CITY OF ELK CITY

IDENTITY THEFT PREVENTION POLICY

PURPOSE

Identity theft, the fraudulent use of an individual's personal identifying information, is a high-level risk to consumers and therefore to our city and our customers. This policy reaffirms and formalizes the actions and processes our city will take with respect to identity theft.

This policy includes the final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act.

The rules implementing section 114 require each creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or existing covered accounts.

In addition, the agencies issued joint rules under section 315 that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

The agencies also issued guidelines to assist creditors in the formulation and maintenance of a Program that satisfies the requirements of these rules.

OBJECTIVES

The guidance and standards set forth in this policy are intended to take specific steps to:

- Comply with the "Interagency Final Rule Regarding Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003".
- Minimize the threat of identity theft through disclosure or compromise of customer information held by the city.
- Respond to known or suspected identity theft involving our city or its customers.
- Provide assistance to city customers who may have been victims of identity theft.
- Establish processes or procedures for the training of city personnel.
- Establish processes or procedures for the education of city customers.

DEFINITIONS

For the purposes of this policy, the following definitions apply:

Creditor means

- Any person or firm who regularly extends, renews, or continues credit
- Any person or firm who regularly arranges for the extension, renewal or continuation of credit, or
- Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Account means a continuing relationship established by a person with the city to obtain a product or service for personal, family, household or business purposes. Account includes:

- An extension of credit, such as the utility billing (water, electricity, sewer, garbage and internet) involving a deferred payment, and
- A deposit account.

Covered Account means:

- An account that our city offers or maintains primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions such as utility billing (water, electricity, sewer, garbage and internet) or the purchase of property.
- Any other account that our 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.
- This definition may include accounts established for business purposes and covers any relationship the account holder has with the city, including deposit relationships, utility relationships, and include fiduciary, agency, custodial, and other advisory relationships.

Customer means a person that has a covered account with the city. This includes not only consumers but also other types of persons for which our city believes there is a reasonably foreseeable risk to its customers or to the city's safety and soundness from identity theft.

Clear and conspicuous means reasonably understandable and designed to call attention to the nature and significance of the information presented.

Identity Theft means a 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:

- Name, social security number, date of birth, official state or governmental issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device.

Notice of address discrepancy means a notice sent to a user by a consumer reporting agency pursuant to the law that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

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

Service Provider means a person that provides a service directly to the city.

ELEMENTS OF THE IDENTITY THEFT PREVENTION PROGRAM

- Identify relevant red flags and incorporate them into the Program
- Detect red flags that are part of the Program
- Respond appropriately to any red flags that are detected
- Ensure the Program is updated periodically to address changing risks.

GUIDELINES OF THE IDENTITY THEFT PREVENTION PROGRAM

- Incorporate all existing anti-fraud policies and procedures into the Program.
- Program to be approved by the Elk City Commission, Elk City Public Works Authority, Elk City Industrial Authority and Elk City Airport Authority
- Ensure oversight of the Program by the City Manager, City Treasurer and City Clerk
- Train appropriate staff
- Oversee any service provider arrangements made

ADMINISTRATION OF THE IDENTITY THEFT PREVENTION PROGRAM

- The city's Identity Theft Prevention Program will be administered by the City Clerk.
- The Program will be monitored at least annually.
- Service provider's activities will be conducted in accordance with the city's Program.

REPORTING REQUIREMENTS

- The City Manager will make a report to the Elk City Commission, the Elk City Public Works Authority, the Elk City Industrial Authority and the Elk City Airport Authority at least on an annual basis.
- Significant incidents involving identity theft will be reported as they happen.
- The Program will be reviewed and critiqued to determine the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the city's covered accounts.
- All service providers' activities will be conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

IDENTIFICATION OF COVERED ACCOUNTS INCLUDING A RISK ASSESSMENT

The city performed an initial risk assessment of the likelihood that we offer covered accounts taking into consideration:

- The types of covered accounts that we offer
- The methods we use to open accounts
- The methods we use to provide access to our accounts
- Previous experiences with identity theft

To assist us in this process, we used the illustrative examples of Red Flags that are contained in the FACT Act.

PERIODIC UPDATES OF THE IDENTITY THEFT PREVENTION PROGRAM

The city will review its existing, Identity Theft Prevention Program at least annually and make such revision and amendments, as it deems appropriate to reflect changes in risks to customers and to the safety and soundness of the city from identity theft.

STAFF TRAINING

Our staff will be trained to recognize and properly react to unauthorized or fraudulent attempts to obtain customer information. Employees will also be trained to protect customer information through appropriate measures, such as taking additional steps to verify that a caller is a bona fide customer.

Employees will also be trained to implement the city's written policies and procedures governing the disclosure of customer information, and will be informed and reminded on a periodic basis not to deviate from them. Moreover, employees must also know to whom and how they should report suspicious activity.

OVERSIGHT OF SERVICE PROVIDERS

The City will adopt and implement an information security program that establishes adequate administrative, technical and physical safeguards to protect customer information against misuse, alteration, destruction, or unauthorized disclosure. The City will perform due diligence on service providers and will require that all contracts with service providers, who have access to customer non-public personal information in the course of providing services to our city, have a clause that requires the provider to maintain an information security program designed to achieve these objectives.

PREVENTION AND DETERRENCE OF IDENTITY THEFT

Our city will employ a variety of methods to safeguard customer information and reduce the risk of loss from identity theft, including:

- Verification of personal information to establish the identity of individuals applying for new or addition services.
- Consumer reports can be an important source for preventing fraud. When processing an application for a new account, the city may rely on a consumer report from a consumer reporting agency. Our city will not process an application when there is an existing fraud alert without contacting the individual in accordance with instructions that usually accompany a fraud alert (i.e., a victim's statement), or otherwise employing additional steps to verify the individual's identity. Consumer reports may also be a source for detecting fraud. Signs of possible fraudulent activity that may appear on consumer reports may include late payments on a consumer's accounts in the absence of a previous history of late payments, numerous credit inquiries in a short period of time, higher-than-usual monthly credit balances, and a recent change of address in conjunction with other signs. The city will institute procedures to share a fraud alert across our various lines of business.
- When an applicant fails to provide all requested information on an application, our city will not process the incomplete application without further explanation.
- Inasmuch as a change of address request on an existing account may be a sign of fraudulent activity, our city will verify the customer information before executing an address change.
- Our city will implement appropriate controls and procedures to limit access to customer records. We will also ensure that our service providers adopt similar controls.
- Because insiders could be identity thieves, our city will consider conducting background checks for its employees, in accordance with applicable law.
- Our city will also monitor its service providers to confirm that they have implemented appropriate measures to limit access to customer records.
- Appropriate protective measure will also be taken for disclosing information through other communication channels (e.g., e-mail or wireless devices) which our city may use. It is our policy that in most cases e-mail is not an appropriate

channel to communicate certain types of account information unless it is secure e-mail.

- Our city will implement appropriate controls and procedures to limit access to customer records which are to be destroyed by shredding. We will also ensure that our service providers adopt similar controls.

RESPONSE TO SUSPECTED IDENTITY THEFT SCHEMES

In order to properly respond to instances of suspected identity theft, we will:

- Incorporate notification of known email-related frauds into the response program to alert customers of fraudulent requests for information and to caution them against responding.
- Notify Internet service providers, domain name issuing companies, and law enforcement to shut down fraudulent Web sites and other Internet resources that are being used to facilitate phishing or other fraudulent e-mail practices.
- Increase suspicious activity monitoring and employ addition identity verification controls.
- If fraud is detected in connection with customer accounts, we will report the fraud and offer our customers assistance consistent with regulatory guidance on this subject.
- In the event that our city is a victim of an email-related scam, we will promptly notify law enforcement by filing a Suspicious Activity Report (SAR).

RESPONSE PROGRAM FOR KNOWN IDENTITY THEFT

The city will take all necessary steps to prevent unauthorized access to or use of sensitive customer information. Sensitive customer information includes the customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, and their credit or debit card number. It also includes any combination of customer information that would allow someone to log on or access a customer's account, such as the user name and personal identification number (PIN) or password.

In the event that sensitive customer information is accessed or used, the city will:

- Assess the nature ad the scope of the incident and identify what customer information systems and types of customer information have been misused or accessed;
- Notify our law enforcement and file a SAR as the city becomes aware of the incident;
- Promptly notify the appropriate law enforcement authorities when a reportable violation is ongoing;
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information;
- Notify customers of the incident.

INCIDENT INVOLVING A SERVICE PROVIDER

The City will notify our customers and when an incident of unauthorized access to sensitive customer information involves our customer information systems maintained by a service provider. The city may, however, elect to authorize or contract with the service provider to notify our customers on our behalf.

CUSTOMER NOTICE OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION

The City will notify customers when we become aware of an incident of unauthorized access to customer information and at the conclusion of our investigation if the city determines that misuse of information has occurred or the city believes it is reasonably possible that misuse will occur.

The customer notice will be given in a clear and conspicuous manner and will be delivered in a manner designated to ensure that a customer can reasonably be expected to receive it. Acceptable methods that the city will use include telephone and mail. E-mail notices are acceptable for those customers who have valid e-mail addresses and who have agreed to receive communications with the city electronically.

The notice will contain the following items:

- Description of the incident;
- Type of information subject to unauthorized access;
- Measures taken by the city to protect customers from further unauthorized access;
- Contact information for the nationwide consumer reporting agencies;
- Telephone number customers can call for information and assistance; and
- A reminder to customer to remain vigilant over the next twelve to twenty four months and to report any suspected identity theft incidents to the city.

EDUCATION OF CUSTOMERS

Educating consumers about preventing identity theft and identifying potential pretext calls may help reduce their vulnerability to these fraudulent practices. We will make available to our customers, brochures in our lobbies or on our Web site, describing preventative measures consumers can take to avoid becoming victims of these types of fraud.

ASSISTANCE FOR VICTIMS

In the event that one of our customers becomes a victim of identity theft, we will take the following steps, as appropriate, to assist them:

- Have trained personnel respond to customer calls regarding identity theft or pretext calling.
- Determine if it is necessary to close the account immediately after a customer reports unauthorized use of that account. Where a customer has multiple accounts with us, we will assess whether any other account has bee the subject of potential fraud.
- Help educate the customer about appropriate steps to take if they have been victimized.

INDEPENDENT TESTING

Periodic unannounced independent testing will be conducted to ensure that city personnel are aware of and abiding by this policy. This testing will include in its activities testing to determine if any city customers have been the victims of ID theft and, if so, where the city took the proper steps thereafter. In addition, this testing will focus on additional modifications that should be made to the city's identity theft prevention program.

REVIEW OF POLICY

The Elk City Commission, Elk City Public Works Authority, Elk City Industrial Authority, and the Elk City Airport Authority shall review this policy at least annually, making such revisions and amendments, as is deemed appropriate.

ALERTS, NOTIFICATIONS, OR OTHER WARNINGS RECEIVED

The City Will:

- Verify identity of the customer.
- Authenticate customer's information.
- Monitor transactions on the customer's accounts.
- Verify validity of address changes or changes in personal information.

Requirement to Form a Reasonable Belief

Whenever our city receives an alert, notification, or other warning of address discrepancy from a consumer reporting agency that has a substantial difference between the address the city submitted to the consumer reporting agency and the address(s) in the agency's file for the consumer, the city will take steps to form a reasonable belief that the consumer report relates to the consumer about whom the city requested the report.

In order to develop a reasonable belief that the consumer report relates to the consumer about whom we requested a report, we will compare the information in the consumer report provided by the consumer reporting agency with information that the city;

- Obtained and used to verify the consumer's identity;

- Maintains in our records, such as applications, change of address notifications, other customer account records; (or)
- Obtained from a third-party source(s);
- In addition, the city will verify the information in the consumer report provided by the consumer reporting agency with the customer.

Requirement to Furnish a Consumer's Address to a Consumer Reporting Agency

The city will furnish an address for the consumer that the city has reasonably confirmed is accurate to the consumer reporting agency from whom the city received the notice of address discrepancy whenever the city can form a reasonable belief that the consumer report relates to the consumer about whom the city requested the report.

The city will furnish this information if the city establishes a continuing relationship with the consumer and if the city regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

Examples of confirmation methods that may be used by the city are:

- Verification of the address with the consumer about whom it has requested the report, or
- Review of its records to verify the address of the consumer, or
- Verification of the address through third-party sources; or
- Use of other reasonable means.

Timing

The city will furnish the consumer's address that the city has confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which the city established a relationship with the consumer.

DUTIES REGARDING CHANGES OF ADDRESS

The city will assess the validity of a change of address if it receives notification of a change of address for a consumer's account.

Form of Notice

Any written or electronic notice that the city provides under this paragraph will be clear and conspicuous and provided separately from its regular correspondence with the consumer.

SUSPICIOUS DOCUMENTS

- Documents provided for identification which appear to be altered

- Personal information provided that is inconsistent with external information sources
- Unusual use of the account in a manner that is not consistent with historical patterns of activity
- Notice from customer of unauthorized charges or use

APPROPRIATE RESPONSES TO RED FLAGS

- Monitor accounts
- Contact customer
- Change passwords or sign ons
- Refuse to open an account
- Don't collect on an account
- Notify law enforcement as deemed appropriate
- No response