered as authoritative. The content contained in these publications may be outdated, and the laws referenced therein may have changed or may not be applicable to your city or circumstances.
For current information, please visit the MTAS website at: mtas.tennessee.edu.

Recommended Citation
Jones, Josh, "Model Identity Theft Policy and FACTA Compliance" (2008). *MTAS Publications: Full Publications.*
http://trace.tennessee.edu/utk_mtaspubs/91

This Report is brought to you for free and open access by the Municipal Technical Advisory Service (MTAS) at Trace: Tennessee Research and Creative Exchange. It has been accepted for inclusion in MTAS Publications: Full Publications by an authorized administrator of Trace: Tennessee Research and Creative Exchange. For more information, please contact trace@utk.edu.

MODEL IDENTITY THEFT POLICY AND FACTA COMPLIANCE

by Josh Jones, Legal Consultant

September 2008

THE UNIVERSITY of TENNESSEE

MUNICIPAL TECHNICAL ADVISORY SERVICE

In cooperation with the Tennessee Municipal League

Model Identity Theft Policy and FACTA Compliance

by Josh Jones, Legal Consultant

September 2008

MTAS OFFICES

Knoxville (Headquarters).....(865) 974-0411
Johnson City.....(423) 854-9882
(423) 282-0416
Nashville.....(615) 532-6827
Jackson .....(731) 423-3710
Martin .....(731) 881-7055

www.mtas.tennessee.edu

The Municipal Technical Advisory Service (MTAS) was created in 1949 by the state legislature to enhance the quality of government in Tennessee municipalities. An agency of the University of Tennessee Institute for Public Service, MTAS works in cooperation with the Tennessee Municipal League and affiliated organizations to assist municipal officials.

By sharing information, responding to client requests, and anticipating the ever-changing municipal government environment, MTAS promotes better local government and helps cities develop and sustain effective management and leadership.

MTAS offers assistance in areas such as accounting and finance, administration and personnel, fire, public works, law, ordinance codification, and water and wastewater management. MTAS houses a comprehensive library and publishes scores of documents annually.

MTAS provides one copy of our publications free of charge to each Tennessee municipality, county and department of state and federal government. There is a $10 charge for additional copies of "Model Identity Theft Policy and FACTA Compliance."

Photocopying of this publication in small quantities for educational purposes is encouraged. For permission to copy and distribute large quantities, please contact the MTAS Knoxville office at (865) 974-0411.

Model Identity Theft Policy and FACTA Compliance

IDENTITY THEFT

Upon the death of Ivan the Terrible, three imposters all claimed to be the rightful heir to the Russian throne. These men, known as the three Dimitris, went to great lengths to usurp the power and riches that came with assuming a royal identity. This was 400 years ago, and identity theft was already a profitable trade. Back then such a scheme required years of deceitful effort, stores of charisma, and the ability to live every day as a fraud. In today's electronic world, however, a fraud need not don the clothes of his mark. An identity can be stolen with nothing more than a stolen string of numbers and malicious intent. With a few pieces of personal identifying information, an identity thief can easily secure an account in someone else's name. This information can be obtained from a variety of sources, including stolen mail, computer hacking, fraudulent address changes and other nefarious schemes.

FEDERAL LEGISLATION

In response to the growing threat of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Public Law 108-159. This amendment to the Fair Credit Reporting Act charged the Federal Trade Commission with promulgating rules regarding identity theft. On November 7, 2007, the Federal Trade Commission promulgated the final rules, known as "Red Flag" rules, which have an effective date of November 1, 2008. 16 CFR 681. These rules, implementing sections 114 and 315 of FACTA, require certain municipal departments to enact certain policies and procedures by the November 1, 2008, effective date.

DEFINITIONS AND SCOPE

The rules apply to "financial institutions" and "creditors" with "covered accounts."

Financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a transaction account belonging to a consumer.

Creditor "has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies."

A covered account is 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."

A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

All municipal water, wastewater, natural gas, and electric utilities are explicitly covered under these rules. The Federal Trade Commission has suggested that municipal departments that "defer payments" for goods or services are also covered.

PROGRAM REQUIREMENTS

Every affected municipality must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be appropriate to the size and complexity of the municipality and the nature and scope of its activities.

The program must include provisions to:

- Identify relevant red flags for covered accounts signaling possible identity theft and incorporate those red flags into the program;
- Detect red flags that have been incorporated into the program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks.

The policy must also provide for continued administration and oversight of the program, including:

- Obtaining approval of the initial written program by the governing body or an appropriate committee designated by the governing body;
- Involving the governing body, a committee of the governing body, or a designated management-level employee in the development, implementation, administration and oversight of the program;
- Staff training as necessary to effectively implement the program; and
- Exercise of appropriate and effective oversight of service provider arrangements.

Annually, the designated overseer of the municipality's identity theft program must report to the governing body on the effectiveness of the program and compliance with the regulatory requirements.

POLICY

The aforementioned ends of the federal legislation can be achieved by adopting and diligently implementing the attached Identity Theft Policy. 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, we are compiling a list of available training providers. 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.

VIOLATIONS

The Federal Trade Commission is authorized to commence action in a federal district court in the event of a knowing violation of FACTA. Civil penalties for violations are capped at $2,500 per offense. For municipalities that pull consumer reports of customers, failure to comply with the address discrepancy regulations subjects violators to penalties not exceeding $1,000.

Please review the attached policy with your governing body, affected department heads, IT staff and legal counsel before adoption. Should you have any questions, please contact your UT MTAS management consultant.

Helpful Links:

Fair and Accurate Credit Transactions Act of 2003 (complete text): http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf

Fair Credit Reporting Act: http://www.ftc.gov/os/statutes/031224fcra.pdf

Federal Trade Commission: http://www.ftc.gov

Model Identity Theft Policy and Adopting Resolution

_____, Tennessee

RESOLUTION NO. _____

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 _____ (insert governing body's name) has determined that the following policy is in the best interest of the municipality and its citizens. NOW, THEREFORE,

BE IT RESOLVED by the _____ (insert governing body's name) 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

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.

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: Periodic reviews will include an assessment of which accounts are covered by the program.

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

7.D: 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 _____.

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. _____ 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 _____ day of _____, 2008

_____

Mayor

Attest: _____

City Recorder

THE UNIVERSITY of TENNESSEE

MUNICIPAL TECHNICAL ADVISORY SERVICE

The University of Tennessee does not discriminate on the basis of race, sex, color, religion, national origin, age, disability, or veteran status in provision of educational programs and services or employment opportunities and benefits. This policy extends to both employment by and admission to the university.

The university does not discriminate on the basis of race, sex, or disability in its education programs and activities pursuant to the requirements of Title VI of the Civil Rights Act of 1964, Title IX of the Education Amendments of 1972, Section 504 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act (ADA) of 1990.

Inquiries and charges of violation concerning Title VI, Title IX, Section 504, ADA or the Age Discrimination in Employment Act (ADEA) or any of the other above referenced policies should be directed to the Office of Equity and Diversity (OED), 1840 Melrose Avenue, Knoxville, TN 37996-3560, telephone (865) 974-2498 (V/TTY available) or 974-2440. Requests for accommodation of a disability should be directed to the ADA Coordinator at the UTK Office of Human Resources, 600 Henley Street, Knoxville, TN 37996-4125.

MTAS1313 09/08 • E14-1050-000-016-09