Providing Quality Services... **NATURAL GAS • WATER • WASTEWATER**

NBU
NORTH BALDWIN UTILITIES

IDENTITY THEFT PREVENTION PROGRAM

Red Flag Rule

Effective May 1, 2009

PO Box 1207 | 25 Hand Ave | Bay Minette, AL 36507 | 251.580.1626 *phone* | 251.937.0345 *fax* | www.northbaldwinutilities.com

I. Program Adoption

North Baldwin Utilities ("NBU") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flag Rule ("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 NBU Board of Directors. After consideration of the size and complexity of NBU operations and account systems and the nature and scope of NBU activities, the Board of Directors determined that this Program was appropriate for NBU and therefore adopted this Program on April 23, 2009.

II. Program Purpose and Definitions

A. Fulfilling requirements of the Red Flag Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to it size, complexity and 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
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 Flag Rule definitions used in this Program

The Red Flag Rule defined "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 municipal utility 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 good or services, they, too, are to be considered creditors."

All utility accounts that are individual utility service accounts held by customers of utility whether residential, commercial or industrial are covered by the Rule.

Under the Rule, a "covered account" is:

1. Any account NBU offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions

2. Any other account NBU offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of NBU 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 codes.

III. Identification of Red Flags

In order to identify relevant Red Flags, NBU considers the type of accounts it offers and maintains, the methods it provides to open accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. NBU indentifies 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 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

B. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (ex: inconsistent birth dates)
2. Identifying information presented this is inconsistent with other sources of information (ex: 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 (ex: 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 persona indentifying information on an application when reminded to do so (by law social security numbers must not be required)
8. 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 (ex: very high activity)
4. Mail sent to the account holder is repeatedly returned as undeliverable
5. Notice to NBU that a customer is not receiving mail sent by NBU
6. Notice to NBU that an account has unauthorized activity
7. Breach in NBU's computer system security
8. Unauthorized access to or use of customer account information

D. Alerts from Others

Red Flags

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

IV. Detecting Red Flags

A. New Account

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

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

V. Preventing and Mitigating identity Theft

In the even NBU personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed:

A. Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft
2. Contact the customer
3. Change any password 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
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 NBU accounts, NBU will take the following steps with respect to its internal operating procedures:

1. Ensure complete and secure destruction of paper documents and computer files containing customer information
2. Ensure that office computers are password protected and that computer screens lock after a set period of time
3. Keep offices clear of papers containing customer information
4. Request only the last 4 digits of social security numbers (if any)
5. Ensure computer virus protection is up to date
6. Require and keep only the kinds of customer information that are necessary for NBU purposes

VI. Program Updates

This program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of NBU from Identity Theft. Once a year, the Program Administrator will consider NBU's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts NBU maintains and changes in NBU'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 and present the NBU Board of Directors with his/her recommended changes. NBU Board of Directors 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 NBU management. Management will appoint two or more supervisors as responsible for the Program Administration, for ensuring appropriate training of NBU staff, reviewing the detection of Red Flags and the steps for preventing and mitigating Identity Theft. Appointed supervisors will determine which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

NBU staff responsible for implementing the Program shall be trained either by or under the direction of the Billing Supervisor or Customer Service Coordinator 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 NBU engages a service provider to perform an activity in connection with one or more account, NBU will take the following steps to ensure the service provider performs its activities 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
2. Require by contract, that service providers review NBU's Program and Reports any Red Flags to the Program Administrator

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft Prevention Programs, the Red Flags Rule envisions a degree of confidentiality regarding NBU's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such practices is to be limited to the Identity theft Committee and those employees who need to know them for the purpose of preventing Identity Theft. Because this Program is to be adopted by a public body and this 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.