RESOLUTION 020-09

A RESOLUTION ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM FOR JOHNSON COUNTY GOVERNMENT

At a regular meeting of the Board of County Commissioners of Johnson County, Kansas was held on Thursday, April 16, 2009, there came before the Board for consideration the matter of adopting an identity theft prevention program to comply with federal regulations.

The Board, upon a motion duly made, seconded and carried, adopted Resolution 020-09; to-wit:

The federal Fair Credit Reporting Act, the Federal Trade Commission adopted 16 CFR § 681.2 which requires certain defined creditors to adopt and implement a "red flag" program to prevent and mitigate identity theft with respect to certain accounts; and

WHEREAS, federal regulations define a "creditor" broadly and would include County programs which may extend, renew, or continue "credit" which is defined to include the right to defer payment for services rendered; and

WHEREAS, the County, through its departments, agencies, and programs, may provide services that bring the County within the scope of the federal regulations, for example, providing wastewater services, or by accepting multiple payments for County-provided services; and

WHEREAS, the Federal Trade Commission regulations require each creditor of an account covered by the regulations to adopt an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft related to information used in covered accounts; and

WHEREAS, the scope of the newly-adopted federal regulations, as well as the regulations' applicability to the various and several County services and programs, is yet unknown and is likely to be modified and refined in the future; and

WHEREAS, the Board in adopting a general "red flag" program by this Resolution intends to allow and encourage compliance with the federal regulations by permitting each County department and agency to implement the Board's program as appropriate for that particular department or agency.

NOW, THEREFORE, BE IT RESOLVED by Board of County Commissioners of Johnson County, Kansas, that the "Identity Theft Prevention Program for Johnson County Government" is adopted as follows:

Section 1. Purpose. The Board hereby adopts this Identity Theft Prevention Program for the Johnson County Government to comply with federal requirements, including those found at 16 CFR §681.2, in order to detect, prevent, and mitigate identity theft by identifying and detecting identity theft "red flags" and by responding to such "red flags" in a manner that will limit and prevent identity theft.

Section 2. Rules Adopted. The Board hereby approves for use for all County departments and agencies the "Identity Theft Prevention Program Policies and Procedures" ("Red Flag Rules") attached hereto as Exhibit A and incorporated herein by reference. The attached Exhibit A is a general template which may be modified as necessary and appropriate by each County department or agency for use by such department or agency.

Section 3. Applicability. Any department or agency that provides goods or services to the public and accepts payments in arrears, or otherwise meets the definition of a "creditor" as defined by federal regulations, shall implement the Red Flag Rules for such department or agency.

Section 4. Department and Agency Directors to Oversee Red Flag Rules. Each department and agency director shall have the authority to implement the Board's adopted Red Flag Rules for such director's department or agency and may amend and modify the Red Flag Rules from time to time to address department or agency-specific matters. Each department or agency that so modifies the Red Flag Rules shall provide a copy of such modified document to the County Manager.

Section 5. Discretionary Actions. Each department and agency director shall have discretion in the implementation of the Red Flag Rules to determine whether activities involving department or agency accounts suggest possible identity theft with respect to existing covered accounts and to take action deemed appropriate under the applicable Red Flag Rules.

Section 6. Updating the Red Flag Rules. Each department and agency director shall annually review and, as deemed necessary by the director, update the Red Flag Rules in order to reflect changes in risks to customers or to the safety and soundness of the County and its covered accounts from identity theft. Each director shall consider the following factors and exercise discretion in amending the program:

(1) The department's experiences with identity theft;
(2) Updates in methods of identity theft;
(3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
(4) Updates in the types of accounts that the department offers or maintains; and
(5) Updates in service provider arrangements.

Section 7. Administration. Each department and agency director, as senior management, is responsible for oversight of the Red Flag Rules for their respective departments and agencies. The County Manager is responsible for reviewing reports

prepared by senior management regarding compliance with "red flag" requirements and to recommend to the Board any material and significant changes to the County's program to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material and substantive change to the program shall be submitted to the Board of County Commissioners for review and consideration, provided, however, changes in the County's program made necessary by new or modified federal requirements shall not be deemed material or substantive and may be implanted by the County Manager without express Board action. The County Manager, and every director, may delegate to another the tasks required by this Resolution and the County's Red Flag Rules.

Section 8. Annual Review of Program. The County Manager shall undertake an annual review of the County's compliance with federal regulations governing identity theft as follows:

The department and agency directors shall report to the County Manager at least annually on compliance with the "red flag" requirements. The director's report should address the program and evaluate issues such as:

a. The effectiveness of the policies and procedures of department in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
b. Service provider arrangements;
c. Significant incidents involving identity theft and management's response; and
d. Recommendations for material and significant changes to the adopted Red Flag Rules.

Section 9. Training. The department and agency directors are responsible for providing training to employees involved in covered accounts with respect to the implementation and requirements of the Red Flag Rules. Directors shall determine the scope and substance of training.

Section 10. Outside Service Providers. If a department or agency engages a service provider to perform an activity in connection with one or more covered accounts, reasonable efforts shall be made to ensure that the service provider's activities are conducted in accordance with the department's Red Flag Rules, as agreed upon by contract, or that the service provider otherwise takes appropriate steps to prevent or mitigate identity theft.

This is an ordinary home rule Resolution and shall become effective upon its adoption.

BOARD OF COUNTY COMMISSIONERS
OF JOHNSON COUNTY, KANSAS

Annabeth Surbaugh, Chairman

ATTEST:

Casey Joe Carl, Clerk of the Board

041609

APPROVED AS TO FORM:

Robert A. Ford
Assistant County Counselor

APR 2009

CASEY JOE CARL
CLERK OF THE BOARD
JOHNSON COUNTY KANSAS

EXHIBIT A

(Template for Departments' Use)

JOHNSON COUNTY KANSAS IDENTITY THEFT PREVENTION PROGRAM

Implemented as of May 1, 2009*

***May 1, 2009 is the date mandated by the federal government for implementation. If the federal regulators extend the date, then the County's Program shall go into effect on that later date unless the County Manager determines otherwise.**

I. INTRODUCTION

By a Resolution adopted on April 16, 2009, the Board of County Commissioners of Johnson County, Kansas ("Board") approved 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. (See 16 C FR § 681.2.)

After consideration of the size and complexity of the various County departments and agencies (collectively referred to as "Departments") comprising the Board's operations, and the nature and scope of the various County Departments' activities, the Board determined that this Program was appropriate for the Departments.

This document is designed to be a template for use by each County Department in the Department's effort to detect, prevent, and mitigate "Identity Theft" (as defined below) in connection with the opening and maintenance of Department accounts. For some Departments, this template may be appropriate for use without modification. For other Departments, this template may need to be modified by the Department Director to address specific or unusual aspects of the Department's operations. In the implementation of the "Red Flag" procedures, because of the varied nature of the services provided, and the limited information obtained, many of the Departments' operations will not be subject to improper use by those wishing to obtain personal information for Identify Theft purposes. However, despite the limited exposure these Departments' practices provide for Identity Theft activities, to ensure compliance with the intent and spirit of the federal regulations, the Board is adopting this Identify Theft Program which the Board intends to be used as a guide by each Department as appropriate.

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 any Department account which is for primarily for personal, family or household purposes and involves multiple payments or transactions.

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 Department will consider the types of Accounts it offers and maintains, the methods it provides to open its Accounts, the methods it provides to access its Accounts, the relationship of the Department with others who may be providing billing information to the Department, and the Department's previous experiences of any known occurrences of Identity Theft.

The following are recognized as potential Red Flags, some of which may not be applicable to each Department's operations at this time:

A. Red Flags for Documents:

1) Documents provided for identification that appear to be forged or altered;
2) Documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;
3) Documentation with information that is not consistent with existing customer information; and
4) An application for service that appears to have been altered or forged.

B. Red Flags for Personal Identifying Information:

1) A person's identifying information is inconsistent with other information the customer provides;
2) A person's identifying information is the same as shown on other applications found to be fraudulent;
3) A person's identifying information is consistent with fraudulent activity;
4) A person's Social Security Number (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 fails to provide complete personal identifying information on an application when asked to do so; and
7) A person's identifying information is not consistent with the information that is on file for the customer.

C. Red Flags for 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;
3) Mail sent to the Account holder is repeatedly returned as undeliverable;
4) The Department receives notice that a customer is not receiving paper statements; and
5) The Department receives notice that an Account has unauthorized activity.

D. Notice Regarding Possible Identity Theft:

1) The Department receives notice that a Department-maintained account is being used by a person engaged in Identity Theft.

III. DETECTION OF RED FLAGS.

It is required, under the federal regulations, that each Department be diligent in detecting any of the Red Flags identified above in connection with the opening of a new Account and to take the following steps, as appropriate, to obtain and verify the identity of the person opening a new account:

1) Verifying an individual's identity by reviewing and, if necessary, copying a driver's license or other identification card;
2) Reviewing documentation showing the existence of a business entity; and
3) Requiring, as applicable, the name, date of birth, residential or business address, principal place of business for an entity, and social security number, tax identification number, driver's license information, or other identification.

In order to detect any of the Red Flags identified above for an existing Account, Department personnel should be trained to take the following steps to monitor transactions involving such Accounts:

1) Verifying the identification of a customer request for information that could lead to Identity Theft;
2) Verifying the validity of a request to change a billing address; and
3) Verifying changes in banking information given for billing or payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT.

If Department personnel detect any identified Red Flag, such personnel shall take appropriate action which may include, among other things:

1) Monitor the Account for evidence of Identity Theft;
2) Contacting the customer;
3) Not opening a new Account;
4) Closing an existing Account;
5) Notifying law enforcement;
6) Determining that no response is warranted under the circumstances; or
7) Notifying the Program Administrator (as defined below) for determination of the appropriate action to take.

V. UPDATING THE PROGRAM AND THE RED FLAGS

This Program will be periodically reviewed and updated by each Department Director to reflect changes in risks to the Department's customers. At least annually, the Department shall review the Department's experiences with Identity Theft situations and determine whether changes are warranted in Identity Theft methods, detection, and prevention, as well as consider appropriate changes to the types of Accounts the Department maintains. After considering these factors, the Director will determine whether changes to the Program, including the criteria for identifying Red Flags, are warranted.

VI. PROGRAM ADMINISTRATION.

A. Oversight

The implementation of this Program will be overseen by the Director of the Department or the Department's designee, who shall be the "Program Administrator" for such Department. The Program Administrator shall be responsible for the Program's administration, for ensuring appropriate training of Department staff, for general oversight of staff's efforts regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft and, generally, determining which prevention and mitigation measures should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program. Because the variety of services provided and Accounts maintained by County Departments, each Department may tailor the general methods of preventing and mitigating Identity Theft to address the needs of such Department.

B. Staff Training and Reports

Department staff responsible for implementing this Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the response to be taken when a Red Flag is detected.

C. Service Provider Arrangements

If the Department engages a third-party service provider to perform an activity in connection with one or more Accounts, the Department should 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, including:

1) Requiring that service providers have Identity Theft policies and procedures in place;
2) Requiring that service providers review the Department's Program and report any Red Flags to the Program Administrator.

END OF DOCUMENT