

RESOLUTION NO. 4-2009

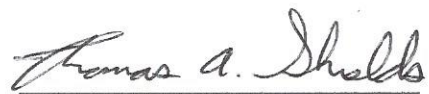
A RESOLUTION OF THE MAYOR AND COUNCIL OF THE CITY OF CLARK FORK,
IDAHO, ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, Section 114 of the Fair and Accurate Transaction Act of 2003 (FACTA) and 12 CFR 41.90 and 41.91 require the City as a utility provider that provides utility services to customers on a credit basis to adopt an Identity Theft Prevention Program to protect the customer;

NOW, THEREFORE, BE IT RESOLVED by the Mayor and Council of the City of Clark Fork, Idaho, that the city hereby adopts the **IDENTITY THEFT PREVENTION PROGRAM** attached as Exhibit "A."

The administrative staff of the City is authorized to take all necessary steps to carry out the Identity Theft Prevention Program provided by this Resolution.

Passed by the Clark Fork City Council the 13th day of April 2009 and approved by the Mayor on the 13th day of APRIL, 2009.


Thomas A. Shields, Mayor

Attest:

Jonell Davisson, City Clerk/Treasurer

CITY COUNCIL MEMBERS	YES	NO	ABSENT	ABSTAIN
Russell W. Schenck	☒	☐	☐	☐
James Junget	☒	☐	☐	☐
Brian L. Cantrell	☒	☐	☐	☐
Linda V. Reed	☒	☐	☐	☐

City of Clark Fork, Idaho

**Identity Theft
Prevention Program**

**City of Clark Fork, Idaho
110 East Third Avenue
Clark Fork, Idaho, 83811**

Identity Theft Prevention Program

for the

Clark Fork Water System

City of Clark Fork

110 East Third Avenue

Clark Fork, Idaho, 83811

City of Clark Fork 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 were not opened using false information, and measures to respond to such events.

Contact Information:

The Senior Person responsible for this program is:

Clark Fork City Mayor

110 East Third Avenue

Clark Fork, ID, 83811

Phone number: 208-266-1315

The Governing Body of the Clark Fork Water System is the Clark Fork City Council

Risk Assessment:

The City of Clark Fork 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 utility was able to identify red flags that were appropriate to prevent identity theft.

- ☐ New accounts opened In Person
 - ☐ New accounts opened via Telephone
 - ☐ New accounts opened via Fax
 - ☐ Account information accessed In Person
 - ☐ Account information accessed via Telephone (Person)
 - ☐ Identity theft occurred in the past from someone falsely opening a utility account
-

Detection (Red Flags):

The City of Clark Fork 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.

- ☐ Fraud or active duty alerts included with consumer reports
- ☐ Notice of credit freeze provided by consumer reporting agency
- ☐ Notice of address discrepancy provided by consumer reporting agency
- ☐ Inconsistent activity patterns indicated by consumer report such as:
 - ☐ Recent and significant increase in volume of inquiries
 - ☐ Unusual number of recent credit applications
 - ☐ A material change in use of credit
 - ☐ Accounts closed for cause or abuse
- ☐ 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)
- ☐ 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 the Mayor.
 - ☐ Notify law enforcement: The City will notify Bonner County Sheriff's Department at 4001 N. Boyer, Sandpoint, Idaho, 208-263-8417 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 Clark Fork City Council adopts the following security procedures:

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Employees log off their computers when leaving their work areas
7. Employees lock file cabinets when leaving their work areas

8. Employees lock file room doors when leaving their work areas
9. Access to offsite storage facilities is limited to employees with a legitimate business need.
10. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
11. No visitor will be given any entry codes or allowed unescorted access to the office.
12. 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.
13. Passwords will not be shared or posted near workstations.
14. Anti-virus and anti-spyware programs will be run on individual computers and on servers weekly.
15. When sensitive data is received or transmitted, secure connections will be used
16. The computer network will have a firewall where your network connects to the Internet.
17. Any wireless network in use is secured.
18. Do background checks before hiring employees who will have access to sensitive data.
19. Access to customer’s personal identify information is limited to employees with a “need to know.”
20. Employees will be alert to attempts at phone phishing.
21. Employees are required to notify the Mayor 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. Paper records will be shredded before being placed into the trash.
24. Paper shredders will be available in the office, next to the photocopier.
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 Clark Fork City Council on this _____ th day of _____, 2009. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Council Members:

Russell W. Schenck

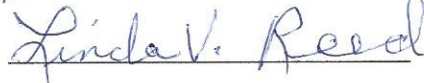


James J. Junget

Brian L. Cantrell



Linda V. Reed



Thomas A. Shields, Mayor

Attest:



Jonell Davisson, City Clerk/Treasurer

A report will be prepared annually and submitted to the Clark Fork City 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.