NILES TOWNSHIP
COOK COUNTY, ILLINOIS

RESOLUTION NO. 2022 - 02

A RESOLUTION APPROVING AND IMPLEMENTING AN IDENTITY THEFT PREVENTION PROGRAM POLICY IN NILES TOWNSHIP, COOK COUNTY, ILLINOIS

BONNIE KAHN OGNISANTI, Township Supervisor
CHARLES LEVY, Township Clerk

DONALD GELFUND
MARK COLLINS
PEGGY TOLLESON
KITTY KENDRICK
Trustees

Published in pamphlet form by authority of the Supervisor and Board of Trustees of Niles Township on February 14, 2022

Prepared by ODELSON, STERK, MURPHEY, FRAZIER & McGrath, LTD.- Township Attorneys
3318 West 95th Street - Evergreen Park, Illinois 60805

NILES TOWNSHIP

RESOLUTION NO. 2022 - 02

A RESOLUTION APPROVING AND IMPLEMENTING AN IDENTITY THEFT PREVENTION POLICY IN NILES TOWNSHIP, COOK COUNTY, ILLINOIS

WHEREAS, Niles Township, Cook County, Illinois (the "Township"), is a duly organized and existing township and unit of local government created under the provisions of the laws of the State of Illinois, and is operating under the provisions of the laws of the State of Illinois, and is operating under the provisions of Illinois Township Code, 60 ILCS 1/1-1, *et seq.* (the "Code"), and all laws amendatory thereto; and

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 red flags in a manner that will prevent identity theft; and

WHEREAS, the Niles Township has determined that the Identity Theft Prevention Program Policy, attached hereto and incorporated herein as **Exhibit A**, is in the best interest of the Township and its citizens.

NOW, THEREFORE, BE IT RESOLVED, by the Supervisor and the Board of Trustees of Niles Township as follows:

Section 1. The foregoing recitals shall be and are hereby incorporated as findings of fact as if said recitals were fully set forth herein.

Section 2. The Identity Theft Prevention Program Policy, attached hereto and incorporated herein as **Exhibit A** to this Resolution, is hereby approved and adopted as a written policy of Niles Township.

Section 3. **Exhibit A** shall be uploaded on the Township's website and shall be incorporated into the Township's Personnel Manual.

Section 4. If any section, paragraph, clause, or provision of this Resolution shall be held invalid, the invalidity thereof, shall not affect any of the other provisions of this Resolution.

Section 5. All resolutions, motions, policies, and orders in conflict herewith are hereby repealed to the extent of such conflict.

Section 6. This Resolution shall be in in full force and effect after its passage, approval, and publication, as provided by law.

ADOPTED by the Supervisor and Board of Trustees of Niles Township, Cook County, Illinois this 14 day of February, 2022, pursuant to a roll call vote, as follows:

	YES	NO	ABSENT	PRESENT
Trustee Gelfund	X			
Trustee Collins			X	
Trustee Tolleson	X			
Trustee Kendrick	X			
Supervisor Kahn Ognisanti	X			
TOTAL	4			

APPROVED at a Regular meeting of the Board of Trustees of Niles Township, on February 14, 2022.

BONNIE KAHN OGNISANTI, Supervisor

ATTEST:

Sandie Capsuto, Deputy Clerk

CHARLES LEVY, Township Clerk

CERTIFICATION

State of Illinois)
) ss.
County of Cook)

I, Charles Levy, do hereby certify that I am the duly qualified and acting Township Clerk of Niles Township, Cook County, Illinois, and as such official I am the keeper of the records and files of Niles Township.

I further certify that the foregoing or attached is a complete, true and correct copy of the Resolution No. 2022-02, entitled "**A RESOLUTION APPROVING AND IMPLEMENTING AN IDENTITY THEFT PREVENTION PROGRAM POLICY IN NILES TOWNSHIP, COOK COUNTY, ILLINOIS**," which was adopted by the Supervisor and the Board of Trustees on February 14, 2022.

IN THE WITNESS WHEREOF, I have hereunto set my hand in the County of Cook, and State of Illinois, on February 14, 2022.

Charles Levy

Charles Levy, Township Clerk

(Corporate Seal)

EXHIBIT A

NILES TOWNSHIP
IDENTITY THEFT PREVENTION PROGRAM POLICY

NILES TOWNSHIP
IDENTITY THEFT PREVENTION PROGRAM POLICY

The Niles Township (the "Township") adopts this Identity Theft Prevention Program Policy (the "Policy" or "Program") pursuant to the Fair and Accurate Credit Transactions Act of 2003. In addition, this Policy will establish its procedures pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule.

I. Statement of Purpose

The Purpose of the Identity Theft Prevention Program Policy is to protect individuals from harm and damages related to, or caused by, the loss or misuse of Sensitive Information. The Policy will also assist the Township in detecting, preventing, and mitigating Identity Theft. The Policy does so by identifying certain "Red Flags" that suggest or indicate the possibility of Identity Theft, and by providing guidelines on how the Township should respond once it detects any such Red Flags. The Policy will:

A. Define Sensitive Information;

B. Describe the electronic security of data when stored and distributed; and

C. Place the Township in compliance with state and federal law regarding Identity Theft protection.

The Policy has been tailored to the size, complexity, and the nature of the Township's operations. The Policy also has been designed to:

A. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Policy;

B. Detect Red Flags that have been incorporated into the Policy;

C. Allow the Township to respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

D. Ensure that the Policy is reviewed periodically and updated, if necessary, to reflect changes in risks to individuals or to the safety and soundness of the Village from Identity Theft.

II. Definitions

The following words, terms, and phrases, when used in this article, shall have the meanings ascribed to them in this Section, except where the context clearly indicates a different meaning:

- Covered Account: an account that the Township offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a utility account; and any other account that the Township offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Village, including financial, operational, compliance, reputation, or litigation risks.
- Identity Theft: a fraud committed or attempted using identifying information of another person without authority.
- Red Flag: a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

- Sensitive Information: any name or number that may be used, alone or in conjunction with other information to identify a specific person, including, but not limited to a person's credit card account information, debit card information, bank account information, driver's license information, social security number, mother's birth name, date of birth, electronic identification number, computer internet protocol address, and routing code.

III. Identification of Red Flags

Examples of Red Flags include:

1. Alerts, notifications, or warnings from a consumer reporting agency or service provider.
2. Suspicious documents, such as:
   a. Identification document or card that appears to be forged, altered, or otherwise inauthentic;
   b. Identification document or card on which a person's photograph or physical description is inconsistent with the person presenting the document;
   c. Other documentation with information that is not consistent with existing customer information (e.g., a person's signature on a check appears forged); and
   d. Application for service that appears to have been altered or forged.
3. Suspicious personal identifying information, such as:
   a. Identifying information presented that is inconsistent with other information the customer provides (e.g., inconsistent birth dates);

b. Identifying information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a credit report);

c. Identifying information presented that is the same as information shown on other applications were found to be fraudulent;

d. Identifying information presented that is consistent with fraudulent activity (e.g., an invalid phone number or an answering service, or fictious billing address, mail drop or prison);

e. Social security numbers presented that is the same as one given by another customer;

f. An address or phone number presented that is the same as that of another person;

g. A person fails to provide complete personal identifying information on an application when reminded to do so; and

h. A person's identifying information is inconsistent with the information that is on file for the customer.

4. Suspicious account activity or unusual use of account, such as:

a. Change of address for an account followed by a request to change the account holder's name;

b. Payments cease on an otherwise consistently up to date account;

c. Account used in a manner that is inconsistent with prior use (e.g., remarkably high activity);

d. Mail sent to the account holder is repeatedly returned as undeliverable;

e. Notice to the Township that a customer is not receiving mail sent by the Township;

f. Notice to the Township that an account has unauthorized activity;

g. Breach of the Township's computer security system; and

h. Unauthorized access to or use of customer account information.

5. Alerts from others, such as:

a. Notice to the Township from a customer, Identity Theft victim, law enforcement, or other person that Township has opened or is maintaining a fraudulent account for a person engaged Identity Theft.

IV. Detecting Red Flags

Opening Covered Accounts

In order to try and detect any of the Red Flags identified in Section III, the Township personnel should take the following steps to obtain and verify the identity of the person opening a Covered Account:

A. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification for individuals/residents;

B. Verify the customer's identity (e.g., review a driver's license or other identification card);

C. Review documentation showing the existence of a business entity; and independently contact the customer if appropriate.

Existing Covered Account.

In order to detect any of the Red Flags identified in Section III, the Township personnel should take the following steps to monitor transactions with an existing Covered Account:

A. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via e-mail, or otherwise);

B. Verify the validity of requests to change billing addresses; and

C. Verify changes in banking information given for billing and payment purposes.

V. Preventing and Mitigating Identity Theft

Sensitive Information:

A. Township personnel are encouraged to use common-sense, judgment in securing sensitive and confidential information. Furthermore, in exercising such judgment, consideration should be given to the Illinois Freedom of Information Act (FOIA), when an employee contacts his or her supervisor or the program administrator. Further, if the Township receives a FOIA or other request seeking Sensitive Information, or documents containing Sensitive Information, said requests should be forwarded to the Township Supervisor, Township Administrator, and the Township Attorney.

B. In order to further prevent the likelihood of Identity Theft occurring with respect to the Township accounts, the Township shall make reasonable efforts to take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that the Township's website is secure;
2. Ensure destruction of paper documents and computer files containing Sensitive Information;
3. Keep file cabinets, desk drawers, and any other storage space containing documents with Sensitive Information locked when not in use;
4. Lock storage rooms containing documents with Sensitive Information and lock record retention areas at the end of the workday or when unsupervised;
5. Ensure that office computers with access to Covered Accounts and/or Sensitive Information are password protected and that computer screens lock after a set period of time;
6. Keep workstations, work areas, and offices clear of papers containing Sensitive Information at the end of the workday or when unsupervised
7. Request an individual's social security number only if, and when, necessary;
8. Ensure that computer virus protection is up-to-date;
9. Require and keep only Sensitive Information that is necessary for the Township's purposes; and
10. Account statements and receipts for Covered Accounts shall only include the last four digits of the credit card, debit card, or the bank account used for payment of the Covered Account.

Electronic Distribution

Each employee, service provider, or contractor performing work for the Township will comply with the following policies:

A. With respect to internal electronic distribution, Sensitive Information may be transmitted using approved Township's electronic mail.

B. With respect to external electronic distribution, Sensitive Information should only be transmitted in an encrypted format and should contain a statement such as the following:

"This message may contain sensitive, confidential and/or propriety information and is intended for the person/entity whom it was originally addressed. Any use by others is strictly prohibited."

Responding to Detected Red Flags.

In the event Township personnel detect any identified Red Flags, such personnel should take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Continue to monitor an account for evidence of Identity Theft;

B. Contact the customer to notify him/her of the potential data breach;

C. Change any passwords on computers or other security devices that permit access to Covered Accounts;

D. Decline or otherwise refuse to open a new Covered Account;

E. Reopen a Covered Account with a new number;

F. Notify the program administrator for determination of the appropriate steps to take;

G. Notify and cooperate with appropriate law enforcement; and/or

H. Determine that no response is warranted under the particular circumstances.

VI. Periodic Updates to Program

This Program will be periodically reviewed and updated reflect changes in risks to customers and the soundness of the Township from Identity Theft. At least annually, the Township'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 Township 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 revisions to reduce potential damages or losses to the Township and its clients. If warranted, the Township Administrator (or any delegated IT-manager and/or Program Administrator) will update the Policy and present it to the Township Board with recommended changes. The Township Board will make a determination of whether to accept, modify, or reject any recommended changes to the Program.

VII. Program Administration

Oversight

1. This Program Policy shall operate separately and shall not operate as an extension to existing fraud prevention programs; its importance warrants the highest level of attention.

2. Implementation of this Program Policy is the responsibility of the Township Administrator. The approval of the initial Policy by the Township Board is to be appropriately documented and maintained.

3. Oversight responsibility for this Program Policy may be delegated by the Township Administrator to a specific IT-manager and/or a specific Program Administrator.

Staff Training

Township personnel responsible for implementing the program shall be trained either by or under the direction of the Township Administrator or the designated Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Further, training shall also be provided on a yearly basis or as needed to address changes in the program.

Oversight of Service Provider Arrangements

In the event the Township engages a service provider to perform an activity in connection with one or more Covered Accounts, the Township will require, by contract, that services provided have such policies and procedures in place and require, by contract, that service providers review the program and report any Red Flags to the Township Administrator or Program Administrator to ensure that the service provider performs its activities in accordance with this Policy.

VIII. Specific Program Elements and Confidentiality

For the effectiveness of this Identity Theft Prevention Program Policy, the Red Flag Rules envision a degree of confidentiality regarding the Township's specific practices relating to Identity Theft detection, prevention, and mitigation. Therefore, under this Program Policy, knowledge of such specific practices is to be limited to the Township Administrator or the designated Program Administrator or those employees who need to know such specific practices for the purposes of preventing Identity Theft. Because this Program is to be adopted by the Township Board 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.