VILLAGE OF ORLAND PARK
IDENTITY THEFT PREVENTION PROGRAM
APRIL, 2009

I. PROGRAM ADOPTION

The Village of Orland Park ("Village") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed by the Village Finance and MIS Departments with oversight and approval of the Village of Orland Park Board. After consideration of the size and complexity of the Village's operations and account systems, and the nature and scope of the Village's activities, the Board determined that this Program was appropriate for the Village of Orland Park, and therefore approved this Program on May 4, 2009**.**

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, every financial institution and/or 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:

- Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program
- Detect Red Flags that have been incorporated into the Program
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
- 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 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 goods or services, they, too, are to be considered creditors".

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

pool and Sportsplex member accounts, as well as all recreation program accounts, are covered by the Rule. Under the Rule, a "covered account" is:

- Any account the Village offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions
- Any other account the Village offers or maintains for which there is a reasonably foreseeable risk of identity theft to customers and\or to the Village

"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, 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 Village 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 Village identified the following Red Flags, in each of the listed categories including, but not limited to:

A. Notifications and Warnings from Credit Reporting Agencies

- Notice or report from a credit agency of a credit freeze on a customer or applicant
- Notice or report from a credit agency of an active duty alert for an applicant

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged)
- Application for service that appears to have been altered or forged

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report)
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (example: invalid phone number or fictitious billing address)
- An address or phone number presented that is the same as that of another person

- Incomplete personal identifying information provided on an application when reminded to provide complete information
- Inconsistent identifying information as compared with the information that is on file for the customer

D. Suspicious Account Activity or Unusual Use of Account

- Account change of address followed by a request to change the account holder's name
- Payments stop on an otherwise consistently up-to-date account
- Account used in a way that is not consistent with prior use, such as very high activity
- Mail sent to the account holder is repeatedly returned as undeliverable
- Notice to the Village that a customer is not receiving mail sent by the Village
- Notice to the Village that an account has unauthorized activity
- Unauthorized access to or use of customer account information

E. Alerts from Others

- Notice to the Village 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, Village personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, principal place of business, driver's license or other identification
- Verify the customer's identity, i.e., review a driver's license or other government issued identification card
- Review documentation showing the existence of a business entity, i.e., state license or other documentation
- Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, Village personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information whether it be in person or by telephone, facsimile or email
- Verify the validity of requests to change billing addresses
- Verify changes in banking information given for billing and payment purposes

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Village 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(s):

- Continue to monitor an account for evidence of identity theft
- Contact the customer
- Change any passwords or other security devices that permit access to accounts
- Not open a new account
- Close an existing account
- Reopen an account with a new number
- Notify the Program Administrator for determination of the appropriate steps to take
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances

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

- Ensure that its website is secure or provide clear notice that the website is not secure
- Ensure complete and secure destruction of paper documents and computer files containing customer information
- Ensure that office computers are password protected and that computer screens lock after a set period of time
- Keep offices clear of papers containing customer information
- Ensure computer virus protection is up to date
- Require and keep only the types of customer information necessary for Village purposes

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Finance and MIS Departments. The Finance Director and MIS Manager will be responsible for Program administration, ensuring appropriate training of Village staff on the Program, reviewing any staff –issued 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 updates to the Program.

B. Staff Training and Reports

Village staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator 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 Village engages a service provider to perform an activity in connection with one or more accounts, the Village 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:

- Require, by contract, that service providers have such policies and procedures in place
- Require, by contract, that service providers review the Village's Program and report any Red Flags to the Program Administrator

D. Specific Program Elements and Confidentiality

For the effectiveness of the Program, the Red Flags Rule envisions a degree of confidentiality regarding the Village'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 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.

VII. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risk to customers and the soundness of the Village from identity theft. If warranted, the Finance and MIS Departments will update the Program and present the updated program to the Village Board for acceptance and approval.