RESOLUTION NO. R 37-09

A RESOLUTION APPROVING AN
IDENTITY THEFT PROGRAM AND PREVENTION POLICY

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, requires that rules regarding identity theft protection be promulgated by covered entities; and

WHEREAS, those rules become effective November 1, 2008, and require municipal utilities and other departments to adopt and implement an identity theft program and prevention policy; and

WHEREAS, the Corporate Authorities of the Village of Lombard have considered an Identity Theft Program and Prevention Policy, a copy of which is attached hereto and made a part hereof as Exhibit "1" (the "Policy"), and have determined that said Policy is in the best interest of the Village of Lombard and its residents and complies with the aforementioned federal rules;

NOW, THEREFORE, BE IT RESOLVED BY THE PRESIDENT AND BOARD OF TRUSTEES OF THE VILLAGE OF LOMBARD, DUPAGE COUNTY, ILLINOIS, AS FOLLOWS:

SECTION 1: The recitals as set forth above are incorporated herein by reference and made a part hereof as material and operative provisions of this Resolution.

SECTION 2: The Policy attached hereto as Exhibit "1" and made part hereof is hereby adopted and approved.

SECTION 3: Effective November 1, 2008, the Village of Lombard and all its officers and employees are subject to the provisions of the attached Policy and shall follow and abide by the provisions thereof.

SECTION 4: The Village Clerk shall cause a copy of this Resolution and the attached Policy to be delivered to each officer and employee of the Village who is subject to the provisions of the Policy.

SECTION 5: This Resolution shall be in full force and effect from and after its adoption and approval as provided by law.

ADOPTED this 6th day of November, 2008, pursuant to a roll call vote as follows:

AYES: Trustees Gron, Tross, O'Brien, Moreau, Fitzpatrick and Soderstrom

NAYS: None

ABSENT: None

William J. Mueller, Village President

ATTEST:

Brigitte O'Brien, Village Clerk

Exhibit "1"

VILLAGE OF LOMBARD
IDENTITY THEFT PROGRAM AND PREVENTION POLICY

(see attached)

VILLAGE OF LOMBARD
IDENTITY THEFT PROGRAM AND PREVENTION POLICY

The following Identity Theft Program and Prevention Policy (the "Policy") is to implement the requirements of the Fair and Accurate Credit Transactions Act of 2003 and the associated final "Red Flag" rules promulgated by the Federal Trade Commission requiring certain municipal utilities and departments to enact certain policies and procedures regarding Identity Theft Red Flags and Prevention by November 1, 2008.

Section 1: Background

The risk to the Village, its employees and customers from data loss and identity theft is of significant concern to the Village and can be reduced only through the combined efforts of every employee and contractor.

Section 2: Purpose

A. The Village adopts this Policy to help protect employees, customers, contractors and the Village from damages related to the loss or misuse of sensitive information. This Policy will:

1. Define sensitive information; and
2. Place the Village in compliance with state and federal law regarding identity theft protection.

B. This Policy enables the Village to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the Village from fraudulent new accounts. The Policy will help the Village:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the Policy periodically, including reviewing the accounts that are covered and the identified risks that are part of the Policy.

Section 3: Scope

This Policy applies to employees, contractors, consultants, temporary workers and other workers at the Village, including all personnel affiliated with third parties.

Section 4: Sensitive Information Policy

A. Definition of Sensitive Information: Sensitive Information includes the following items whether stored in electronic or printed format which could be used on its own or in conjunction with other information to commit identity theft:

1. Credit card information, including any of the following:
   a. Credit card number (in part or whole)

b. Credit card expiration date
c. Cardholder name
d. Cardholder address

2. Tax identification numbers, including:
   a. Social Security number
   b. Business identification number
   c. Employer identification numbers

3. Payroll information, including, among other information:
   a. Paychecks
   b. Pay stubs

4. Other personal information belonging to any customer, employee or contractor, examples of which include:
   a. Date of birth
   b. Address
   c. Phone numbers
   d. Maiden name
   e. Names
   f. Customer number

B. Village personnel are encouraged to use common sense judgment in securing Sensitive Information to the proper extent. Furthermore, this section should be read in conjunction with the Illinois Local Records Act and the Village's local records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor.

Section 5: Identity Theft Prevention Program

A. Definition of a Covered Account: Any customer account that involves or is designed to permit multiple payments or transactions. Every new and existing account that meets the following criteria is a Covered Account and is covered by this Policy:

1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or

2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the Village from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. Definition of a Red Flag: Any potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification. Examples of Red Flags include:

1. Alerts, notifications or warnings from a consumer reporting agency or service provider.

2. Suspicious documents, such as:

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

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

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

d. Other information on the identification is not consistent with readily accessible information that is on file with the Village.

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

3. Suspicious personal identifying information, such as:

a. Personal identifying information provided is inconsistent when compared against external information sources used by the Village. For example:
   (i) The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
   (ii) 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 information and date of birth.

b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Village. For example, the address on an application is the same as the address provided on a fraudulent application.

c. 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:
   (i) The address on an application is fictitious, a mail drop, or a prison.
   (ii) The phone number is invalid or is associated with a pager or answering service.

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

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

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

g. Personal identifying information provided is not consistent with personal identifying information that is on file with the Village.

h. When using security questions (mother's maiden name, pet's name, etc.), 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.

4. Unusual use of, or suspicious activity related to, a Covered Account, such as:

a. Shortly following the notice of a change of address for a covered account, the Village receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

b. A new revolving credit 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.

c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   (i) Nonpayment when there is no history of late or missed payments.
   (ii) A material change in purchasing or usage patterns.

d. 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).

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

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

g. The Village is notified of unauthorized charges or transactions in connection with a customer's covered account.

h. The Village receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the Village.

i. 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.

Section 6: Responding to Red Flags

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the Village from potential damages and loss.

B. Once potentially fraudulent activity is detected, the employee should gather all related documentation and write a description of the situation. This information should be presented to the designated authority for review, assessment and determination.

C. The designated authority will complete additional investigation and authentication to determine whether the attempted transaction was fraudulent or authentic.

D. If a transaction is determined to be fraudulent or an attempt at fraud, appropriate actions should be promptly taken including:

1. Closing the existing Covered Account;
2. Notifying and cooperating with appropriate law enforcement agency;
3. Determining the extent of liability of the Village; and
4. Notifying the actual customer that fraud appears to have been committed or attempted.

Section 7: Periodic Updates to Policy

A: At least annually, this Policy will be re-evaluated to determine whether all aspects of the Policy are up to date and applicable in the current business environment and whether any changes need to be made in response to any instances of identity theft or to changing identity theft risks.

B. Periodic reviews will include an assessment of which accounts are covered by the Policy and whether there are any new accounts.

C. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce potential damages or losses to the Village and its customers.

Section 8: Policy Administration

A. Involvement of Management

1. This Policy shall be a separate program and operation and shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. Implementation of this Policy is the responsibility of the corporate authorities of the Village and approval of the initial Policy is to be appropriately documented and maintained.
3. Operational responsibility for the Policy is delegated to the Village Manager.

B. Staff Training

1. Staff training shall be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the Village or its customers.
2. The Village Manager is responsible for ensuring identity theft training for all requisite employees.
3. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Policy are made.

C. Oversight of Service Provider Arrangements

1. It is the responsibility of the Village to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.