Identity Theft Prevention Program

for

Town of Washington

405 North Washington Street

Washington, LA, 70589

337-826-3626

adopted November 18, 2024

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 were not opened using false information, and measures to respond to such events.

The Town of Washington is governed by the Town of Washington Home Rule Charter. The municipal government provided by the charter is known as the mayor-council form of government. It consists of a legislative and an executive branch of government. The elected town council shall be the legislative branch of government and shall be the governing authority of the Town for purposes of legislation and policy making. The Mayor and his/her department shall comprise the executive department and he shall be the chief executive officer who shall direct the department operations in conformity with the legislation passed by the Council.

Risk Assessment

The Town of Washington 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 evaluated how new accounts were opened and the methods used to access the account information. Using this information the Town was able to identify red flags that were appropriate to prevent identity theft. The following current and past processes were evaluated during the risk assessment to detect possible red flags:

- New accounts opened In Person
- New accounts opened via Fax
- New accounts opened via Web
- Account information accessed In Person
- Account information accessed via Telephone (Person)
- Account information is accessed via Telephone (Automated)
- Account information is accessed via Web Site
- Knowledge of identity theft occurred in the past from someone utilizing a deceased customer's utility account

Detection (Red Flags)

The Town of Washington 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.

- Unexpired Identification documents appear to be altered
- 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)
- 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 in the utility system
- 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 Municipal Clerk and/or Mayor.

- Ask applicant for additional documentation
- Notify immediate supervisor
- Notify law enforcement: The employee will notify the appropriated law enforcement agency of any attempted or actual identity theft.
- Do not open the account
- Disconnect Services and/or Close the account

Personal Information Security Procedures

The Town of Washington adopts the following security procedures:

1. Only employees with a legitimate need will have keys to the business office and filing systems (paper and electronically) which hold all identity information for customers.
2. Employees lock their computers when leaving their work areas.
3. Employees will log off computers when leaving for the day.
4. Employees lock doors when leaving their work areas.
5. Access to offsite storage facilities is limited to employees with a legitimate business need.
6. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
7. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
8. No visitor will be given any entry codes or allowed unescorted access to the office.
9. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. Usernames and passwords will be different. Passwords will be changed at least monthly.
10. Passwords will not be shared or posted near workstations.
11. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
12. The use of laptops is restricted to those employees who need them to perform their jobs.
13. Laptops are stored in a secure place.
14. Laptop users will not store sensitive information on their laptops.
15. Any wireless network in use is secured.

16. Check references or do background checks before hiring employees who will have access to sensitive data.
17. Access to customer's personal identifying information is limited to employees with a "need to know."
18. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
19. Implement a regular schedule of employee training.
20. Employees will be alert to attempts at phone phishing.
21. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
22. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
23. 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.
24. Paper records will be shredded before being placed into the trash.
25. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Town Council. Appropriate employees will be trained on the contents and procedures of this Identity Theft Prevention Program.

1. _____ Date 11/18/24
Beau Wilson, Council Member for District 1

2. _____ Date 11-18-24
Rogers Malveaux, Council Member for District 2

3. _____ Date 11-18-24
Tanya Doucet, Council Member for District 3

4. _____ Date 11-18-24
Mary Lavergne, Council Member for District 4

5. _____ Date 11-18-24
Erick Fontenot, Council Member At-large

A report will be prepared annually and submitted to the mayor-council to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third-party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.