CHAPTER 20

IDENTITY PROTECTION AND IDENTITY THEFT PREVENTION POLICIES

1-20-1: PURPOSE:

The risk to the Village, its employees, residents, agents, service providers, 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. The purpose of this Chapter is to comply with 16 CFR §681.2 in order to detect, prevent, and mitigate identity theft by identifying, detecting, and responding to identity theft red flags and to comply with the Illinois Identity Protection Act (5 ILCS 179/1, et seq.) in order to protect social security numbers from unauthorized disclosure.

1-20-2: DEFINITIONS: For purposes of this Chapter, the following definitions apply:

ACT: The Illinois Identity Protection Act (5 ILCS 179/1, et seq.).

CORPORATE AUTHORITIES: The President and Board of Trustees of the Village.

COVERED ACCOUNT: (A) An account that the Village 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 (B) Any other account that the Village offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

CREDIT: The right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

CUSTOMER: A person that has a covered account with the Village.

IDENTITY THEFT: A fraud committed or attempted using identifying information of another person without authority.

PERSON: A natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

PUBLICLY POST OR PUBLICLY DISPLAY: To intentionally communicate or otherwise intentionally make available to the general public.

RED FLAG: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

SENSITIVE INFORMATION: Includes the following information:

(A) Credit card information, including any of the following:
  (1) Credit card number (in part or whole)
  (2) Credit card expiration date
  (3) Cardholder name
  (4) Cardholder address

(B) Tax identification numbers, including:
  (1) Social Security Number
  (2) Business Identification Number
  (3) State or Federal Employer Identification Number(s)

(C) Payroll information, including, among other information:
  (1) Paychecks
  (2) Pay stubs

(D) Other personal information belonging to any resident, agent, service provider, customer, employee, or contractor, including but not limited to:
  (1) Date of birth
  (2) Address
  (3) Phone numbers
  (4) Maiden name
  (5) Names
  (6) Customer number

SERVICE PROVIDER: A person that provides a service directly to the Village.

VILLAGE: The Village of Holiday Hills, McHenry County, Illinois.

1-20-3: SCOPE:

These policies and this protection program apply to employees, contractors, consultants, temporary workers, and other workers at the Village, including all personnel affiliated with third parties.

1-20-4: IDENTITY PROTECTION POLICY:

Pursuant to the Illinois Identity Protection Act (5 ILCS 179/1, et seq.) ("the Act"), in order to protect social security numbers (SSNs) from unlawful use and/or unauthorized disclosure, the following Identity Protection Policy is hereby adopted:

(A) The Village and all officers, employees, and agents will comply with the Act.

(B) All employees of the Village identified as having access to SSNs in the course of performing their duties for the Village will be trained to protect the confidentiality of SSNs. Training will include instructions on the proper handling of information that contains SSNs from the time of collection through the destruction of the information.

(C) Only employees who are required to use or handle information or documents that contain SSNs will have access to such information or documents.

(D) SSNs requested from an individual will be provided in a manner that makes the SSN easily redacted if required to be released as part of a public records request.

(E) All officers, employees, and agents of the Village will redact SSNs from the information or documents before allowing the public inspection or copying of the information or documents.

(F) When collecting a SSN or upon request by the individual, a statement of the purpose or purposes for which the agency is collecting and using the SSN will be provided.

(G) The Village and all officers, employees, and agents of the Village will not:

1. Publicly post or publicly display in any manner an individual's SSN.
2. Print an individual's SSN on any card required for the individual to access products or services provided by the person or entity.
3. Require an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted.
   Print an individual's SSN 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 SSN to be on the document to be mailed. Notwithstanding any provision to the contrary in this policy and the Act, SSNs 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 SSN. A SSN that is permissibly mailed under this policy and the Act will 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 being opened.

(H) Except as otherwise provided in this policy and the Act, the Village and all officers, employees, and agents will not:

1. Collect, use, or disclose a SSN 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 SSN is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the SSN is documented before collection of the SSN; and (iii) the SSN collected is relevant to the documented need and purpose.
2. Require an individual to use his or her SSN to access an Internet website.
3. Use the SSN for any purpose other than the purpose for which it was collected.

(I) Subsection (H) does not apply in the following circumstances:

1. The disclosure of SSNs to agents, employees, contractors, or subcontractors of the Village or disclosure by the Village to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the Village to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the Village will first request and receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed on the Village under this policy and the Act to protect an individual's SSN will be achieved, which policy shall be in a form acceptable to the Village.
2. The disclosure of SSNs pursuant to a court order, warrant, or subpoena.
3. The collection, use, or disclosure of SSNs in order to ensure the safety of: State and Village 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 Village facility.
4. The collection, use, or disclosure of SSNs for internal verification of administrative purposes.
5. The disclosure of SSNs by a State agency to the Village for the collection of delinquent child support or of any State debt or to the Village to assist with an investigation or the prevention of fraud.
6. The collection or use of SSNs 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.

(J) The Village and all officers, employees, and agents will not encode or embed a SSN in or on a card or document, including but not limited to, using a bar code, a chip, magnetic strip, or other technology, in place of removing the SSN as required by this policy and the Act.

(K) This policy and the Act do not apply to:

1. The collection, use, or disclosure of a SSN as required by State or federal law, rule or regulation.
2. 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.

(L) A written copy of this Identity Protection Policy will be filed with the President and Board of Trustees of the Village within thirty (30) days after approval of the policy by its incorporation into the Holiday Hills Village Code. The Village will advise its employees of the existence of this Policy and make a copy of this Policy available to each of its employees and will also make this Policy available to any member of the public, upon request. If this Policy is amended, then a written copy of the amended Policy will be filed with the President and Board of Trustees of the Village and all employees will be advised of the existence of the amended Policy, and a copy of the amended Policy will be made available to each of the Village's employees.

(M) In order to comply with the provisions of the Act, the Village will implement this Policy within twelve (12) months after the date this Identity Protection Policy is approved.

(N) To the extent that the standards for the collection, use, or disclosure of SSNs and identity protection are stricter than the standards under the Act with respect to the protection of those SSNs, then, in the event of any conflict with the provisions of the Act, the stricter standards adopted by the State or the Village shall control.

(O) This policy and the Act do not supersede any more restrictive law, rule, or regulation regarding the collection, use, or disclosure of SSNs.

1-20-5: IDENTITY THEFT PREVENTION POLICY:

Village personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this Chapter shall be read and interpreted in conjunction with the Illinois Freedom of Information Act and the Illinois Identity Protection Act. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their supervisor.

(A) Hard Copy Distribution: Each employee, contractor, and subcontractor performing work for the Village will comply with the following policies:

(1) File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

(2) Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

(3) Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.

(4) Whiteboards, dry-erase boards, writing tablets, etc., displaying any sensitive information, in common shared work areas will be erased, removed, or shredded when not in use.

(5) When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded. Municipal records, however, may only be destroyed in accordance with the Local Records Act and the Village's records retention policy.

(B) Electronic Distribution: Each employee, contractor, and subcontractor performing work for the Village will comply with the following policies:

(1) Internally, sensitive information may be transmitted using approved Village e-mail. All sensitive information must be encrypted when stored in an electronic format.

(2) Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

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

1-20-6: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM:

(A) Covered Accounts: A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

(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, operations, compliance, reputation, or litigation risks.

(B) Red Flags: The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it shall be investigated for verification:

(1) Alerts, notifications or warnings from a consumer reporting agency;

(2) A fraud or active duty alert included with a consumer report;

(3) A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

(4) A notice of address discrepancy from a consumer reporting agency as defined in Section 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

(5) Red flags also include consumer reports that indicate a pattern of activity 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.

(6) Suspicious Documents:

(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, such as a signature card or a recent check.
(e) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

(7) Suspicious Personal Identifying Information:

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

(i) The address does not match any address in the consumer report;
(ii) The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or

(iii) 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.

(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; or
(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.

(8) Unusual use of, or suspicious activity related to, the covered account:

(a) Shortly following the notice of a change of address for a covered account, the Village received 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.

1-20-7: RESPONDING TO RED FLAGS:

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

(1) Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the Village President, or his or her designee, for determination.

(2) The Village President, or his or her designee, will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

(B) If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include, but not be limited to:

(1) Canceling the transaction;

(2) Notifying and cooperating with appropriate law enforcement;

(3) Determining the extent of liability of the Village; and

(4) Notifying the actual customer that fraud has been attempted.

(5) Any other actions the Village President, or his or her designee, deems appropriate to further prevent or mitigate identity theft.

1-20-8: PERIODIC UPDATES TO THE PROGRAM:

(A) At periodic intervals as may be established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

(B) Periodic reviews will include an assessment of which accounts are covered by the program.

(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 damage to the Village and its customers.

(E) The Corporate Authorities may consider the following factors in exercising its discretion in amending the program:

(1) The Village's experiences with identity theft;

(2) Updates in methods of identity theft;

(3) Updates in customary methods used to detect, prevent, and mitigate identity theft;

(4) Updates in the types of accounts that the Village offers or maintains; and

(5) Updates in service provider arrangements.

1-20-9: PROGRAM ADMINISTRATION:

(A) Involvement of Management:

(1) The Identity Protection and the Identity Theft Prevention Program (hereinafter collectively known as "the Program") will not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.

(2) Operational responsibility for the program is delegated to the Village President, or any Village employee, official, or independent contractor to whom the Village President delegates such responsibility (i.e., his or her designee).

(3) The Village President, or his or her designee, shall report to the Corporate Authorities on the effectiveness of the program and the compliance with the regulatory requirements.

(4) The Village President, or his or her designee, may also propose recommendations or any amendments to the program to the Corporate Authorities.

(B) Staff Training:

(1) Staff training shall be conducted for all employees, officials and contractors who may reasonably be anticipated to come into contact with accounts or personally identifiable information that may constitute a risk to the Village or its customers, including but not limited to its employees, residents, agents, contractors, and/or service providers.

(2) The Village President, or his or her designee, may delegate staff training responsibilities to a person or persons who will be responsible for ensuring identify theft training for all requisite employees and contractors.

(3) The applicable Village employees should receive an initial training in all elements of this policy and additional training as changes to the program are implemented by the Corporate Authorities.

(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 the Illinois Identity Protection Act (5 ILCS 179/1, et seq.) 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.

(Ord. 314-11, Passed 05/16/11)