RESOLUTION _____

A RESOLUTION ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM AS REQUIRED BY THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003.

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 utilities, to comply with the Act no later than November 1, 2008; and

WHEREAS, the City of Lexington is, as defined under 15 U.S.C. Section 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; and

WHEREAS, that said Identity Theft Prevention Program is appropriate to the size and complexity of the City of Lexington and the scope of its activities, that the Program is reasonably calculated to identify and detect relevant Red Flags indicating a potential risk of identity theft, and that the Program includes appropriate responses to such Red Flags that will mitigate and prevent identity theft.

NOW, THEREFORE, BE IT RESOLVED by the Mayor and Council of the City of Lexington, Nebraska, that the attached City of Lexington Identity Theft Prevention Program is hereby adopted.

PASSED AND APPROVED THIS 28TH DAY OF OCTOBER, 2008.

City of Lexington, NEBRASKA

_____

John Fagot, Mayor

ATTEST:

_____

Deputy City Clerk, Pamela Berke

City of Lexington, Nebraska

Identity Theft Prevention Program

Implemented as of November 1, 2008

I. INTRODUCTION

The City of Lexington, Nebraska including Lexington Utilities System, (the "City") 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 and other credit 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 City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; 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.

This Program was developed with oversight and approval of the City Council. After consideration of the size and complexity of the City's operations and Account systems, and the nature and scope of the City's activities, the City Council determined that this Program was appropriate for the City of Lexington, and therefore approved this Program on October 28, 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 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:

A. Notifications and Warnings from Consumer Reporting Agencies.

Possible Red Flags for this category include:

1) Receiving a report or notice from a consumer reporting agency of a credit freeze;
2) Receiving a report of fraud with a consumer group; and
3) Receiving indication from a consumer report of activity that is inconsistent with a customer's usual pattern of activity.

B. Suspicious Documents.

Possible Red Flags for this category include:

1) Receiving documents that are provided for identification that appear to be forged or altered;
2) Receiving documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;
3) 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); and
4) Receiving an application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information.

Possible Red Flags for this category include:

1) A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a consumer report or a SSN that was never issued);
2) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent SSNs or birth dates);
3) A person's identifying information is the same as shown on other applications found to be fraudulent;
4) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5) A person's SSN is the same as another customer's SSN;
6) A person's address or phone number is the same as that of another person;
7) A person fails to provide complete personal identifying information on an application when reminded to do so; and
8) 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.

Possible Red Flags for the category include:

1) A change of address for an Account followed by a request to change the Account holder's name;
2) 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);
3) Mail sent to the Account holder is repeatedly returned as undeliverable;
4) The City receives notice that a customer is not receiving his paper statements; and
5) The City receives notice that an Account has unauthorized activity.

E. Notice regarding possible identity theft.

Red Flags for this category include:

1) 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.

III. 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:

Steps can include:
1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, SSN, driver's license or other identification;
2) Verifying the customer's identity, such as by copying and reviewing a driver's license or other identification card;
3) Reviewing documentation showing the existence of a business entity; and
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:

Steps can include:
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; and
3) Verifying changes in banking information given for billing and payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event City personnel detects 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:

Steps can include:
1) Continue to monitor an Account for evidence of Identity Theft;
2) Contact the customer;
3) Change any passwords or other security devices that permit access to Accounts;
4) Reopen an Account with a new number;
5) Not open a new Account;
6) Close an existing Account;
7) Notify law enforcement;
8) Determine that no response is warranted under the particular circumstances; or
9) Notify the Program Administrator (as defined below) for determination of the appropriate step(s) to take.

In order to further 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:

Possible steps may include:
1) Provide a secure website or clear notice that a website is not secure;
2) Ensure complete and secure destruction of paper documents and computer files containing customer information;
3) Ensure that office computers are password protected and that computer screens lock after a set period of time; and
4) Require only the last 4 digits of SSNs on customer applications.

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 City from Identity Theft. At least annually, the Program Administrator will consider the City's experiences with Identity Theft situations, 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 his or her recommended changes and the City Council will make a determination of whether to accept, modify, or reject those changes to the Program.

VI. PROGRAM ADMINISTRATION

A. Oversight.

The City's Program will be overseen by a Program Administrator. The Program Administrator shall be the City's Finance Director. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of City 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 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.

C. 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.

Possible steps may include:

1) Requiring, by contract, that service providers have such policies and procedures in place;
2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator.