STATE OF ILLINOIS)
)
COUNTIES OF COOK)
AND DU PAGE)

CLERK'S CERTIFICATE

I, EIRA L. CORRAL SEPÚLVEDA, the Municipal Clerk for the Village of Hanover Park in the Counties of Cook and DuPage, in the State of Illinois, do hereby certify that the following, hereinafter described, is a true and correct copy of the original documents which is part of the official records of the Village of Hanover Park:

Resolutions No. R-09-06: *A Resolution approving an identity theft prevention program for the Village of Hanover Park*

* * * * *

I, hereby subscribed my name as Municipal Clerk and affix the Official Corporate Seal of the Village of Hanover Park on this 11th day of August, 2016.

Eira L. Corral Sepúlveda, Village Clerk

RESOLUTION NO. R-09-06

A RESOLUTION APPROVING AN IDENTITY THEFT PREVENTION PROGRAM FOR THE VILLAGE OF HANOVER PARK

WHEREAS, the Fair and Accurate Credit Transactions Act, which was an amendment to the Fair Credit Reporting Act, requires the adoption of rules and procedures to detect, prevent, and mitigate identity theft by identifying and detecting identity theft red flags and responding to such red flags in a manner that will prevent identity theft; and

WHEREAS, the purpose of the Village's *Identify Theft Prevention Program*, as attached as Exhibit A, is to protect employees, customers, contractors, and the Village from the loss or misuse of sensitive information by identity theft; and

WHEREAS, the Village's *Identity Theft Prevention Program* meets the requirements of, and brings the Village into compliance with, certain identity theft prevention laws and regulations, including those promulgated by the Federal Trade Commission.

NOW, THEREFORE, BE IT RESOLVED by the President and Board of Trustees of the Village of Hanover Park, Cook and DuPage Counties, Illinois, as follows:

SECTION 1: That the foregoing recitals are incorporated herein as if fully set forth.

SECTION 2: That the Village of Hanover Park *Identity Theft Prevention Program*, attached hereto and made a part hereof as Exhibit A, is hereby approved.

SECTION 3: This Resolution and the Village of Hanover Park's *Identity Theft Prevention Program* shall be in full force and effect from and as of April 23, 2009, and its approval in the manner provided by law.

ADOPTED this 23rd day of April, 2009 pursuant to a roll call vote as follows:

AYES:	Manton, Carter, Kaiser, Nicolosi, Packham, Eby
NAYS:	None
ABSENT:	None
ABSTENTION:	None

Approved: _____
Village President

Attest: _____
Village Clerk

VILLAGE OF HANOVER PARK
IDENTITY THEFT PREVENTION PROGRAM

The following Identity Theft Prevention Program (the "Program") 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.

Section 1: Background

The risk to the Village and its 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 Program to help protect employees, customers, contractors, and the Village from damages related to the loss or misuse of sensitive information. This Program will:

1. Define sensitive information; and

2. Place the Village in compliance with state and federal law regarding identity theft protection.

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

1. Identify risks (red flags) that signify potentially-fraudulent activity within new or existing covered accounts;

2. Detect risks (red flags) when they occur in covered accounts;

3. Respond to risks (red flags) 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 Program applies to employees, contractors, consultants, temporary workers, and other workers at the Village that request, view, or process sensitive information.

Section 4: Sensitive Information Policy

A. 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

   b. Credit card expiration date

Section 4: Sensitive Information Policy (cont'd.)

c. Cardholder name

d. Cardholder address

2. Other personal information belonging to any customer, employee, or contractor, examples of which include:

a. Name

b. Address

c. Phone number

d. Social Security Number

e. Date of birth

f. Customer account number

B. Village personnel are expected to use the utmost of care in securing Sensitive Information. Furthermore, this section should be read in conjunction with the Illinois Local Records Act, the Freedom of Information Act, the Village's information technology policies and guidelines, 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

Under the Red Flag Rules, the Village is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity, and the nature of its operation.

A. Identity Theft: A fraud committed using the identifying information of another person.

B. 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. Any business, personal, and household account the Village offers or maintains for which there is a reasonably foreseeable risk of identity theft; or

2. Any business, personal, and household account 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.

C. Red Flags: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft or 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:

Section 5: Identity Theft Prevention Program (cont'd.)

a. Documents provided for identification that appear to have been altered, forged, or not authentic.

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. 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 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.

b. 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:

- The address on an application is fictitious, a mail drop, or a prison.
- The phone number is invalid or is associated with a pager or answering service.

c. 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.

d. 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.

e. Personal identifying information provided is not consistent with personal identifying information that is on file with the Village such as a signature.

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

a. 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.

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

- Nonpayment when there is no history of late or missed payments.
- A material change in purchasing or usage patterns.

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

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

Section 5: Identity Theft Prevention Program (cont'd.)

e. The Village is notified of unauthorized activity in connection with a customer's covered account.

f. 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.

g. 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: 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 a person opening the account:

1. Require certain identifying information such as name, residential or business address, driver's license, or other identification;

2. Verify the customer's identity, for example, review a driver's license or other identification card; and

3. Review documentation showing the existence of a business entity, such as business license records;

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:

1. Verify the identification of customers if they request information either in person or via the telephone, facsimile, or email;

2. Verify the validity of requests to change billing addresses by viewing supporting information such as a drivers license; and

3. Verify changes in banking information given for billing and payment purposes; for example, by viewing a voided check.

Section 7: Preventing Identity Theft and 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 their supervisor for review, assessment, and determination.

C. The supervisor will review and complete an 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:

Section 7: Preventing Identity Theft and Responding to Red Flags (cont'd.)

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Not open a new account;
4. Close an existing account;
5. Reopen an account with a new number;
6. Notify and cooperate with appropriate law enforcement; and
7. Determine that no response is warranted under the particular circumstances.

Section 8: Protecting Customer Identifying Information

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:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure the office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Ensure information is properly secured in locked cabinets and limit access to keys;
6. Request only the last four digits of social security numbers;
7. Ensure computer virus protection is up to date; and
8. Require and keep only the kinds of customer information that are necessary for Village purposes.

Section 9: Periodic Updates to Program

This Program will be reviewed and updated periodically to reflect changes in risk to customers and the soundness of the Village from identity theft. At least annually, the Village's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection, and prevention methods and changes in the types of accounts the Village maintains will be reviewed. As part of the review, Red Flags may be revised, replaced, or eliminated. Defining new Red Flags may also be appropriate. 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. If warranted, the Finance Department will update the Policy and present it to the Village Board with recommended changes. The Village Board will make a determination of whether to accept, modify, or reject those changes to the Program.

Section 10: Program Administration

A. Oversight

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 Village Manager and approval of the initial Policy by the Village Board is to be appropriately documented and maintained.

3. Oversight responsibility for the Policy is delegated to the Finance Director.

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 Assistant Finance Director is responsible for developing specific Identity Theft Prevention procedures and 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. The Village will require that service providers have such policies and procedures in place.

3. The Village will require that service providers read, understand, and agree to the guidelines set forth in the Village's Identity Theft Program and Prevention Policy and report any Red Flags to the Finance Director.

4. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft Prevention Programs, the Red Flag Rules envision 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 the Finance Director, Assistant Finance Director, and those employees who need to know them for the purposes of preventing Identity Theft. Because this Program is to be adopted by the Village Board and thus publicly available, it would be counter productive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation, and prevention practices are listed in this document.

Village of Hanover Park

Identity Theft Prevention Program

Approved by the Village President and Board of Trustees this April 23, 2009

Rodney S. Craig
Village President

Sherry L. Craig
Village Clerk

STATE OF ILLINOIS)
)
COUNTIES OF COOK)
AND DU PAGE)

CLERK'S CERTIFICATE

I, EIRA L. CORRAL SEPÚLVEDA, the Municipal Clerk for the Village of Hanover Park in the Counties of Cook and DuPage, in the State of Illinois, do hereby certify that the following, hereinafter described, is a true and correct copy of the original documents which is part of the official records of the Village of Hanover Park:

Resolutions No. R-11-06: A Resolution adopting the Village of Hanover Park Identity Protection Policy

* * * * *

I, hereby subscribed my name as Municipal Clerk and affix the Official Corporate Seal of the Village of Hanover Park on this 11th day of August, 2016.

Eira L. Corral Sepúlveda, Village Clerk

RESOLUTION NO. R-11-06

RESOLUTION ADOPTING THE VILLAGE OF HANOVER PARK

IDENTITY PROTECTION POLICY

WHEREAS, the President and Board of Trustees of the Village of Hanover Park desire to establish policies and procedures to protect social security numbers from unauthorized disclosure in accordance with the Identity Protection Act (5 ILCS 179/1 et seq.); and

WHEREAS, the Village of Hanover Park is a home rule unit by virtue of the provisions of the 1970 Constitution of the State of Illinois and may exercise and perform any function pertaining to its government and affairs including adoption of this Resolution; now, therefore,

BE IT RESOLVED by the President and Board of Trustees of the Village of Hanover Park, Illinois, as follows:

That the President and Board of Trustees hereby adopt the "VILLAGE OF HANOVER PARK IDENTITY PROTECTION POLICY" and related statement of purpose, consisting of four (4) pages inclusive of the Attachment, a copy of said policy is attached hereto as Exhibit A and made a part hereof.

ADOPTED this 7th day of April, 2011, pursuant to a roll call vote as follows:

AYES: Trustees Carter, Cannon, Roberts, Kaiser, Nicolosi, Zimel

NAYS: None

ABSENT: None

ABSTENTION: None

APPROVED: _____
Rodney S. Craig, Village President

ATTEST: _____
Eira L. Corral, Village Clerk

VILLAGE OF HANOVER PARK IDENTITY PROTECTION POLICY

This policy is adopted pursuant to the mandate of 5 ILCS 179/35 requiring each local government to draft and approve an Identity Protection Policy as provided in the Identity Protection Act (5 ILCS 179/1 *et seq.)* to protect social security numbers from unauthorized disclosure.

I. **PROHIBITED ACTS.** No Village employee may do any of the following:

(a) Publicly post or publicly display or otherwise intentionally communicate or otherwise intentionally make available to the general public in any manner an individual's social security number.

(b) Print an individual's social security number on any card required for the individual to access products or services provided by the Village.

(c) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(d) Print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this section to the contrary, social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Illinois Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope's having been opened.

(e) Collect, use, or disclose a social security number from an individual, unless:

(i) required to do so under state or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities;

(ii) the need and purpose for the social security number is documented before collection of the social security number; and

(iii) the social security number collected is relevant to the documented need and purpose.

(f) Require an individual to use his or her social security number to access an Internet website.

(g) Use the social security number for any purpose other than the purpose for which it was collected.

(h) Encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, RFID technology, or other technology, in place of removing the social security number as required by this policy.

II. **EXCLUSIONS FROM PROHIBITIONS.** The above-listed prohibitions in I. above do not apply in the following circumstances:

(a) The disclosure of social security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under the Identity Protection Act on a governmental entity to protect an individual's social security number will be achieved.

(b) The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.

(c) The collection, use, or disclosure of social security numbers in order to ensure the safety of: state and local government employees; persons committed to correctional facilities, local jails, and other law enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a state or local government agency facility.

(d) The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.

(e) The disclosure of social security numbers by a state agency to any entity for the collection of delinquent child support or of any state debt or to a governmental agency to assist with an investigation or the prevention of fraud.

(f) The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

III. **FREEDOM OF INFORMATION ACT REQUESTS.** Consistent with the Illinois Freedom of Information Act, Village employees must redact social security numbers from information or documents being supplied to the public pursuant to a Freedom of Information Act request before allowing the public inspection or copying of the information or documents.

IV. **APPLICABILITY.** This policy does not apply to the collection, use, or disclosure of a social security number as required by state or federal law, rule, or regulation. This policy does not apply to documents that are recorded with a county recorder or required to be open to the public under any state or federal law, rule, or regulation, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, any Village employee that complies with the federal law shall be deemed to be in compliance with this policy.

V. **IDENTITY PROTECTION PROCEDURES.** All Village employees having access to social security numbers in the course of performing their duties shall be trained to protect the confidentiality of social security numbers. The training shall include instructions on the proper handling of information that contains social security numbers from the time of collection through the destruction of the information.

Only Village employees who are required to use or handle information or documents that contain social security numbers have access to such information or documents.

Social security numbers requested from an individual shall be provided in a manner that makes the social security number easily redacted if required to be released as part of a public records request.

When collecting a social security number, or upon request by the individual, a statement of the purpose or purposes for which the Village is collecting and using the social security number shall be provided to the individual. A copy of said policy is attached and approved.

VI. **DISTRIBUTION OF POLICY.** A written copy of this policy has been provided to the Village's elected officials.

Each current Village employee shall be provided and shall acknowledge receipt of a copy of this policy. Each employee hereinafter hired by the Village shall be provided and shall acknowledge receipt of a copy of this policy upon commencing his or her employment. A copy of this policy shall be made available to any member of the public, upon request. If the Village Board amends this policy, the Village shall file a written copy of the amended policy with the Village Manager, who shall also advise all Village employees of the existence of the amended policy and make a copy of the amended policy available to each of its employees. The acknowledged copy of this policy shall be filed and maintained in each Village employee's personnel file.

This policy is effective May 28, 2011.

ACKNOWLEDGMENT BY EMPLOYEE

I received a copy of this Identity Protection Policy this _____ day of _____ 2011.

Name of Employee: _____

_____

Signature