RESOLUTION 2008-23

WHEREAS, the City of Gothenburg Public Works Division is a retail seller of electricity, water, and sewer services to residential and commercial customers in Gothenburg, Nebraska; and

WHEREAS, Public law 108-159 went into effect on December 4, 2003 and amends the Fair Credit Reporting Act; and

WHEREAS, such amendment, known as the *FACT Act*, requires creditors, including utility companies, to comply with the *Act* no later than November 1, 2008; and

WHEREAS, the City of Gothenburg Public Works Division is, as defined under 15 U.S.C §1681a (r) (5), a creditor that maintains and offers accounts for which there is a reasonably foreseeable risk of identity theft; and

WHEREAS, compliance with the *Act* requires a creditor to create and implement a written Identity Theft Prevention Program;

NOW, THEREFORE, BE IT RESOLVED, by the Mayor and City Council of the City of Gothenburg, Nebraska that the Council hereby adopts the "City of Gothenburg Identity theft Prevention Program" which is attached to this Resolution as Appendix A.

BE IT FURTHER RESOLVED by the Mayor and City Council that said Program is appropriate to the size and complexity of the City of Gothenburg Public Works Division and the scope of its activities; and that the Program is reasonably calculated to identify and detect relevant Red Flags indicating a potential risk of identity theft, and includes appropriate responses to such Red Flags that will mitigate and prevent identity theft.

BE IT FURTHER RESOLVED by the Mayor and City Council that appropriate staff appointed by the Mayor and Council to design and implement the Program shall report annually to the Mayor and Council, or to a senior employee appointed by the Mayor and Council, on the Public Works Division's compliance with CFR §681.2 as required by the Act.

BE IT FURTHER RESOLVED by the Mayor and City Council of the City of Gothenburg, Nebraska that the Council or a senior employee appointed by the Mayor and City Council will review the Program from time to time in order to update policies as needed, in order to reflect changes in risks to City of Gothenburg Public Works Division's customers.

Passed and approved this 21st day of October, 2008.

Joyce Hudson, Mayor

Connie L. Dalrymple, City Clerk

City of Gothenburg Public Works

Identity Theft Prevention Program

Implemented as of November 1, 2008

I. INTRODUCTION

The City of Gothenburg Public Works Division (the "Utility") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. 16 C. F. R. § 681.2. This Program is designed to detect, prevent and mitigate Identity Theft in connection with the opening and maintenance of certain utility accounts. For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The accounts addressed by the Program, (the "Accounts"), are defined as:

1. An account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

This Program was developed with oversight and approval of the Governing Body of the City of Gothenburg. After consideration of the size and complexity of the Utility's operations and Account systems, and the nature and scope of the Utility's activities, the Governing Body determined that this Program was appropriate for the City of Gothenburg Public Works Division, and therefore approved this Program on October 21, 2008; to be implemented November 1, 2008.

II. IDENTIFICATION OF RED FLAGS.

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the Utility considered the types of Accounts that it offers and maintains, the methods it provides to open its Accounts, the methods it provides to access its Accounts, and its previous experiences with Identity Theft. The Utility identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings From Consumer Reporting Agencies.
   Not applicable – Do not use consumer reporting agencies.

B. Suspicious Documents.
   a. Receiving documents that are provided for identification that appear to be forged or altered.
   b. Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged)
   c. Receiving an application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information.
   a. Customer provides identifying information inconsistent with (1) information provided by any external source of information, (2) information on file, or (3) other information the customer provides;

b. Customer's identifying information is the same as shown on other documents found to be fraudulent;
c. Customer's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address; Customer's address or phone number is the same as that of another person)
d. A person fails to provide complete personal identifying information on an application when reminded to do so; and
e. A person's identifying information is not consistent with the information that is on file for the customer.

D. Unusual Use Of or Suspicious Activity Related to an Account.
a. Customer calls wishing to alter account information;
b. Mail sent to the account holder is repeatedly returned as undeliverable;
c. Utility receives notice that an account has unauthorized activity;
d. Employees with access to computer billing system refuses to sign confidentiality agreement, which is required of all employees with access;
e. Member of personnel breaches applicable policy regarding confidentiality of customer information;
f. Suspicious or unusual personnel action is displayed during log-in time to the billing system;
g. Unauthorized access to or use of customer account information; and
h. Utility's computer system is breached such that a customer's personal information has become accessible.

E. Notice regarding possible identity theft.
a. The Utility receives notice from a customer, an identity theft victim, law enforcement or any other person that is has opened or is maintaining a fraudulent Account for a person engage in Identity Theft.

III. DETECTION OF RED FLAGS.

In order to detect any of the Red Flags identified above with the opening of a new Account, Utility personnel will take the following steps to obtain and verify the identity of the person opening the Account:

A. The Utility requires name, address, last four digits of social security number, birth date, place of employment and contact phone numbers.

In order to detect any of the Red Flags identified above for an existing Account, Utility personnel will take the following steps to monitor transactions with an Account:

A. Verify the identification of customers if they request information or to change billing information whether in person, via telephone, via facsimile, or by e-mail.
B. Verify changes in banking information given for billing and payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT.

In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Continue to monitor an Account for evidence of Identity Theft;
B. Contact the customer;
C. Change passwords that permit access to Accounts;
D. Reopen an Account with a new number;
E. Not opening an new Account;
F. Closing an existing Account;
G. Notifying law enforcement;
H. Determining no response is warranted under the particular circumstances;
I. Notifying the Program Administrator for determination of the appropriate steps to take.

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures:

A. Ensure that office computers are password protected and that computer screens lock after a set period of time.

V. UPDATING THE PROGRAM AND THE RED FLAGS

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. At least once per year, the Program Administrator will consider the Utility's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator may adopt the changes in order to ensure the effectiveness of the program.

VI. PROGRAM ADMINISTRATION.

A. Oversight.
The Utility's Program will be overseen by a Program Administrator. The Program Administrator shall be the Gothenburg City Clerk. The Program Administrator will be responsible for the Program's administration, for

ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

B. Staff Training.
Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements.
In the event the Utility engages a service provider to perform an activity in connection with one or more Accounts, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.
   a. Requesting that service providers review the Utility's Program and report any Red Flags to the Program Administrator.