Unified Government of Wyandotte County and Kansas City, Kansas

Adopted: 5/11/2011

Red Flag Policy and Identity Theft Prevention Program

Authority:
The Mayor and the Board of Commissioners are responsible for legislation, policy formulation, and overall direction setting of the government. This includes the approval of financial policies which establish and direct the operations of Unified Government (UG). The County Administrator is responsible for carrying out the policy directives of the UG Board of Commissioners and managing the day-to-day operations of the executive departments.

I. Purpose:

The Unified Government of Wyandotte County/Kansas City, Kansas (the "UG") developed this Identity Theft Prevention Program to comply with the Federal Trade Commission's Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. See 16 C. F. R. § 681.1; 15 U.S.C. § 1681c(h). This program is designed to detect, prevent, and mitigate identity theft in connection with the opening and maintenance of the following UG accounts:

- Any account that the UG offers or maintains primarily for personal, family, or household purposes and that involves multiple payments or transactions; and
- Any other account that the UG offers or maintains for which there is a reasonably foreseeable risk to customers or to the UG's safety and soundness from identity theft.

For the purposes of this program, "identity theft" is defined as fraud committed or attempted using the identifying information of another person without authority. This program was developed with oversight and approval of the chief financial officer. After considering the size and complexity of the UG's operations and account systems and the nature and scope of the UG's activities, the Board of Commissioners determined that this program is appropriate for the UG and approved it on 05/11/2011.

II. Identification of Red Flags:

A "red flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. To identify relevant red flags, the UG considered the types of accounts that it offers and maintains, the methods that it provides to open accounts, the methods that it provides to access accounts and its previous experiences with identity theft. The UG has identified in the listed categories the following red flags:

<u>Category A</u>: Alerts, notifications, or warnings from a consumer reporting agency or service provider

Red flags:

- A fraud or active duty alert is included with a consumer report.

- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with a person's history or usual pattern of activity, such as a recent and significant increase in the volume of inquiries; an unusual number of recently established credit relationships; a material change in the use of credit; or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Category B: Suspicious documents

***Red flags*:**

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not information on the identification and is not consistent with other information provided by the person presenting the identification.
- Other information on the identification is not consistent with readily accessible information on file, such as a previous signature or recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Category C: Suspicious personal identifying information

Red Flags:

- Personal identifying information provided is inconsistent with other sources of information (such as an address not matching an address on a consumer report or a Social Security number [SSN] that was never issued).
- Personal identifying information provided by a person is inconsistent with other information provided by the person (such as inconsistent SSNs or birth dates).
- Personal identifying information (for example, address or phone number) is the same as shown on other applications or documents known to be fraudulent.
- Personal identifying information is of a type commonly associated with fraudulent activity (such as a fictitious billing address or an invalid phone number).
- The SSN provided is the same as another customer's SSN.
- The address or phone number provided is the same as or similar to that submitted by an unusually large number of other persons opening accounts or by other customers.
- A person fails to provide complete personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with information that is on file.

Category D: Unusual use of or suspicious activity related to an account

Red flags:

- A change of address for an account followed by a request to change the account holder's name.

- An account is 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).
- Mail sent to the account holder is repeatedly returned as undeliverable even though transactions continue to be conducted in connection with the account.
- The UG receives notice that a customer is not receiving paper account statements.
- The UG receives notice that an account has unauthorized activity.
- The UG receives notice that there has been a breach in the UG's computer system.
- The UG receives notice that there has been unauthorized access to or use of customer account information.
- The UG receives notice that there has been unauthorized access to the UG's plans to take steps with certain data it maintains that contains customer information (i.e. destroying computer files).

Category E: Notice of possible identity theft

Red flags:

- The UG 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.
- The UG receives notice from another company or utility that identity fraud is suspected.

III. Detection of Red Flags

To detect red flags in connection with the opening of a new account, UG personnel will take one or more of the following steps to obtain and verify the identity of the person opening the account:

- Require 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;
- Verify the customer's identity, such as by copying and reviewing a driver's license or other identification card;
- Verify identity via a consumer reporting agency;
- Review documentation showing the existence of a business entity; or
- Independently contact the customer.

To detect red flags for an existing account, UG personnel will take the following steps to monitor account transactions:

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

IV. Preventing and Mitigating Identity Theft

UG personnel who detect red flags will take one or more of the following steps, depending on the degree of risk posed:

- Continue to monitor the account for evidence of identity theft;
- Contact the customer;
- Change passwords or other security devices that permit access to the account;
- Reopen the account with a new number;
- Do not open a new account;
- Close the existing account;
- Notify law enforcement;
- Determine that no response is warranted under the particular circumstances; or
- Notify the program administrator for determination of the appropriate steps to take.

To prevent the likelihood of identity theft occurring with respect to UG accounts, the UG will take the following steps with respect to its internal operating procedures:

- Provide a secure website or clear notice that a website is not secure;
- When destroying paper documents or computer files containing customer information, completely and securely destroy the documents or files;
- Password protect office computers and set computer screens to lock after a set period of time;
- Require only the last 4 digits of SSNs (if any);
- Keep offices clear of papers containing customer information;
- Review reports and documentation and delete unneeded identity information;
- Keep computer virus protection is up to date;
- Require and keep only the kinds of customer information that are necessary for program administrative purposes; and
- Secure information that is being stored for state or federal retention guidelines.

V. Duties Regarding Addressing Discrepancies

When the UG receives notice from a nationwide consumer reporting agency that the address given by a customer substantially differs from the address contained in the consumer report, the UG may reasonably confirm that the address provided by the customer is accurate by any of the following means:

- Verifying the address with the customer;
- Reviewing utility records;
- Verifying the address through third-party sources; or
- Other reasonable means.

If an accurate address is confirmed, the UG will furnish the address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if the UG establishes a continuing relationship with the customer and regularly and in the ordinary course of business furnishes information to the consumer reporting agency.

VI. Updating the Program and Red Flags

This program will be periodically reviewed and updated to reflect changes in risks to customers or to the UG's safety and soundness from identity theft. At least annually, the chief financial officer will consider the UG's experiences with identity theft; changes in identity theft methods; changes in identity theft detection, prevention, and mitigation methods; changes in types of accounts that the UG maintains; and changes in the UG's business arrangements with other entities. After considering these factors, the chief financial officer will determine whether changes to this program, including the listing of red flags, are warranted. If the chief financial officer determines that administrative changes are warranted, he or she will implement such changes. Specific policy changes will be presented to the Board of Commissioners with the recommended changes and the Board of Commissioners will determine whether to accept, modify, or reject them.

VII. Program Administration

a) *Oversight*. The chief financial officer will act as program administrator and oversee this program. The program administrator will be responsible for the program's implementation and administration, including ensuring appropriate training of staff, reviewing staff compliance reports, determining which preventive or mitigating measures should be taken in particular circumstances and approving changes to the program to address changing identity theft risks.

b) *Staff reports*. UG staff responsible for developing, implementing, and administering this program will report to the program administrator at least annually on compliance by the UG with the Red Flag Rule, 16 C.F.R. § 681.1. The report will address material matters related to the program and evaluate issues such as the effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of accounts and existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes to the program.

c) *Service provider arrangements*. When the UG engages a service provider to perform an activity in connection with one or more accounts, it will take steps to ensure that the service provider conducts its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. These steps may include requiring the service provider by contract to have policies and procedures to detect red flags that may arise in the performance of its activities, to report any red flags to the program administrator, and to take appropriate steps to prevent or mitigate identity theft.