City of Garnavillo

Financial Policy

Subject: Identity Theft Prevention Program	**Approved By:** City Council
Resolution Number: 2008-26	**Effective Date:** 10/14/2008
Resolution Number:	

PURPOSE

The purpose of this policy is to update the 2008 Identity Theft Prevention Program adopted by Resolution 2008-26.

INTRODUCTION

The purpose of this policy is to establish an Identity Theft Prevention Program ("Program") for all departments of the City of Garnavillo designed to detect, prevent and mitigate identity theft in connection with the opening and maintenance of a covered account and to provide continued administration of the Program in compliance with the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACTA) 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 accounts: 1. Utility 2. Accounting. 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. *Utility Accounts* – A utility account offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. *Vendor Accounts Payable/Receivable Account* – Vendor Accounts Payable/Receivable Accounts maintain individual and business information for which there is a reasonably foreseeable risk to the vendor or to the safety and soundness of the vendor from Identity Theft.

This Program was originally developed with the oversight and approval of the Garnavillo City Council. After consideration of the size and complexity of the Utility's activities, the Garnavillo City Council determined that this Program was appropriate for the City of Garnavillo Utility Department on October 14, 2008.

This Program was reviewed and updated with the oversight and approval of the Garnavillo City Council to include Utility and Vendor Accounts. The Garnavillo City Council determined that the updates were appropriate for the City of Garnavillo on _____, 2021.

DEFINITIONS

Account means a continuing relationship established by a person with the City to obtain services for personal, family, household or business purposes and includes an extension of credit, such as the purchase of services involving a deferred payment.

Covered account means:

1. An account the City offers or maintains primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include utility billing; and
2. Any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft, including financial, operational, compliance, reputation or litigation risks.

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

1. Name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration Page 2 number, government passport number, employer or taxpayer identification number;
2. Medicare number;
3. Member identification number; or
4. Claim number

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

PROGRAM

The City establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft.

The Program shall include reasonable policies and procedures to:

1. Identify relevant Red Flags for covered accounts it offers or maintains and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;

3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the customers form identity theft

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 City 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 City identifies the following Red Flags, in each of the listed categories:

1. Suspicious Documents:
    a. Receiving documents that are provided for identification that appear to be forged or altered
    b. Receiving documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation.
    c. 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)
    d. Receiving an application for service that appears to have been altered or forged.
2. Suspicious Personal Identifying Information:
    a. A person's identifying information is inconsistent with other sources of information (such as a SSN that was never issued)
    b. A person's identifying information is inconsistent with other information the customer proves (such as inconsistent SSNs or birth dates)
    c. A person's identifying information is the same as shown on other applications found to be fraudulent
    d. A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address.
    e. A person's SSN is the same as another customer's SSN
    f. A person's address or phone number is the same as that of another person
    g. A person fails to provide complete personal identifying information on an application when reminded to do so
    h. A person's identifying information is not consistent with the information that is on file for the customer.
3. Unusual Use Of or Suspicious Activity Related to an Account.
    a. A change of address for an Account followed by a request to change the Account holder's name

   b. An account being used in a way that is not consistent with prior use (such as late or no payments when the Account has been timely in the past)
   c. Mail sent to the Account holder is repeatedly returned as undeliverable
   d. The City receives notice that a customer is not receiving his paper statements
   e. The City receives notice that an Account has unauthorized activity.
4. Notice Regarding Possible Identity Theft
   a. The City receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

DETECTION OF RED FLAGS

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

1. Require certain identifying information such as name, date of birth, residential or business address, SSN, photo identification or other identification
2. Verifying the customer's identity, such as copying and reviewing a driver's license or other identification card
3. Reviewing documentation showing the existence of a business entity
4. Independently contacting the customer.

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

1. Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email)
2. Verifying the validity of requests to change billing addresses
3. Verifying changes in banking information given for billing and payment purposes

PREVENTING AND MITIGATING IDENTITY THEFT

In the event City 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:

1. Continue to monitor an Account for evidence of Identity Theft
2. Contacting the customer
3. Changing any passwords or other security devices that permit access to Accounts
4. Reopening an Account with a new number
5. Not opening a new Account
6. Closing an existing Account

7. Notifying law enforcement
8. Notifying the Program Administrator for determination of the appropriate step(s) to take

In the event that the City receives notice that its system has been compromised so that a customer's personal information has become accessible, the City will notify the customer as soon as possible and take immediate steps to change passwords. If the City receives notice that a person has provided inaccurate identification information, the Account in question will be closed and law enforcement contacted.

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

1. Providing a clear notice on any website established for the City that the website is or may not be secure
2. Ensuring complete and secure destruction of paper documents and computer files containing customer information
3. Ensuring that office computers are password protected and that computer screens lock after a set period of time

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 City from Identity Theft. At least every year the Program Administrator will consider the City'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 City maintains and changes in the City'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 will present the City Council with recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

PROGRAM ADMINISTRATION

1. *Oversight.*
   The City's Program will be overseen by a Program Administrator shall be the City and Sewer Committee as appointed by the Mayor. The Program Administrator will be responsible for the Program's administration for ensuring appropriate training of City staff on the Program, for reviewing a 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.

2. *Staff Training and Reports.*
   City 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.
3. *Service Provider Arrangements.*
   In the event the City engages a service provider to perform an activity in connection with one or more Accounts, the City 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. Require, by contract, that service providers have such policies and procedures in place
   b. Require, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator.

_____
Chad Schmelzer, Mayor

Attest:

_____
Melissa Atkinson, City Administrator/Clerk