SCANNED
2-20-09
CB

RESOLUTION NO. 2009-03

A RESOLUTION ADOPTING IDENTITY THEFT PREVENTION PROGRAM AS MANDATED BY FEDERAL TRADE COMMISSION

NOW, THEREFORE, BE IT ORDAINED BY THE GOVERNING BODY OF THE CITY OF BASEHOR, KANSAS, AS FOLLOWS:

Section 1. The attached Identify Theft Prevention Program is hereby adopted by the City.

Section 2. This Resolution will become effective upon its adoption by the Governing Body.

ADOPTED February 17, 2009.

CITY OF BASEHOR, KANSAS

Mayor, Chris Garcia

(SEAL)

SEAL OF THE CITY OF BASEHOR, KANSAS
CORPORATE
SEAL

ATTEST:

City Clerk, Mary A. Mogle

APPROVED AS TO FORM:

Patrick G. Reavey, City Attorney

BASEHOR

Identity Theft Prevention Program

Implemented as of February 17, 2009

I. INTRODUCTION

The City of Basehor (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 city 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, they determined that this Program was appropriate for the City of Basehor, and therefore approved this Program on February 17, 2009.

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. Suspicious Documents.

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.

B. Suspicious Personal Identifying Information.

1) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent SSNs or birth dates);
2) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
3) A person's identifying information is the same as shown on other applications found to be fraudulent;
4) A person's SSN is the same as another customer's SSN;
5) A person's address or phone number is the same as that of another person;
6) A person's identifying information is not consistent with the information that is on file for the customer; and
7) A person fails to provide complete personal identifying information on an application when reminded to do so.

C. Unusual Use Of or Suspicious Activity Related to an Account.

1) The City receives notice that there has been unauthorized access to or use of customer Account Information; and
2) The City receives notice that there has been unauthorized access to the City's plans to take steps with certain data it maintains that contains customer information (i.e. destroying computer files.)

D. Notice Regarding Possible Identity Theft.

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:

1) Requiring certain identifying information such as name, date of birth, residential or business address, and 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.

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 changes in banking information given for billing and payment purposes.
2) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);
3) Verifying the validity of requests to change billing addresses;
4) Do not share identity and banking information with anyone including the customer; require them to give the information and verify with the information on the account.

IV. 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) Continuing 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) Notifying law enforcement.

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:

1) Ensuring complete and secure destruction of paper documents and computer files containing customer information;
2) Ensuring 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 City from Identity Theft. At least annually, the Utility Clerk 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 City Finance Officer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the City Administrator will present the City Council with their 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: Utility Clerk.

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.