Sedgwick County

Red Flag Policy

and

Identity Theft Prevention Program

Implemented as of May 1, 2009

Sedgwick County...
working for you

I. INTRODUCTION

Sedgwick County, Kansas (the "County") 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 & 15 USCA § 1681c(h). This Program is designed to detect, prevent and mitigate Identity Theft in connection with the opening and maintenance of certain County 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 County offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the County offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the County from Identity Theft.

This Program was developed with oversight and approval of the Chief Financial Officer. After consideration of the size and complexity of the County’s operations and account systems, and the nature and scope of the County’s activities, the Board of County Commissioners determined that this Program was appropriate for Sedgwick County, Kansas, and therefore approved this Program on April 1, 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 County 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 County identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings from Consumer Reporting Agencies.

1. **Receiving a report or notice from a consumer reporting agency of a credit freeze;**
2. **Receiving a report of fraud with a consumer report;**
3. **Notice or report from a credit agency of an active duty alert for an applicant; and**

4. **Receiving indication from a consumer report of activity that is inconsistent with a customer's usual pattern or activity.**

B. 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.**

C. Suspicious Personal Identifying Information.

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.

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 County receives notice that a customer is not receiving his paper statements;**
5. **The County receives notice that an Account has unauthorized activity;**

6. **The County receives notice that there has been a breach in the County's computer system;**
7. **The County receives notice that there has been unauthorized access to or use of customer Account Information; and**
8. **The County receives notice that there has been unauthorized access to the County's plans to take steps with certain data it maintains that contains customer information (i.e. destroying computer files).**

E. Notice Regarding Possible Identity Theft.

1. **The County 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.**
2. **Notification from another company or utility that identity fraud is suspected.**

F. Suspicious Customer Complaint.

1. **Complaint or question from a customer based on the customer's receipt of**
   a. **A bill for another individual**
   b. **A bill for services not received**
   c. **Notice of insurance benefits or an explanation of benefits for services never received**
2. **Records for treatment or other services that are inconsistent with known facts or circumstances regarding the customer**
3. **Complaint or question from a customer regarding collection notices from a collection agency for bills contested by the customer**
4. **Notice that coverage for services has been denied because policy limits have been reached**

III. DETECTION OF RED FLAGS.

A. In order to detect any of the Red Flags identified above with the opening of a new Account, County personnel will take one or more of 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, 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. **Verifying identity via a consumer reporting agency;**
4. **Reviewing documentation showing the existence of a business entity; and**
5. **Independently contacting the customer.**

B. In order to detect any of the Red Flags identified above for an existing Account, County personnel will take each of 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. **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; and**
4. **Verifying changes in banking information given for billing and payment purposes.**

IV. PREVENTING AND MITIGATING IDENTITY THEFT.

A. In the event County 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. **Reopening an Account with a new number;**
5. **Not opening a new Account;**
6. **Closing an existing Account;**
7. **Notifying law enforcement;**
8. **Determining that no response is warranted under the particular circumstances; or**
9. **Notifying the Program Administrator (as defined below) for determination of the appropriate step(s) to take.**

B. In order to further prevent the likelihood of identity theft occurring with respect to County accounts, the County will take the following steps with respect to its internal operating procedures:

1. **Providing a secure website or clear notice that a website is not 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; and**
4. **Requiring only the last 4 digits of SSNs (if any);**
5. **Keep offices clear of papers containing customer information;**

6. **Review reports and documentation and delete any unneeded identity information;**
7. **Ensure computer virus protection is up to date; and**
8. **Require and keep only the kinds of customer information that are necessary for program administrative purposes.**
9. **Secure information that is being stored for state or federal retention guidelines.**

V. Duties Regarding Address Discrepancies

In the event the County receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, the County may reasonably confirm that an address is accurate by any of the following means:

1. **Verification of the address with the consumer;**
2. **Review of a utility's records;**
3. **Verification of the address through third-party sources; or**
4. **Other reasonable means.**

If an accurate address is confirmed, the County shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

VI. 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 County from Identity Theft. At least annually the Chief Financial Officer will consider the County'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 County maintains and changes in the County's business arrangements with other entities. After considering these factors, the Chief Financial Officer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Chief Financial Officer will present the Board of County Commissioners with his or her recommended changes and the Board of County Commissioners will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

The County's Program will be overseen by a Program Administrator. The Program Administrator shall be: Chief Financial Officer.

The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of County 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

County 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 County engages a service provider to perform an activity in connection with one or more Accounts, the County 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.

These 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 County's Program and report any Red Flags to the Program Administrator.**

For the effectiveness of Identity Theft prevention Programs, a degree of confidentiality regarding the County's specific practices relating to Identity Theft detection, prevention and mitigation must be maintained. Therefore, under this Program, knowledge of such specific practices is to be limited to the Program Administrator and those employees who need to know them for purposes of preventing Identity Theft.