www.hometownconnections.com
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
P — 970 682 4217

Hometown Connections

August 2021

Your Utility Is Required By Law To Establish An Identity Theft Prevention Program

Federal and many state regulations require electric, water, wastewater, and gas utilities to establish an identity theft prevention program. Utilities must have policies and procedures in place to detect, prevent, and mitigate the theft of personal customer information. What does this mean for your community-owned utility? You must evaluate and address all of the ways people can open and access your customer accounts which contain personally identifiable information (PII). Failure to comply with these regulations puts your utility at risk of hefty financial penalties and potential civil lawsuits.

Every utility keeps sensitive personal information within systems and files—names, addresses. Social Security numbers, credit card, and other identifying information. This information is necessary to create accounts, collect payments, and perform other business functions within the utility. However, if sensitive information and data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms.

Compliance Is Necessary. And Easier Than You Think.

Identity theft prevention covers everything from pieces of paper in file cabinets to records in billing systems and software hosted by third-party vendors. However, there's no reason to feel overwhelmed by requirements to keep private the personal information you collect from your customers. Some of the most effective security measures are process and policy changes—limiting access, using strong passwords, locking up sensitive paperwork, training your staff, etc. The changes do not require costly investments. Furthermore, it's cheaper in the long run to invest in better identity information security than to lose the goodwill of your community, defend yourself in legal actions, and face other possible consequences of a records breach.

Information To Protect

You must protect any information that can be used to distinguish or trace an individual's identity. Examples include, but are not limited to:

- Full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including picture, (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Medical or health insurance information protected by health care laws
- Information about an individual that is lined or can be lined to other data (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment data, medical data, education information, financial data)

Yes, Federal Customer Information and Data Regulations Apply to You

For all utilities, prioritizing online security and safeguarding private information are obligations, not options. The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) set standards for protecting consumer information. On November 1, 2007, the FACT Act was amended to include Red Flag guidelines or the Red Flags Rule, for the detection, prevention, and mitigation of identity theft. The Red Flags Rule is enforced by the Federal Trade Commission (FTC) and applies to "financial institutions" and "creditors" with "consumer accounts." **Utilities are considered creditors** because service is extended prior to payment. Furthermore, the FTC defines utilities as creditors maintaining two categories of consumer accounts:

1. Accounts for personal, family, or household purposes involving or designed to permit multiple payments or transactions.
2. Accounts that carry a reasonably foreseeable risk of identity theft.

The Red Flags Rule specifies how businesses and organizations with "consumer accounts" must develop, implement, and administer a written Identity Theft Prevention Program. The Program must include four basic elements that together create a framework to address the threat of identity theft:

1. The Program must include reasonable policies and procedures to recognize red flags of identity theft that may occur in the day-to-day business operations.
2. The Program must be designed to detect the red flags a business has identified. For example, if a business has identified fake IDs as a red flag, procedures must be in place to detect possible fake, forged, or altered identification.
3. The Program must spell out appropriate actions the business will take when red flags are detected.
4. Because identity theft is an ever-changing threat, the business must address how it will periodically re-evaluate the Program to include new risks if applicable.

Federal Fines Add Up Fast

Violations of the Red Flags Rule will result in FTC penalties up to $3,500 maximum in civil fines per violation and up to $2,500 per infraction. This means civil liabilities could easily reach several million dollars. The FTC provides detailed information on the Red Flags Rule.

State Regulations

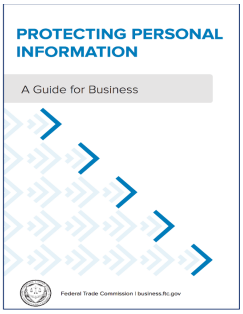
Privacy regulations vary by state, change often, and are becoming more stringent. An increasing number of state laws require measures to protect sensitive information from unauthorized access, destruction, use, modification, or disclosure. Some state laws address the security of health care data, financial or credit information, social security numbers, or other privacy-related data. Your utility's or city's general counsel should check with your state's attorney general for the state requirements.

Developing An Identify Theft Protection Program (ITPP)

The first step to building an effective program for protecting identity information is to review utility and city practices in their entirety. The assessment will indicate the sufficiency of current practices and identify risks and gaps. The resulting Identity Theft Prevention Program (ITPP) should cover ongoing management of the program, outline roles and responsibilities, incorporate policies and procedures, and provide training materials. The ITPP must be an ongoing program, updated, and changed periodically as new Red Flags, risk, or changes to policies and procedures are identified. The following is a sample checklist for conducting an internal risk assessment of policies and procedures related to opening and maintaining account information.

Identity Theft Prevention Program Development Checklist
Identify an Executive Sponsor for the ITPP Program
Identify an Oversight Committee to oversee the ITPP Program that includes representatives from at least 3 key areas or departments
Identify a Core Project Team to conduct risk assessment and manage development and implementation of the ITPP
Define and outline responsibilities for Executive Sponsor, Oversight Committee, and ITPP Core Team
Conduct a Risk Assessment to determine current vulnerability to identity theft, identify current policies/procedures to be incorporated, and identify potential risks and gaps
Write and Identity Theft Prevention Program Plan
Include current policies and procedures in the ITPP and identify any additional policies or procedures to be developed
Develop and implement ongoing reporting, training, and maintenance for program

5 Key Principles of an Identify Theft Protection Program



Given the cost of a security breach—losing your customers' trust, defending yourself against a lawsuit, and paying hefty fines—safeguarding personal information is just plain good business. In a brochure entitled *Protecting Personal Information: A Guide for Business*, the FTC offers 5 key principles for building a sound personal information security plan.

1. **TAKE STOCK**
   Know what personal information you have in your files, on your computers, or entrusted to third-party vendors. Effective data security starts with assessing what information you maintain and who has access to it. Understanding how personal information moves into, through and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities.

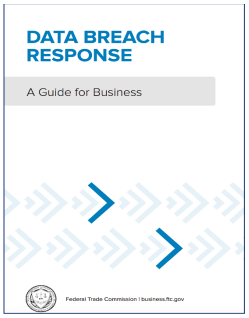
If a third-party vendor hosts your customer information, YOU are responsible for protecting that information from identity theft—not the vendor. Your customer information belongs to you, no matter who manages or processes it. Therefore, you must make sure your vendors comply with your utility's Identity Theft Prevention Program requirements.

2. **SCALE DOWN**
   Keep only what you need. If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it, but keep it secure, with limited access.

3. **LOCK IT**
   Protect the information that you keep. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers. You'll need to follow the best practices for such functions as locking facilities, using firewalls and spam filters, scanning the data network for vulnerabilities, password management, encrypting critical data, limiting access to data, monitoring data security of third parties connected to your system, and training employees to avoid phishing emails and phone calls seeking account information and access codes. Hometown Connections, Inc. and its partners help utilities address all of their security and cyber liability needs. For help deploying comprehensive physical and cybersecurity programs, send an email to info@hometownconnections.com.

4. **PITCH IT**
   Properly dispose of what you no longer need. Shred paper records. When disposing of old computers and portable storage devices, use software for wiping data. Make sure employees who work from home follow the same procedures.

5. **PLAN AHEAD**
   Create a plan to respond to security incidents. Taking steps to protect data can go a long way toward preventing a security breach. Nevertheless, breaches can happen. For guidelines on how to respond to security incidents, consult the FTC's *Data Breach Response: A Guide for Business*.



Given today's threatening security environment, it's vital that you pay attention to protecting the personal information of your customers. Criminals want that information and are skilled at getting it. Federal and state regulators will hold you financially responsible if you don't follow the rules for maintaining a detailed identify theft protection program.

For More Information

Charise M. Swanson
Vice President, Client Services
Hometown Connections, Inc.
m – 719 439 8811
cswanson@hometownconnections.com

Sources

- Cybersecurity Frequently Asked Questions, Hometown Connections, Inc.
- Protecting Personal Information: A Guide for Business Federal Trade Commission, business.ftc.gov
- Data Breach Response: A Guide for Business, Federal Trade Commission, business.ftc.gov

About Hometown Connections, Inc.

Hometown Connections, Inc. is a national, non-profit utility services organization serving community-owned utilities. A single source for many utility products and services, our team of consultants and vendor partners provide affordable and high-quality solutions to help community utilities transform business operations, planning, employee engagement, the customer experience, and much more. Supporting operational and service excellence, all of our services and deliverables are scalable based on the size and objectives of the utility. @HTConnections, Facebook, LinkedIn.

Hometown Connections, AESI-US, Inc., and Marsh USA offer comprehensive cyber and physical security consulting and insurance solutions. Send your inquiry to info@hometownconnections.com for complete information.