Town of Nags Head
Post Office Box 99
Nags Head, North Carolina 27959
Telephone 252-441-5508
Fax 252-441-0776
www.townofnagshead.net

Board of Commissioners Policy

Town of Nags Head Identity Theft Protection Program

Adopted October 22, 2008

BACKGROUND

Identity theft has become a serious nationwide problem in the United States, especially for municipalities like Nags Head that have utilities accounts. According to utility industry information, it is number three on the list of favorite places for identify thieves to hunt for information, ranking behind credit card companies and cell phone companies.

To combat the problem, as part of the Fair and Accurate Credit Transactions Act of 2003 (FACT), the Federal Trade Commission and several other federal agencies have issued rules requiring creditors to develop, adopt, and implement written Identity Theft Prevention Programs, as more fully described in the Federal Register at 72 Fed. Reg. 63771 (codified at 16 C.F.R. Part 681). These programs are required to be in place by November 1, 2008.

The Town of Nags Head Identify Theft Protection Program ("Program") has therefore been developed in order to address this problem and satisfy the requirements of the foregoing FACT legislation.

OBJECTIVE AND ADMINISTRATION

The objective of the Program is the identification, detection, and response to "Red Flags." Under the foregoing FACT rules, "Red Flags" are a pattern, practice, or specific activity that indicates the possible existence of identity theft, such as receipt of a warning from consumer reporting agencies, presentation of suspicious documents or personal identifying information, or the unusual use of a utility account. The Program seeks to identify relevant Red Flags for its utility accounts and incorporate them into the Program; to detect Red Flags that have been incorporated into the Program; to respond appropriately to any Red Flags that are detected to prevent and mitigate identify theft; and to ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the Town from identify theft.

The Finance Officer is the designated employee who is responsible for the oversight, implementation, and administration of the Program. The Finance Officer is also responsible for providing training to Town in order to effectively implement the Program.

OVERALL DESCRIPTION OF UTILITY SYSTEM

The Town of Nags Head operates a water system collection service to approximately 4695 customers. Customers are billed bi-monthly; utility accounts are established and maintained for these customers by the Customer Service Coordinator. Payments are processed by the Customer Service Cashier; payments consist of cash, checks, electronic checks, and credit cards which are received by mail, in person at the front desk, on-line or by telephone through a private vendor. The Town currently uses "MUNIS", an accounting and utility billing software. Its utility accounts constitute "covered accounts" under Section 681.2 of the FACT legislation. The Town has on-staff an Information Technology professional who coordinates security for the system by maintaining physical security, firewall security, administration security, network/wireless security, and backup/disaster recovery. Opening and accessing accounts is password protected.

CATEGORIES OF RED FLAGS

Alerts, Notifications or Warnings from a Consumer Reporting Agency

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

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 571.82(b) of FACT.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

   a. A recent and significant increase in the volume of inquiries;

   b. An unusual number of recently established credit relationships;

   c. A material change in the use of credit, especially with respect to recently established credit relationships; or

   d. An account that was closed for cause or identified for abuse of account privileges.

Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with the Town.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the Town. For example:

   a. The address does not match any address in the consumer report; or

   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Town. For example:

   a. The address on an application is the same as the address provided on a fraudulent application; or

   b. The phone number on an application is the same as the number provided on a fraudulent application.

4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Town. For example:

   a. The address on an application is fictitious, a mail drop, or a prison; or

   b. The phone number is invalid, or is associated with a pager or answering service.

5. The SSN provided is the same as that submitted by other persons opening an account or other customers.

6. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

7. The person opening the account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

8. Personal identifying information provided is not consistent with personal identifying information that is on file with the Town.

Unusual Use of, or Suspicious Activity Related to, the Account

1. Shortly following the notice of a change of address for an account, the Town receives a request for the addition of authorized users on the account.

2. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

   a. Nonpayment when there is no history of late or missed payments;

   b. A material increase in the use of available credit;

   c. A material change in purchasing or spending patterns;

3. An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

4. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

5. The Town is notified that the customer is not receiving paper account statements.

6. The Town is notified of unauthorized charges or transactions in connection with a customer's account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Accounts Held by the Financial Institution or Creditor

1. The Town is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

RESPONSES TO RED FLAGS

When the Administrative Services Staff has identified a Red Flag for any of its utility accounts, the appropriate response is commensurate with the degree of risk posed. The foregoing employees shall immediately bring any Red Flags detected to the attention of the Finance Officer. In determining the appropriate response, the Finance Officer should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the Town, or notice that a customer has provided information related to an account held by the Town to someone fraudulently claiming to represent the Town. Appropriate responses may include the following:

1. Monitoring an account for evidence of identity theft;

2. Contacting the customer;

3. Reopening an account with a new account number;

4. Not opening an account;

5. Closing an existing account;

6. Not attempting to collect on an account or not selling an account to a debt collector;

7. Notifying law enforcement – specifically, the Nags Head Police Department - ; or

8. Determining that no response is warranted under the particular circumstances.

UPDATING THE PROGRAM

The Town periodically updates its Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

1. The experiences of the Town with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;