I. PURPOSE

The creation and implementation of an Identity Theft Prevention Policy at the County of Yadkin that will identify, detect, mitigate and update Red Flags that signal the possibility of identity theft in connection with the opening of a covered account or any existing covered account. This program is in compliance with the Fair and Accurate Credit Transactions (FACT) Act of 2003.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

According to the Rule, a County is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the County's accounts that are individual service accounts held by customers of the County whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any 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.

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the County considers 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 Credit Reporting Agencies

Red Flags

1) Report of fraud accompanying a credit report;
2) Notice or report from a credit agency of a credit freeze on a customer or applicant;
3) Notice or report from a credit agency of an active duty alert for an applicant; and
4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and,
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that 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 (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the County that a customer is not receiving mail sent by the County;

6. Notice to the County that an account has unauthorized activity;
7. Breach in the County's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the County from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, County personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, County personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

Communicate to employees and third-parties their responsibility for protecting sensitive information pursuant to governmental laws and regulations as required by current merchant services contracts, various legislation (including the "Identity Theft Protection Act of 2005") and prudent financial management. This procedure provides instructions on how to securely maintain sensitive information (i.e. credit card numbers, bank account information and social security numbers) and a response plan in the event of a breach.

Procedure

Definitions:

Cashier station- Any location in the county that accepts payments

Essential tasks- Job duties required for managing the responsibilities of a position

Security Breach- A breach is considered to have happened if any sensitive information is suspected to have been stolen, viewed, copied or otherwise compromised by an unauthorized

individual or is it is suspected that information has been lost and could be accessed by unauthorized individual(s). A breach of information can occur physically or virtually via technology.

> *Sensitive Information*- Information such as credit card numbers, banking account information, social security numbers and any other information as identified in the Identity Theft Protection Act of 2005 (NCGA 75-60)

Prevention of Breach

Access

Employees who have access to sensitive information are required to create, handle, maintain and dispose of such information with prudent care in order to ensure proper security. Access to sensitive information will be limited and only provided in order for employees to perform essential tasks. Department Directors in each department will minimize the number of employees with access to sensitive information. System access will be granted and authorized according to the County's current policies and procedures.

Daily Use and Storage

The following procedures shall be followed on any electronic device while creating, handling, maintaining, storing and disposing of sensitive information:

1. Where possible, enter the information directly into the system (to its final destination) and refrain from documenting the information in other areas.
2. If numbers are written on paper for reference, shred immediately upon completion of task. Do NOT leave the paper in an unsecured area.
3. Never include sensitive information in emails.
4. Segregate sensitive information from public information.
5. Restrict the number of employees who have access to maintenance screens where sensitive information is stored.
6. Only maintain printed documentation of sensitive information in a secured cabinet or room and limit access to these areas.
7. Do not include sensitive information on printed reports except as needed for the performance of essential tasks and only with your supervisor's approval.
8. Properly destroy all documents containing sensitive information on a timeless basis according to procedures outlined below.
9. Where technologically possible, utilized encryption to secure the information in the database or storage system.
10. While away from your desk or laptop, do NOT leave it signed on or unlocked, since this may leave applications open to access by unauthorized individuals. All computing devices, including portable devices like cell phones, tablets, pdas, flashdrives, etc. are to be set-up to be auto-locked, password protected and encrypted and remain that way for the duration of use.
11. Do not store files with sensitive information on any non-county-owned device.
12. Loss of any county-owned computing device is to be reported immediately to IT.

Destruction

Information will be kept according to County policy and procedures, as well as the recommendations of the NC Archives standards. Documents that contain sensitive information

and are scheduled to be destroyed shall be destroyed either in-house or via an approved service provider. The method of destruction must meet all requirements from merchant services contracts, legislative orders, NC Statutes and County policies.

Detection
In the event a County employee detects 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. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

VI. PROGRAM UPDATES

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 every year, the Program Administrator will consider the County's experiences with Identity Theft situation, 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 Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the Board of Commissioners with his or her recommended changes and the Board of Commissioners will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the County. The Committee is headed by a Program Administrator who may be the head of the County or his or her appointee. Two or more other individuals appointed by the head of the County or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program 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 and considering periodic 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. *(The County may include in its Program how often training is to occur. The Program may also require staff to provide reports to the Program Administrator on incidents of Identity Theft, the County's compliance with the Program and the effectiveness of the Program.)*

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.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the County's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the County's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the Identity Theft Committee and 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.

Kevin Austin, Chairman
Board of Commissioners

11-5-12
Date