County of Bladen
North Carolina

Identity Theft Detection and Prevention Program

in compliance with the Federal FACTAct (2003)
Identity Theft Red Flags Rule

Effective May 1, 2009

I. PROGRAM ADOPTION

The County of Bladen developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C.F.R.§681.2. This Program was developed with oversight and approval of the County Board of Commissioners. 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 County Board of Commissioners determined that this Program was appropriate for the County of Bladen, and therefore approved this Program on May 4, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

The goal of this policy is to prevent identity theft. The County of Bladen recognizes the responsibility to safeguard customer's personal information during its collection, recording, and handling of such information. Under the Red Flags 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 utility, tax collector, and fees of other sources 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 accounts held by customers 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. 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);
4. Application for service that appears to have been altered or forged; and
5. Conflicting names on identification and other documentation.

B. 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.

C. 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.

D. 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:

1. Require certain identifying information such as name, date of birth, residential or business address, driver's license, social security card, or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card); and
3. Require a rental receipt, lease agreement or purchase documents for the service address.

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:

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

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:

A. Prevent and Mitigate

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. Refuse to 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.

B. Protect customer identifying information

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 to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information. The County may enter into a written contract with a third party in the business of record destruction to destroy sensitive information in a manner consistent with this policy;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Release sensitive information to the account holder or individual who own the information only upon confirmation of personal identifying information or a valid picture ID.
6. Ensure computer virus protection is up to date;
7. Require and keep only customer information that is necessary for utility purposes;
8. Sensitive information should not be included on emails;
9. Sensitive information should not be included on printed reports except as needed for the performance of essential tasks;
10. Do not store files with sensitive information on laptops or on flash drives unless the information and the device can be secured and not accessible to unauthorized individuals; and
11. Train County employees who at times make hand written notes to destroy after data is entered.

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.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with each Department Head and Staff. The other individuals to review policy are: The County Manager, Sheriff, Finance Officer, and the Information Technology Director.

B. Staff Training and Reports

County staff responsible for implementing the Program shall be trained either by or under the direction of the Department Head or Supervisor 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.

1. Require that service providers have such policies and procedures in place; and
2. Require that service providers review the County's Program and report any Red Flags to the respective Department Head.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft Detection and Prevention Programs, the Red Flags Rule envisions a degree of confidentiality regarding the County's specific practices relating to Identity Theft detection, prevention and mitigation. This Program is to be adopted by a public body and thus publicly available, therefore, it would be counterproductive to list these specific practices here. Only the Program's general red flag detection, implementation and prevention practices are listed in this document.

County of Bladen, North Carolina

Sensitive Information User Agreement

I have read the Identity Theft Detection and Prevention Program for the County of Bladen, North Carolina and understand how to properly manage, maintain, store, and dispose of sensitive and confidential information while employed with the County of Bladen. I will abide by the policy and will handle sensitive and confidential information with prudent care in order to ensure proper security of the information.

In the event of a suspected or actual breach of sensitive and confidential information, I will notify my supervisor without delay.

I understand the negligent handling or inappropriate use of the County's sensitive and confidential information will be subject to disciplinary action up to and including dismissal and may be criminally and civilly prosecuted as allowed by law.

I have read, understand, and agree to the conditions above.

Printed Name of Employee: _____

Department/Division: _____

Signature of Employee: _____

Date Signed: _____

IDENTITY THEFT PREVENTION PROGRAM

INCIDENT REPORT

DATE	EMPLOYEE	INCIDENT	RESPONSE	MITIGATION