CHAPTER 99: IDENTITY THEFT PREVENTION PROGRAM

Section

(Ord. (O)2008-10.66, passed 10-23-08)

§ 99.01 OBJECTIVE

The purpose of this Identity Theft Prevention Program (Program) is to protect customers of the Village of Huntley's utility services from identity theft. The Program is intended to establish reasonable policies and procedures to facilitate the detection, prevention and mitigation of identity theft in connection with the opening of new Covered Accounts and activity on existing Covered Accounts.

§ 99.02 SCOPE

This Program applies to the creation, modification and access to Identifying Information of a customer of one or more of the utilities operated by the Village (water and sewer) by any and all personnel of the Village, including management personnel. This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program, but rather it is intended to supplement any such existing policies and programs.

§ 99.03 DEFINITIONS

When used in this Program, the following terms have the meanings set forth opposite their name, unless the context clearly requires that the term be given a different meaning:

Covered Account: The term "covered account" means an account that the Village of Huntley offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions. A utility account is a "covered account." The term "covered account" also includes other accounts offered or maintained by the Village for which there is a reasonably foreseeable risk to customers, the Village or its customers from identity theft.

Identity Theft: The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority. FTC's Identity Theft Rules (16 CFR §681.2(b)(8) and 16 CFR §603.2(a)).

Identifying Information: The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. Additional examples of "identifying information" are set forth in 16 CFR §603.2(a).

Red Flag: The term "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Certain terms used but not otherwise defined herein shall have the meanings given to them in the FTC's Identity Theft Rules (16 CFR Part 681) or the Fair Credit Reporting Act of 1970 (15 U.S.C. §1681 *et seq*.), as amended by the Fair and Accurate Credit Transactions Act of 2003 into law on December 4, 2003. (Public Law 108-159).

§ 99.04 POLICY

(A) Administration of the Program

1. Issues to be addressed in the annual Identity Theft Prevention Report include:
    a) The effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of new Covered Accounts and activity with respect to existing Covered Accounts.
    b) Service provider arrangements.
    c) Significant incidents involving Identity Theft and management's response.
    d) Recommendations for material changes to the Program, if needed for improvement.

(B) Identity Theft Prevention Elements

1. *Identification of Relevant Red Flags*

The Village of Huntley has considered the guidelines and the illustrative examples of possible Red Flags from the FTC's Identity Theft Rules and has reviewed the Village's past history with instances of identity theft, if any. The Village hereby determines that the following are the relevant Red Flags for purposes of this Program given the relative size of the Village and the limited nature and scope of the services that the Village provides to its citizens:

a) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.

1. A fraud or active duty alert is included with a consumer report or an identity verification response from a credit reporting agency.

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 §681.1(b) of the FTC's Identity Theft Rules.

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 by a financial institution or creditor.

b) The presentation of 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 covered 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 Village, such as a signature card or a recent check.

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

c) The presentation of suspicious personal identifying information, such as a suspicious address change.

1. Personal identifying information provided is inconsistent when compared against external information sources used by the Village. 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 Village. 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 Village. For example:
    a) The billing 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 covered 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 Village.

9. If the Village uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d) The unusual use of, or other suspicious activity related to, a Covered Account.

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

2. A new utility account is used in a manner commonly associated with known patterns of fraud patterns. For example: the customer fails to make the first payment or makes an initial payment but no subsequent payments.

3. A covered account with a stable history shows irregularities.

4. A covered 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).

5. Mail sent to the customer is returned repeatedly as undeliverable although usage of utility products or services continues in connection with the customer's covered account.

6. The Village is notified that the customer is not receiving paper account statements.

7. The Village is notified of unauthorized usage of utility products or services in connection with a customer's covered account.

e) Notice of Possible Identity Theft.

1. The Village 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.

2. *Detection of Red Flags*

The employees of the Village of Huntley that interact directly with customers on a day-to-day basis shall have the initial responsibility for monitoring the information and documentation provided by the customer and any third-party service provider in connection with the opening of new accounts and the modification of or access to existing accounts and the detection of any Red Flags that might arise. Management shall see to it that all employees who might be called upon to assist a customer with the opening of a new account or with modifying or otherwise accessing an existing account are properly trained such that they have a working familiarity with the relevant Red Flags identified in this Program so as to be able to recognize any Red Flags that might surface in connection with the transaction. An Employee who is not sufficiently trained to recognize the Red Flags identified in this Program shall not open a new account for any customer, modify any existing account or otherwise provide any customer with access to information in an existing account without the direct supervision and specific approval of a management employee. Management employees shall be properly trained such that they can recognize the relevant Red Flags identified in this Program and exercise sound judgment in connection with the response to any unresolved Red Flags that may present themselves in connection with the opening of a new account or with modifying or accessing of an existing account. Management employees shall be responsible for making the final decision on any such unresolved Red Flags.

The Program Administrator shall establish from time to time a written policy setting forth the manner in which a prospective new customer may apply for service, the information and documentation to be provided by the prospective customer in connection with an application for a new utility service account, the steps to be taken by the employee assisting the customer with the application in verifying the customer's identity and the manner in which the information and documentation provided by the customer and any third-party service provider shall be maintained. Such policy shall be generally consistent with the spirit of the Customer Identification Program rules (31 CFR 103.121) implementing Section 326(a) of the USA PATRIOT Act but need not be as detailed. The Program Administrator shall establish from time to time a written policy setting forth the manner in which customers with existing accounts shall establish their identity before being allowed to make modifications to or otherwise gain access to existing accounts.

3. *Response to Detected Red Flags*

If the responsible employees of the Village of Huntley as set forth in the previous section are unable, after making a good faith effort, to form a reasonable belief that they know the true identity of a customer attempting to open a new account or modify or otherwise access an existing account based on the information and documentation provided by the customer and any third-party service provider, the Village shall not open the new account or modify or otherwise provide access to the existing account as the case may be. Discrimination in respect to the opening of new accounts or the modification or access to existing accounts will not be tolerated by employees of the Village and shall be grounds for immediate dismissal.

The Program Administrator shall establish from time to time a written policy setting forth the steps to be taken in the event of an unresolved Red Flag situation. Consideration should be given to 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, or a notice that a customer has provided account information to a fraudulent individual or website. Appropriate responses to prevent or mitigate Identity Theft when a Red Flag is detected include:

a) Monitoring a Covered Account for evidence of Identity Theft.
b) Contacting the customer.
c) Changing any passwords, security codes, or other security devices that permit access to a Covered Account.
d) Reopening a Covered Account with a new account number.
e) Not opening a new Covered Account.
f) Closing an existing Covered Account.
g) Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector.
h) Notifying law enforcement.
i) Determining that no response is warranted under the particular circumstances.

§ 99.05 PROGRAM MANAGEMENT AND ACCOUNTABILITY

(A) Initial Risk Assessment – Covered Accounts

Utility accounts for personal, family and household purposes are specifically included within the definition of "covered account" in the FTC's Identity Theft Rules. Therefore, the Village of Huntley determines that with respect to its residential utility accounts it offers and/or maintains covered accounts. The Village also performed an initial risk assessment to determine whether the utility offers or maintains any other accounts for which there are reasonably foreseeable risks to customers or the utility from identity theft. In making this determination the Village considered (1) the methods it uses to open its accounts, (2) the methods it uses to access its accounts, and (3) its previous experience with identity theft, and it concluded that it does not offer or maintain any such other covered accounts.

(B) Program Updates – Risk Assessment

The Program, including relevant Red Flags, is to be updated as often as necessary but at least annually to reflect changes in risks to customers from Identity Theft. Factors to consider in the Program update include:

a) An assessment of the risk factors identified above.
b) Any identified Red Flag weaknesses in associated account systems or procedures.
c) Changes in methods of Identity Theft.
d) Changes in methods to detect, prevent, and mitigate Identity Theft.
e) Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(C) Training and Oversight

All staff and third-party service providers performing any activity in connection with one or more Covered Accounts are to be provided appropriate training and receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

(D) Other Legal Requirements

Awareness of the following related legal requirements should be maintained:

- 31 U.S.C. 5318 (g) – Reporting of Suspicious Activities
- 15 U.S.C. 1681 c-1 (h) – Identity Theft Prevention; Fraud Alerts and Active Duty Alerts – Limitations on Use of Information for Credit Extensions
- 15 U.S.C. 1681 s-2 – Responsibilities of Furnishers of Information to Consumer Reporting Agencies
- 15 U.S.C. 1681 m – Requirements on Use of Consumer Reports

§ 99.06 RESPONSIBILITY

The initial adoption and approval of the Identity Theft Prevention Program shall be by Ordinance of the Village Board. Thereafter, changes to the Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the Director of Finance (Program Administrator). Major changes or shifts of policy positions under the Program shall only be made by the Village Board.
(Ord. (O)2008-10.66, passed 10-23-08)

Development, implementation, administration and oversight of the Program will be the responsibility of the Program Administrator. The Program Administrator will report at least annually to the Village Manager regarding compliance with this Program.

(Ord. (O)2008-10.66, passed 10-23-08)

§ 99.07 IDENTITY THEFT PREVENTION PROGRAM

Procedure for Opening New Account

I. New Utility Accounts may be opened in the following manners:

- In Person Walk-In
- Via Telephone
- Via Fax
- Via Internet (future)

II. Information and Documentation Required for Walk-in (potential customer to open new account)

- Driver's License or alternate government issued picture ID (required)
- Second form of identification, such as credit card (required)
- New service address (required)
- New service telephone number (if new)
- Most recent previous address (required)
- Social Security Number (optional)
- Permission signed for Credit Reporting Agency (CRA) Report (optional)
- Deed or Lease (optional)
- Set up challenge question (for future use)
- Signature on application (required)

III. Steps to be Taken by the Customer Service/Front Counter

a. Check driver's license/alternate government ID (prior training/detecting fake IDs)

b. Compare signature on application with signature on drivers license and second form of ID

c. Review checklist of Red Flags/determine if any present

d. Computer scan/make a copy of driver's license/alternate government ID

e. Go online with CRA – enter data to computer database/software
    i. Validate name, social security number (SSN), last address
    ii. Ensure SSN not on Death Master File (http://www.ssdmf.com)
    iii. Ensure not on Active Duty List
    iv. Ensure there are no Fraud Alerts

IV. Additional information needed if not present in person

a. SSN (required)
b. Previous two addresses and how long at each
c. Previous employer
d. Current employer
e. Previous utility
f. Identify potential customer depository bank or lending institution

V. Additional Steps by CSR

a. Additional validation of information from CRA for above items

VI. Specific Rules/Steps for Phone, Fax, or Internet

a. Phone
    - Do not process application if Caller ID blocked
    - Verify valid phone number in customer name
b. Fax
c. Internet (future)

VII. Steps for Customer Service/Front Counter to Follow If Validation of ID fails

a. Tactfully advise potential customer of the issue, if appropriate
b. Do not open account
c. Refer customer to external source that is the source of the Red Flag(i.e., SSN Master File)
d. Escalation to supervisor if situation with customer unresolved
e. Management employee/Program Administrator to make final decision in his/her discretion whether to open new account