

REQUEST FOR BOARD ACTION / CONTRACT CONTROL FORM

Tracking Number: _____

9.

Date of Request: October 13, 2008

Date Request Received: October 13, 2008

Board Meeting Date Requested: October 20, 2008

Board Meeting Date Assigned: October 20, 2008

Short Title: Resolution Approving The Pender County Identity Theft Prevention Policy And Program

Request Status:

- Request is proceeding to Board of Commissioners
- More information is needed – see attached
- Request on hold – no further information needed
- Other:

(Administrative Use Only)

Background: In September 2008, local and county governments in North Carolina were informed by the NCLM and NCACC of a new Federal Trade Commission (FTC) requirement concerning the adoption of identity theft prevention programs by all forms of local government that have utility accounts. By November 1, 2008, these entities must have in place written procedures/programs that help protect consumers identity and fight theft of customer account information. The identity theft prevention programs must identify, detect, and respond to possible signals of identity theft known as "Red Flags."

Staff's investigation of the FTC law leads us to believe that other Departments of Pender County Government such as the Tax, Health and Social Services groups may also trigger the "Red Flags Rules."

A powerpoint presentation has been developed and will be presented summarizing the policy and program.

Specific Action Requested: To approve a resolution adopting the Pender County Identity Theft Prevention Policy and Program.

Requested by: Michael G. Mack
Department: Pender Utilities
Title: Director
Contact Phone: 910.259.1570
Contact Fax: 910.259.1579

CONTRACT TYPE

- Renewal
- For Service(s)
- Intergovernmental – County as Grantee
 - Federal Grantor
 - State Grantor
 - Grantor
- County as Grantor
 - County Funds
 - Other Funds:
- Revision
- For Equipment

PURCHASING

Date Rec'd: Budgeted Item: Yes No
 Reviewed and Approved
 Comments on Reverse

Date Sent:

Signed:

ATTORNEY

Date Rec'd: Reviewed and Approved
 Legal Problem(s)
 Comments on Reverse

Date Sent:

Signed:

FINANCE

Date Rec'd: Sufficient Funds Available Not Available
 Budget Amendment Necessary
 Budgeted Amendment is Attached
 Comments on Reverse

Date Sent:

Signed:

CLERK

Signature(s) Required:
 Board Chairman/County Manager
 Other:

Date Rec'd: Approved by Board: Yes No
At meeting on

COUNTY OF PENDER



Identity Theft Prevention Policy and Program

October, 2008

PURPOSE

The County of Pender, NC developed this Identity Theft Prevention Policy and Program pursuant to the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) having issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions Act of 2003. (16 C. F. R. § 681.2). The program and policy must be in place by November 1, 2008.

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.

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 Pender County Manager determined that this Program was appropriate for the County of Pender, and therefore recommends this Policy and Program to the Board of County Commissioners on October 20, 2008.

DEFINITIONS

The Red Flags Rules 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.

The new Rules apply to all utility and other operations that provide a service for which payment is deferred until a future date. For example, when water, sewer or electricity is provided by a city or county and then paid for by the consumer at the end of a billing cycle, the entity has “extended credit” for the purpose of the Rules.

For purposes of this Policy, the following definitions apply¹:

- (a) ‘County’ means the County of Pender.
- (b) ‘Covered account’ means (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- (c) ‘Credit’ means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
- (d) ‘Creditor’ means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.
- (e) ‘Customer’ means a person that has a covered account with a creditor.
- (f) ‘Identity theft’ means a fraud committed or attempted using identifying information of another person without authority.
- (g) ‘Person’ means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
- (h) ‘Personal Identifying Information’ means a person’s credit card account information, debit card information bank account information and drivers’ license information and for a natural person includes their social security number, mother’s birth name, and date of birth.

- (i) 'Red flag' means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- (j) 'Service provider' means a person that provides a service directly to the County.

¹ Other than "County" and "Personal Identifying Information", definitions provided in this section are based on the definitions provided in 16 CFR § 681.2.

PRIVACY COMMITTEE AND PROGRAM ADMINISTRATION

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the County of Pender. The Committee is headed by a Privacy Officer who will be the County Manager or his/her appointee. A representative from the Utilities, ITS, Finance, and Sheriff's Department will comprise the remainder of the committee membership. The Privacy Officer will be responsible for the Program administration, for ensuring appropriate training of Pender 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.

Responsibilities of Departments

1. Each department will implement a standard procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. Departmental procedures will supplement, but not supersede this program or applicable laws.
2. Each department will ensure that service providers who are in contact with sensitive or confidential information are aware of security requirements, as well as the need for confidentiality, through proper contractual agreements and arrangements.
3. Department heads are responsible for determining which employees are authorized to access and handle sensitive and confidential information on a "need to know" basis to the extent necessary for the regular and ordinary course of business. The department head must also ensure that the authorized employees are trained to handle such information in accordance with this policy.
4. Employees who have access to sensitive and confidential information are required to create, handle, maintain, and dispose of such information with prudent care in order to ensure proper security. Access to sensitive and confidential information will be limited and only provided in order for authorized employees and contractual third parties to perform essential tasks for County business.

Procedures

The following procedures should be followed while creating, handling, maintaining, storing, and disposing of sensitive information:

1. Enter information directly to a final destination (i.e. computer system) and refrain from documenting the information in other areas.
2. If sensitive information is written on paper for reference, shred immediately upon recording the information in the final destination.
3. Electronic payment data should be handled by authorized personnel and only the last 4 digits of the customer's credit or debit account number should be visible on reports.
4. Sensitive information should not be included on e-mails.
5. Sensitive information should not be included on printed reports except as needed for the performance of essential tasks.
6. Maintain documents that contain sensitive information in a secured room and limit access to the area.
7. If possible, utilize encryption to secure information in the database or storage system.
8. Do not leave a computer unattended if sensitive information could be accessed by unauthorized individuals. While away from the computer, log off or lock the workstation.
9. 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.
10. Take reasonable measures when destroying sensitive data that will prohibit the information from being read or reconstructed. Documents with sensitive data should be shredded by the individual who has authorized access to the data or by another employee while in the presence of the authorized employee. 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.
11. In order to protect sensitive and confidential information, the County will only release sensitive information to the account holder or individual(s) who own the information upon confirmation of personal identifying information or a valid picture ID. The confirmed account holder or individual may authorize the release of sensitive information to a third party. Confidential information will only be released in accordance with State Statute. The only exception will be the release of specified information pursuant to a court order, warrant, subpoena or other requirement by law.

DETECTION AND IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, Pender 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 of Pender identifies the following red flags, in each of the listed categories:

Notifications and Warnings From Consumer Reporting Agencies

1. Report of fraud or active duty alert accompanying a credit report;

2. Notice or report from a consumer reporting agency of a credit freeze on a customer or applicant in response to a request for a consumer report;
3. Notice or report from a consumer reporting agency of an address discrepancy; and
4. Indication from a consumer reporting agency of activity that is inconsistent with a customer's usual pattern or activity.

Suspicious Documents

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 a signature card, previous check or if a person's signature on a check appears forged;
4. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

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 or a Social Security Number is listed on the Social Security Administration's Death Master File);
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.

Unusual Use of or Suspicious Account Activity

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 Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

Alerts from Others

1. Notice to Pender County by 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.

PREVENTING AND MITIGATING IDENTITY THEFT

New Accounts

In order to prevent and mitigate possible identity theft from detected Red Flags identified above in association with the opening of a **new account**, Pender County personnel will take the following steps:

1. Request certain identifying information such as name, date of birth, residential or business address, Social Security Number, Passport, birth certificate, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Notify the Privacy Officer for determination of the appropriate step(s) to take;
4. Deny the application for the new account; or
5. Notify law enforcement of possible identity theft

Existing Accounts

In order to prevent and mitigate possible identity theft from detected Red Flags identified above in association with an **existing account**, Pender County personnel will take the following steps:

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;
3. Change any passwords or other security devices that permit access to accounts;
4. Verify changes in banking information given for billing and payment purposes;
5. Continue to monitor an account for evidence of Identity Theft;
6. Close an existing account;
7. Reopen an account with a new number;
8. Notify the Privacy Officer for determination of the appropriate step(s) to take;
9. Notify law enforcement; or
10. Determine that no response is warranted under the particular circumstances.

PROTECT CUSTOMER IDENTIFYING INFORMATION

In order to further prevent the likelihood of identity theft occurring with respect to Pender County accounts, Pender County employees and ITS staff will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure complete and secure destruction of paper documents and computer files containing customer information;
2. Keep offices clear of papers containing customer information;
3. Request only the last 4 digits of social security numbers (if any);
4. Ensure the County's website is secure or provide clear notice that the website is not secure;
5. Ensure that office computers are password protected;
6. Ensure computer virus protection, content, email, and website filtering is up to date;
7. Erase all electronic data and effectively destroy the hardware when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information;
8. Provide a secure data center;
9. Provide additional security through the County's Cellular Policy, Computer Use Policy, Password Policy; PCI compliancy, Website Privacy and Security Policy; and
10. Provide up to date and compliant training.

PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of Pender County from Identity Theft. At least once a year, the Pender County Manager or his/her appointee (as Privacy Officer) and the Identity Theft Committee 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 Privacy Officer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Privacy Officer will update the Program or present the Pender County Board of Commissioners with his or her recommended changes and the Pender County Board of Commissioners will make a determination of whether to accept, modify or reject those changes to the Program.

STAFF TRAINING AND REPORTS

Pender County staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator and Identity Theft Committee in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. All Pender County staff will be required to provide immediate reports to the Privacy Officer on incidents of Identity Theft and provide periodic updates on the County's compliance with the Program and the effectiveness of the Program.

SERVICE PROVIDER ARRANGEMENTS

In the event Pender 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 Pender County Program and report any Red Flags to the Privacy Officer.

SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

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