TENNESSEE ASSOCIATION OF UTILITY DISTRICTS

Model "Red Flags" Rule Program

Identity Theft Prevention Program

John Shadwick

8/31/2008

This guide is prepared for use in the classroom to prepare utility staff to develop and implement an Identity Theft Prevention program compliant with the requirements of the Federal Trade Commission's Red Flag Rule.

Table of Contents

Standard Operating Procedures
Identity Theft Prevention

These procedures have been approved and adopted by the board of commissioners of Jakestown Utility District for the protection of its customers against identity theft.

Date of Adoption:

Section 1 – Identifying "Red Flags"

These have been identified as identity theft "red flags" relevant to this utility.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

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

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  a. The address does not match any address in the consumer report; or
  b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- 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.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  a. The address on an application is the same as the address provided on a fraudulent application; or
  b. The phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  a. The address on an application is fictitious, a mail drop, or a prison; or
  b. The phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- For financial institutions and creditors that use challenge questions, 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.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
  a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
  b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
  a. Nonpayment when there is no history of late or missed payments;
  b. A material increase in the use of available credit;
  c. A material change in purchasing or spending patterns;
  d. A material change in electronic fund transfer patterns in connection with a deposit account; or
  e. A material change in telephone call patterns in connection with a cellular phone account.
- 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).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The financial institution or creditor is notified that the customer is not receiving paper account statements.
- The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

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 Financial Institution or Creditor

- The financial institution or creditor 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 2 - Response to Attempted/Suspected Fraudulent Use of Identity

Internal Notification

Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify _____.

External Notification

Affected Individual – The utility will notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:

General information about the incident;

- The type of identifying information involved;
- The telephone number that the person can call for further information and assistance.
- Local Law Enforcement: _____
- Federal Trade Commission: (Toll free) 877-438-4338 or www.consumer.gov/idtheft
- Credit Reporting Agencies: Place fraud alerts on your credit reports by contacting credit bureaus.
  - •Equifax: (800) 525-6285 or http://www.equifax.com
  - •Experian: (800) 397-3742 or http://www.experian.com
  - •TransUnion: (800) 916-8800 or http://www.transunion.com

Method of Contact:

- Written notice, certified mail.
- E-mail, if the e-mail address is in the utility records.
- By telephone, provided the contact is made directly with the affected person and appropriately documented.

Local Law Enforcement

The utility will notify _____ at _____ of any attempted or actual identity theft.

Oversight of Third Party Service Providers

This utility will, as part of its contracts with third party service providers, require as part of the contract that these providers have policies, procedures and programs that comply with the "Red Flag" Rule.

Section 3 - Periodic Updates to the Program

The General Manager will review the program at least annually, or after each and every attempt at identity theft.

Any proposed changes will be presented to the board of commissioners for approval.

Section 4 - Reporting

The General Manager will report to the board of commissioners at its November 2008 meeting, and every January board meeting thereafter, on compliance with the "Red Flag" Rule. The report will include any material matters and issues regarding this program, such as:

- Initial implementation of the program;
- Employee training;
- Effectiveness of policies and procedures in addressing risk in how accounts are opened and maintained;
- Service provider (third party) arrangements;
- Significant incidents involving identity theft and management response;
- Recommendations for changes.

Section 5 -Customer Personal Identification Information

Information Collected

Identifying information is defined as **any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.**

The following identifying information is collected by this utility.

- Name
- Social Security Number
- Date of Birth
- Official State /government issued driver's license or identification number,
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- _____
- _____
- _____
- _____

How Customer Personal Identifying Information Is Collected

Customer personal identifying information is collected by:

- Presentation by customer at the office;
- Telephone;
- Internet;
- Mail.
- _____
- _____
- _____
- _____

Any other methods of collection are not acceptable.

Section 6 - Physical Security of Personal Identifying Information Is Protected

All paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information will be stored in a locked file cabinet.

File cabinets containing personally identifiable information will be stored in a locked room.

The _____ will control keys to the file cabinet and room, make any copies of the keys, and distribute those keys only to employees with a legitimate need.

Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.

Employees will not to leave sensitive papers out on their desks when they are away from their workstations.

At the end of the day, employees put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.

Access to offsite storage facilities is limited to employees with a legitimate business need. Access keys/codes will only be given to those employees. All employees who enter these facilities will document their visit.

Any sensitive information shipped using outside carriers or contractors will be encrypted and an inventory of the information being shipped will be kept. It will be shipped using an overnight shipping service that will allow tracking of the delivery this information.

Building Access

Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.

No visitor will be given any entry codes or allowed unescorted access the office.

Section 7 - Security of Electronic Records

General Network Security

Computers or servers where sensitive personal information is stored.

_____

_____

_____

Connections to the computers where sensitive information is stored. These include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

_____

_____

_____

Connections vulnerable to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

Sensitive consumer data will not be stored on any computer with an Internet connection unless it's essential for conducting your business.

Sensitive information that is sent to third parties over public networks will be encrypted.

Sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees will be encrypted.

Email transmissions within your business will be encrypted if they contain personally identifying information.

Anti-virus and anti-spyware programs will be run on individual computers and on servers on your network daily.

When credit card information or other sensitive financial data is received or transmitted, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

Password Management

Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.

Passwords will not be shared or posted near workstations.

Password-activated screen savers will be used to lock employee computers after a period of inactivity.

When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

Laptop Security

The use of laptops is restricted to those employees who need them to perform their jobs.

Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop.

Laptops are to be stored in secure place.

Laptop users will only have access to sensitive information, but not to store the information on their laptops.

Laptop which contain sensitive data will be encrypted and configured so that users can't download any software or change the security settings without approval from your IT specialists.

All laptops will be configures with an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.

Employees are never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security.

If a laptop must be left in a vehicles, it should be locked in a trunk.

Firewalls

Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.

The computer network will have a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.

If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.

If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.

Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.

Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Detecting Breaches

To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.

Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.

Have in place and implement a breach response plan. See pages 22–23 for more information.

Section 8 – Employee Training

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

Check references or do background checks before hiring employees who will have access to sensitive data.

New employees will sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

Access to customer's personal identify information is limited to employees with a "need to know."

Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Employees will be alert to attempts at phone phishing.

Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.

Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.

Section 9 - Security Practices of Contractors and Service Providers

Our utility's security practices depend on the people who implement them, including contractors and service providers.

Before outsourcing any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—the company's data security practices will be compared to ours. If possible, visit their facilities.

Security issues for the type of data your service providers handle will be addressed in our contract with them.

Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

Section 10 - Disposal of Sensitive Information

Paper Records

Paper records will be shredded before being placed into the trash.

Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.

Computers and Portable Storage Devices

When disposing of old computers and portable storage devices, use a Department of Defense-compliant disc wiping utility program.

Any compact disc (CD or DVD) will be disposed of by shredding, punching holes in, or incineration.

Section 11 – Additional Information

These websites and publications have more information on securing sensitive data:

National Institute of Standards and Technology (NIST)'s Computer Security Resource Center

www.csrc.nist.gov

NIST's Risk Management Guide for Information Technology Systems

www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Department of Homeland Security's National Strategy to Secure Cyberspace

www.dhs.gov/xlibrary/assets/ National_Cyberspace_Strategy.pdf

SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities

www.sans.org/top20

United States Computer Emergency Readiness Team (US-CERT)

www.us-cert.gov

Carnegie Mellon Software Engineering Institute's CERT Coordination Center

www.cert.org/other_sources

Center for Internet Security (CIS)

www.cisecurity.org

The Open Web Application Security Project

www.owasp.org

Institute for Security Technology Studies

www.ists.dartmouth.edu

OnGuard Online

www.OnGuardOnline.gov