Hutchinson City Council Policy - 21

SUBJECT: IDENTITY THEFT PREVENTION

DATE: July 21, 2009

Introduction

The City of Hutchinson, Kansas (the "City") developed this Identity Theft Prevention Policy ("Policy") 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 & 15 USCA § 1681c(h).

This Policy was developed with oversight and approval of the Director of Finance. 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 Director of Finance determined that this Policy was appropriate for the City of Hutchinson, Kansas, and therefore approved this Policy in June 2009. The City Attorney read and approved this policy in June 2009.

An Overview

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs. "Red flags" are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. Our Policy includes four basic elements, which together create a framework to address the threat of identity theft.

First, our Policy includes reasonable procedures to identify the "red flags" of identity theft we may run across in the day-to-day operation of our business.

Second, our Policy is designed to detect the "red flags" we have identified.

Third, our Policy spells out appropriate actions we will take when we detect "red flags".

Fourth, because identity theft is an ever-changing threat, we must address how we will re-evaluate our Policy periodically to reflect new risks from this crime.

Definitions

Identity Theft

A fraud that is committed or attempted using a person's identifying information with authority.

Creditor

The definition of "creditor" is broad and includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later. Utility companies, health care providers, and telecommunications companies are among the entities that may fall within this definition, depending on how and when they collect payment for their services. The Rule also defines a "creditor" as one who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions. Examples include finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers get financing from others, say, by processing credit applications. In addition, the definition includes anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit – for example, a third-party debt collector who regularly renegotiates the terms of a debt.

Covered Accounts
We have concluded that our organization is a creditor, and we have determined that we have "covered accounts" as the Red Flags Rule defines that term. Two categories of accounts are covered. The first kind is a consumer account that we offer our customers that is primarily for personal, family, or household purposes that permits multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, **utility accounts**, checking accounts, and savings accounts.

The second kind of "covered account" is "any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to permit multiple payments or transactions – they always are "covered accounts" under the Rule – other types of accounts are "covered accounts" only if the risk of identity theft is reasonably foreseeable.

Part One
Identify Relevant "Red Flags"
"Red flags" are potential patterns, practices, or specific activities indicating the possibility of identity theft. All employees responsible for or involved in the process of opening a covered account or accepting a payment for a covered account shall check for "red flags" as indicators of possible identity theft and such "red flags" may include:

1. **Alerts from consumer reporting agencies, fraud detection agencies or service providers.**
- Such as a fraud alert or credit freeze;
- Suspicious address change or address discrepancies;
- Activity inconsistent with history or usual patterns;
- Significant increase in the volume of inquiries.

2. **Suspicious Documents.**
- Documents provided for identification that appear to be altered or forged;
- Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
- Identification on which the information is inconsistent with information provided by the applicant or customer;
- Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as the application for service;
- An application that appears to be altered or forged, or appears to have been destroyed and reassembled.

3. **Suspicious Personal Indentifying Information.**
- Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the creditor;
- A social security number has not been issued, or is listed on the Social Security Administration's Death Master File;
- Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity;

- The applicant or customer fails to provide all required personal indentifying information on an application or in response to notification that the application is incomplete;
- The social security number provided is that same as that submitted by other applicants or customers;
- Personal identifying information is not consistent with personal indentifying information that is on file with the creditor;
- The applicant or customer cannot provide authentication information beyond that which generally would be available from a wallet or consumer report.

4. Suspicious Account Activity.

- Shortly after a change in address for an account, the creditor receives a request for additional users on the account;
- Mail sent to the customer is returned undeliverable although transactions continue to be conducted in connection with a customer's account;
- The City is notified that the customer is not receiving paper account statements in the mail;
- An account that is used in a way inconsistent with established patterns;
- An account that has been inactive is suddenly used again;
- An account that was closed for cause;
- An account that was identified for abuse account privileges;
- The City receives notice that there has been a breach in the City's computer system;
- The City is notified of unauthorized charges or transactions in connection with a customer's account.

5. Notice from Other Sources.

- The creditor is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft;
- Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

Part Two
Detect "Red Flags"

New Accounts.

When verifying the identity of the person who is opening a new account in-person, reasonable procedures include getting a name, address, and identification number and checking a current government-issued identification card, like a driver's license. Compare that information with other sources such as a credit reporting company, the Social Security Number Death Master File, or other publicly available information.

Existing Accounts.

To detect "red flags" for existing accounts, our program includes reasonable procedures to authenticate customers, monitor transactions, and verify the validity of change-of-address requests. We have determined that certain types of information, like a social security number, date of birth, mother's maiden name, or mailing address, are not good authenticators because they are so easily accessible.

Part Three
Prevent and Mitigate Identity Theft

When spotting a "red flag" our staff is prepared to respond appropriately. Some appropriate responses are:

- Monitoring covered accounts for evidence of identity theft
- Contacting a customer
- Changing passwords, security codes, or other ways to access a covered account

- Closing an existing account
- Reopening an account with a new account number
- Not opening a new account
- Not trying to collect on account
- Notifying law enforcement
- Determining that no response is warranted under the particular circumstances

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:

- Providing a secure website or clear notice that a website is not secure;
- Ensuring complete and secure destruction of paper documents and computer files containing customer information;
- Ensuring that office computers are password protected and that computer screens lock after a set period of time;
- Requiring only the last 4 digits of social security numbers, if any;
- Keep offices clear of papers containing customer information;
- Review reports and documentation and delete any unneeded identity information;
- Ensure computer virus protection is up to date;
- Require and keep only the kinds of customer information that are necessary for utility purposes;
- Secure information that is being stored for state or federal retention guidelines.

Part Four
Monitor and Update the Program

As new "red flags" emerge and technology changes or identity thieves change their tactics, we will periodically update our Policy to ensure that it keeps current with identity theft risks.

For the effectiveness of Identity Theft Prevention Policies, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to identity theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the program's general "red flag" detection, implementation and prevention practices are listed in this document.