IDENTITY THEFT PREVENTION POLICY - PROGRAM

FOR

CITY OF WINNEMUCCA SEWER/WATER DEPARTMENTS

90 WEST FOURTH ST.
WINNEMUCCA, NV 89445
10.15.08

CITY OF WINNEMUCCA SEWER/WATER DEPARTMENTS IDENTITY THEFT PREVENTION POLICY - PROGRAM

This policy-program is intended to identify red flags that will alert City 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 management personnel responsible for this policy-program is:

Eddy D. Davis
City Clerk / Treasurer
(775) 623-6338
wmcaedd@winnemuccacity.org

The governing body members of the City are:

Mayor and Council Members:
Mayor Di An Putnam
Councilman Richard Stone
Councilman Doug Cain
Councilman Joyce Sheen
Councilman Patty Herzog
Councilman Don Stoker

RISK ASSESSMENT

The City of Winnemucca Sewer and Water Departments (the "City") have 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 (person)
- New accounts opened via fax

DETECTION (RED FLAGS)

The City 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.

- 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
- Application appears altered or destroyed and reassembled
- Other information provided by applicant/customer is inconsistent with information on file
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a known 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, or expired form of identification used)
- 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 City 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 City Clerk/Treasurer.

- Ask applicant for additional documentation
- Notify internal manager: Any City employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identify must notify the City Clerk/Treasurer
- Notify law enforcement: The City will notify the Winnemucca Police Department at 775-623-6397 of any attempted or actual identify 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 adopts the following security procedures:

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.
2. Only specifically identified employees with a legitimate need or job function will have keys to the locked file cabinets.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees log off their computers when leaving their work areas.
5. Employees will lock file cabinets when leaving their work areas.
6. Employees will lock file room doors when leaving their work areas.
7. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
8. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
9. No visitor will be given any entry codes or allowed unescorted access to the office.
10. Access to sensitive information on a computer will be controlled by using passwords. User names and passwords will be different for each employee.
11. Passwords will not be shared or posted near workstations.
12. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
13. Email transmissions of utility billing information to statement mailer vendor will be encrypted as they contain personal identifying information on each customer.
14. Anti-virus and anti-spy ware programs will be run on individual computers and on servers daily.
15. When sensitive data is received or transmitted, secure connections will be used.
16. The use of laptops is restricted to those employees who need them to perform their jobs.

17. Laptop users will not store sensitive information on their laptops.
18. Employees will never leave a laptop visible in a vehicle, a hotel luggage stand, or packed in checked luggage at the airport.
19. If a laptop must be left in a vehicle, it is locked in the trunk.
20. The computer network will have a firewall where the network connects to the Internet.
21. Any wireless network in use is secured.
22. Access to customer's personal identity information is limited to employees on a "need to know" basis.
23. Procedures exist for making sure that workers who leave your employ or transfer to another part of the entity no longer have access to sensitive information.
24. Employees will be alert to attempts at "phone phishing".
25. Employees are required to notify the City Clerk/Treasurer immediately if there is a potential security breach, such as a lost or stolen laptop.
26. Employees who violate security policy are subject to discipline, up to, and including, dismissal.
27. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of data.
28. Paper records will be shredded as appropriate.
29. A paper shredder is available in the immediate City Clerk/Treasurer office area.

IDENTITY THEFT PREVENTION POLICY – PROGRAM REVIEW AND APPROVAL

This plan has been reviewed and adopted by the Winnemucca City Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Policy-Program.

NOTE:

A report will be prepared annually and submitted to the City Council to include matter related to the program, the effectiveness of the policy 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 policy-program, if any.