Ordinance 2009-1

Identity Theft Prevention Program
For
The City of Lockesburg
Water & Sewer Department
P.O. Box 14
Lockesburg, AR 71846

All utilities are required to comply with the FTC's "Identity Theft Red Flag Rule" even if only nominal information such as name, phone number and address are collected.

City of Lockesburg Water & Sewer Systems Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts are not opened using false information, and measures to respond to such events.

Contact Information:
The Senior Management Person responsible for this program is:
Name: Danny R. Ruth
Title: Mayor
Phone number: (870)289-3261

The Governing Body Members of the System are City Council Members:

1. Boyd Roberts
2. Matthew Webb
3. Steven Hill
4. Claudine Tompkins
5. Phyllis Bettell
6. Charles Nash

Risk Assessment

The City of Lockesburg Water & Sewer Systems has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated.

This risk assessment evaluates how new accounts are opened and the methods used to access the account information. Using this information the City of Lockesburg Water & Sewer Department is able to identify red flags that are appropriate to prevent identity theft.

- New accounts that are opened In Person

- New accounts that are opened via Telephone
- New accounts that are opened via Fax
- Account information that is accessed In Person
- Account information that is accessed via Telephone (Person)
- Account information that is accessed via Telephone (Automated)

Detection (Red Flags):

The City of Lockesburg Water & Sewer Systems adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- Lack of correlation between the SS# range and date of birth
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- SS#, address, or telephone # is the same as that of other customer at utility
- Customer fails to provide all information requested
- Personal information provided is inconsistent with information on file for a customer
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official.

- Ask applicant for additional documentation
- Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify Mayor Danny Ruth immediately.
- Notify law enforcement: The City of Lockesburg Water & Sewer Systems will notify the Sevier County at (870)642-2125 of any attempted or actual identity theft.
- Do not open the account
- Close the account

- Do not attempt to collect against the account but notify authorities

Personal Information Security Procedures

The City of Lockesburg Water & Sewer Systems adopts the following security procedures.

1. Only specifically approved individuals will have possession of keys to anything that the City of Lockesburg Water & Sewer Systems owns..
2. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.
3. Only specifically identified employees with a legitimate need will have keys to the cabinets.
4. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
5. Employees will not leave sensitive papers out on their desks when they are away from their workstations for extended periods of time.
6. Employees store files when leaving their work areas at the end of the work day.
7. Employees log off their computers when leaving their work areas for long periods of time.
8. Employees lock file cabinets when leaving their work areas at the end of the work day.
9. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
10. Visitors who must enter areas where sensitive files are kept must be escorted by an employee.
11. No visitor will be given any entry codes or allowed unescorted access to the office.
12. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different.
13. Passwords will not be shared or posted near workstations.
14. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
15. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
16. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
17. When sensitive data is received or transmitted, secure connections will be used
18. Computer passwords will be required.
19. User names and passwords will be different.
20. Passwords will not be shared or posted near workstations.
21. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
22. When installing new software, vendor-supplied default passwords are changed.
23. The use of laptops is restricted to those employees who need them to perform their jobs.
24. Employees never leave a laptop visible in a car.
25. If a laptop must be left in a vehicle, it is locked in a trunk.

26. The computer network will have a firewall where your network connects to the Internet.
27. Any wireless network in use is secured.
28. Check references or do background checks before hiring employees who will have access to sensitive data.
29. New employees sign an agreement to follow your company’s confidentiality and security standards for handling sensitive data.
30. Access to customer’s personal identify information is limited to employees with a “need to know.”
31. Procedures exist for making sure that workers who leave your no longer have access to sensitive information.
32. Implement a regular schedule of employee training.
33. Employees will be alert to attempts at phone phishing.
34. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
35. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
36. Paper records will be shredded before being placed into the trash.
37. Paper shredders will be available at a designated place in the office.
38. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Review

The City of Lockesburg Water & Sewer Systems Governing Body Members will review and make any changes to the policy yearly unless a risk occurs, at which time the Governing Body with address the problem immediately.

NOW, THEREFORE BE IT ORDAINED THAT THIS ORDINANCE WILL BECOME LAW AND BE SIGNED INTO LAW BY THE VOTE OF THE LOCKESBURG CITY COUNCIL THIS _________________ DAY OF _____________, 2009.

____
Mayor, Danny Ruth

____
Recorder/Treasurer, R. Susie Thompson

(SEAL)