ILLINOIS DEPARTMENT OF THE LOTTERY

PERSONAL IDENTITY

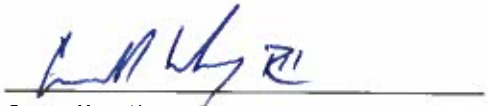
INFORMATION PROTECTION POLICY

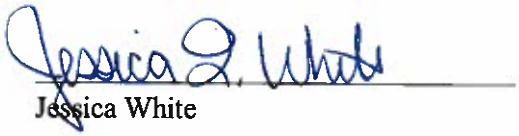
Effective Date: November 2019

Illinois Department of the Lottery
Personal Identity Information Protection Policy

APPROVAL SHEET

Acting Lottery Director:  Harold Mays Date: 11-15-19

General Counsel:  Cornell Wilson, III Date: 2019.11.12

Deputy General Counsel:  Jessica White Date: 11/12/2019

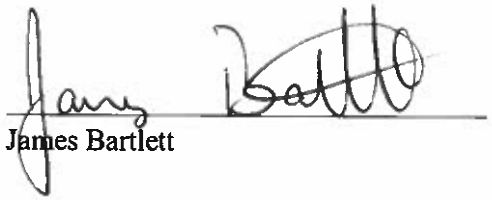
Acting Chief Operations & Technology Officer:  James Bartlett Date: 11/12/19

Table of Contents

POLICY STATEMENT

The Illinois Department of the Lottery (the "Department") establishes the Personal Identity Information Protection Policy (the "PII Policy") under the Identity Protection Act (5 ILCS 179) and the Personal Infonnation Protection Act (815 ILCS 530) (Collectively, the "Statutes") (See Exhibits Band C, respectively).

PURPOSE

The PII Policy ensures that the Department maintains the security, confidentiality, and integrity of the information it acquires from its retailers, employees, contractors, vendors, and customers. Under the Statutes the Department establishes guidelines and procedures to address the protection, collection and utilization of PII. (See Exhibit A)

SCOPE

The PII Policy applies to all information containing Personal Identity Information (defined below) and to all Department employees, vendors and contractors that have been granted access to resources containing Personal Identity Information (defined below). The tenns of the PII Policy intend to encompass the requirements of the Statutes. To the extent that the PII Policy conflicts with any Illinois or federal law, such law shall supersede the language of the PII Policy.

DEFINITIONS

"Breach" means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the Department.

"Disclosure" means permitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, or by electronic or any other means to any person or entity except the party identified as the party that provided or created the record.

"Identity Protection Act" pursuant to *5* ILCS 179/1 seeks to protect the identity of individuals by defining permissible and prohibited practices in the collection, use, and handling of social security numbers by the agencies of the State.

"Personal Identity Information or PU" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name

or the data elements are not encrypted or redacted: (a) Social Security number; (b) Driver's license number or State identification card number; (c) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) medical information (e) health insurance information, (f) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data, and (g) user name or email address, in combination with password or security question and answer that would permit access to an online account. PII does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

"Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the public.

RESPONSIBILITIES

1. Department employees, vendors and contractors are responsible for understanding and enforcing this policy.

2. Department employees, vendors and contractors are responsible for ensuring that all Personal Identity Information shall be used only for the purpose of conducting official state business.

3. Department management is responsible ensuring all Department employees, vendors and contractors who are granted access to PII in the course of performing their duties are properly trained regarding proper identification and protection of personal identity information, from time of collection through proper destruction.

4. The Department will post a copy of the PII Policy on its official website.

POLICY

1. **Data Collection.** Collection, use, or disclosure of PII from an individual on behalf of the Department is not allowed unless:

    (i) required under State or Federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is necessary for the performance of the employee, vendor or contractor's duties and responsibilities;

    (ii) the need and purpose for the PII is documented and communicated before collection of the PII; and

(iii) the PII collected is relevant to the documented need and purpose. Requiring an individual to use his or her PII to access an Internet website is also not allowed as is the use of PII for any purpose other than the purpose for which it was collected.

2. **Training.** All Department employees, vendors and contractors who have access to PII in the course of performing their duties must be trained to protect the confidentiality of PII. Training should include instructions on proper handling of information that contains PII from the time frame of collection through the destruction of the information.

3. **Redaction.** PII requested from an individual must be placed in a manner that makes the PII easily redacted if required to be released as part of a public records request. Public inspection and copying of documents containing social security numbers must be done in accordance with the Identity Protection Act.

4. **Disposal of Data.** Collected PII, electronic data or written material, that is no longer needed or required to be stored must be disposed of in such a manner as to ensure the security and confidentiality of the material and in accordance with the State Records Act (5 ILCS 160) and Personal Information Protection Act (815 ILCS 530/30 and 40).

5. **Restricted Access.** Only employees or contractors who are required to use or handle information or documents that contain PII shall have access to it. All PU obtained must be secured and stored in a manner that prevents and discourages public release. Controls shall be maintained to restrict network access to the electronic PII stored there. Physical PII must be secured (i.e. in a locked cabinet, file or office).

6. **Breach.** If PII has been disclosed via a Breach without being redacted, encrypted, or otherwise protected before exposure, the individuals shall be notified in accordance with the Personal Information Protection Act (815 ILCS 530/12 and 25). Breach does not include good faith acquisition of PII by an employee or agent of the Department for a legitimate purpose of the Department, provided that the personal information is not used for a purpose unrelated to the Department's business or subject to further unauthorized discJosure.

7. **Statement of Purpose.** When collecting a social security number or upon request by the individual, a statement of purpose or purposes for which the Department is collecting and using the social security number must be provided or posted where the individual can see and read the statement of purpose.

8. **Prohibited Activities.** Pursuant to the Identity Protection Act (5 ILCS179/10 and *5* ILCS 179/30, respectively) the following activities are prohibited by the Department unless circumstances exist as outlined in (5 ILCS 179/10 (c):

a. Publicly post or publicly display in any manner a person's social security or other PII.

b. Print a person's social security number or other PII on any card required for the person to access products or services provided by the Department.

c. Require a person to transmit his or her social security number or other PII over the Internet, unless the connection is secure or the PII data is encrypted.

d. Print a person's social security number or other PII on any materials that are mailed to the person, 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 PII to be on the document to be mailed. However, PII 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 tenninate an account, contract, or policy or to confirm the accuracy of the PII. A PII that is permissibly mailed 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 having been opened.

e. As of December 31, 2009, no person or State or local government agency may 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 Act. (5 ILCS 179/30)

9. **Protecting PII.** The following are ways of Protecting PII information:
   a. Use secure methodologies, such as encryption to electronically transmit sensitive PII information.
   b. Encrypt sensitive PII on mobile, computers, media and other devices.
   c. Lock or logoff unattended computer systems.
   d. Destroy sensitive paper PII by shredding or using bum bags.
   e. Delete sensitive PII by emptying electronic "recycle bin".
   f. Store sensitive PII on Government systems, only.
   g. Secure PII data properly while away from your desk or at the end of the day.

10. **Reporting PII Incidents.** What to do in case of a PII breach incident:

    a. Upon discovery/detection, immediately report a suspected or confirmed PII breach incident to your supervisor, DoIT, or Chief Privacy Officer (CPO).
    b. Provide details of the PII breach incident.

c. Maintain or document information and/or actions relevant to the PII breach incident.
d. Complete corrective or remedial actions, if appropriate.

11. **Coordination of PII.** Coordinating PII with the Freedom of Information Act (FOIA) and other laws (5 ILCS 140/1 et.seq.)

Illinois Lottery shall comply with the provisions of FOIA and any other state laws with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's SSN or other PU information. Nevertheless, Illinois Lottery shall redact SSN's and other PII information or documents before allowing the public inspection or copying of the information or documents. When collecting SSN's or other PII information, Illinois Lottery shall request each SSN or other PB information in the manner that makes SSN and PII easy to redact if required to be released as part of a public records request.

Exhibit A
Statement of Purpose for Collection of Certain Information

The Identity Protection Act. 5 ILCS 179/1 et seq., requires each local and State government agency to draft, approve, and implement an Identity Protection Policy that includes a statement of the purposes or purposes for which the agency is collecting, maintaining, and using a person's Social Security number (SSN). The Department of the Lottery also co1lects additional Personal Identity Information and therefore includes their collection, maintenance, and use within this statement of purpose.

The Department requires SSN or other Personal Identity Information to be provided for one or more of the following reasons:

- Claims processing
- Retailer licensing and debt collection
- Vendor/Contractor background checks in executing contracts
- Internal verification
- Administration services including payroll processing and hiring
- Compliance with Federal and State tax law and regulations
- Complaints, hearings or investigations
- Vendor services, such as billing

The Department will only use your SSN or other Personal Identity Information in accordance with the Department's Identity Protection Policy, available on the Illinois Lottery's website at http://illinoislotterv.com

ExhibitB
Identity Protection

Act (5 ILCS 179/1)

Sec 1. Short title. This Act may be cited as the Identity Protection Act.
(Source: P.A. 96 874. Eff. 6-1-10.)

(5 ILCS 179/5)
Sec. 5. Definitions. In this Act:

- **"Identity protection policy"** means any policy created to protect social security numbers from unauthorized disclosure.
- **"Local government agency"** means that term as it is defined in Section 1-8 of the Illinois State Auditing Act.
- **"Person"** means any individual in the employ of a State agency or local government agency.
- **"Publicly post"** or **"publicly display"** means to intentionally communicate or otherwise intentionally make available to the general public.
- **"State agency"** means that tenn as it is defined in Section 1 -7 of the Illinois State Auditing Act.

(Source: P.A. 96 874, eff. 6-1-10.)

(5 ILCS 179/10)
Sec. I0. Prohibited Activities

(a) Beginning July 1, 2010, no person or State or local government agency may do any of the following:

(1) Publicly post or publicly display in any manner an individual's social security number.
(2) Print an individual1s social security number 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 social security number over the Internet, unless the connection is secure, or the social security number is encrypted.
(4) 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 fonns 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 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 having been opened.

(b) Except as otherwise provided in this Act, beginning July 1, 2010, no person or State or local government agency may do any of the following:

(1) Collect, use, or disclose a social security number from an individual unless (i) required to do so under State or federal law, rule, 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 the social security number is documented before the collection of the social security number: and (iii) the social security number collected is relevant to the documented need and purpose.

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

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

(c) The prohibitions in subsection (b) do not apply in the following circumstances:

(1) 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 m 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 this Act on a governmental entity to protect an individual's social security number will be achieved.

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

(3) 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.

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

(5) 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.

(6) 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.

(d) If any State or local government agency has adopted standards for the collection, use, or disclosure of social security numbers that are stricter than the standards under this Act with respect to the protection of those social security numbers, then, in the event of any conflict with the provisions of this Act, the stricter standards adopted by the State or local government agency shall control.
(Source: P.A. 100-159, eff. 8-18-17.)

(S ILCS 179/15)
Sec. 15. Public inspection and copying of documents.

Notwithstanding any other provision of this Act to the contrary, a person or State or local government agency must comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's social security number. A person or State or local government agency must redact social security numbers the information or documents before allowing the public inspection or copying of the information or documents.
(Source: P.A. 96 874, eff. 6-1-10.)

(5 ILCS 179/20)
Sec. 20. Applicability.

(a) This Act does not apply to the collection, use or disclosure of a social security number as required by State or federal law, rule, or regulation.

(b) This Act 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. Notwithstanding this Section, county recorders must comply with Section 35 of this Act.
(Source: P.A. 96 874, eff. 6-1-10.)

(5 ILCS 179/25)
Sec. 25. Compliance with federal law.

If a federal law takes effect requiring any federal agency to establish a national unique patient health identifier program, any State or local government agency that complies with the federal law shall be deemed to be in compliance with this Act. (Source: P.A. 96 874, eff. 6-1 -10.)

(5 ILCS 179/30)
Sec. 30. Embedded social security numbers.

Beginning December 31, 2009, no person or State or local government agency may 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 Act.
(Source: P.A. 96874, eff. 6-1-10.)

(5 ILCS 179/35)
Sec. 35. Identity-protection policy; local government.

(a) Each local government agency must draft and approve an identity-protection policy within 12 months after the effective date of this Act. The policy must do all of the following:

(1) Identity this Act.
(2) Require all employees of the local government agency identified as having access to social numbers in the course of performing their duties to be trained to protect the confidentiality of social security numbers. Training should include instructions on the proper handling of information that contains social security numbers from the time of collection through the destruction of the information.
(3) Direct that only employees who are required to use or handle information or documents that contain social security numbers have access to such information or documents.
(4) Require that social security numbers requested from an individual 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.
(5) Require that, when collecting a social security number or upon request by the individual, a statement of the purpose or purpose for which the agency is collecting and using the social security number be provided.

(b) Each State agency must provide a copy of its identity protection policy to the Social Security Number Protection Task Force within days after the approval of the policy.

(c) Each State agency must implement the components of its identity - protection policy that are necessary to meet the requirements of this Act within 12 months after the date the identity protection policy is approved. This subsection (c) shall not affect the requirements of Section 10 of this Act.

(Source: P.A. 96 874, eff 6-1-10.)

(5 ILCS 179/40)

Sec. 40. Judicial branch and clerks of courts. The judicial branch and clerks of the circuit court are not subject to the provisions of this Act, except that the Supreme Court shall, under its rulemaking authority or by administrative order, adopt requirements applicable to the judicial branch, including clerks of the circuit court, regulating the disclosure of social security numbers consistent with the intent of this Act and the unique circumstances relevant in the judicial process.
(Source: P.A. 96-874, eff. 6-1-10.)

(5 ILCS 179/45)

Sec. 45. Violation. Any person who intentionally violates the prohibitions in Section 10 of this Act is guilty of a Class B misdemeanor.
(Source: P.A. 96 874, eff. 6-1-10.)

(5 (LCS 179/50)

Sec. 50. Home rule. A home rule unit of local govennnent, any non-home rule municipality, or any non-home rule county may regulate the use of social security numbers, but that regulation must be no less restrictive than this Act. This Act is a limitation under subsection (i) f Section 6 of Article VII of the Illinois Constitution on the concurrent exercise by home rule units of powers and functions exercised by the State.
(Source: P.A. 96-874, eff. 6-1-10.)

(5 ILCS 179/55)

Sec. 55. This Act does not supersede any more restrictive law, rule, or regulation regarding the collection, use, or disclosure of social security numbers.
(Source: P.A. 96 874, eff. 6-1-10.)

(5 ILCS 179/90)

Sec. 90 (Amendatory provisions; text omitted).
(Source: P.A. 96 874, eff. 6-1-10; text omitted.)

ExhibitC
Personal Information Protection Act

(815 ILCS 530/1)
Sec. l. Short title. This Act may be cited as the Personal Information Protection Act.
(Source: P.A. 94-36. eff. 1-1 -06.)

(815 ILCS 530/5)
Sec. 5. Definitions. In this Act:

"Data collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or **"breach"** means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data co1lector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

"Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application.

"Personal information" means either of the following:

(]) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) Social Security number.

(B) Driver's license number or State
(C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(D) Medical information
(E) Health insurance information
(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records. (Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/10)
Sec.IO. Notice of breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

{l) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) the toll-free numbers and addresses for consumer reporting agencies;
(B) the toll-free number, address, and website address for the Federal Trade Commission; and
(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form

directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.
(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency detennines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(l) written notice;
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
(3) Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact infonnation. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if thedata collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.
(Source: P.A. 99-503, eff. 1-1-17; 100-201, eff. 8-18-17.)

(815 ILCS 530/12)
Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. "The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to:

i the toll-free numbers and addresses for consumer reporting agencies,
ii the toll-free number, address, and website address for the Federal 'Trade Commission. and:
iii a statement that the individua] can obtain information mm these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents by the bleach. (a-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a crimina] investigation and provides the State agency with a written request for the delay. However. the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(b) For purposes of this Section. notice to residents may be provided by one of the following methods:

i written notice;
ii e]ectronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
iii substitute notice, if the State agency demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

1. email notice if the State agency has an email address for the subject persons;

2. conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and

3. notification to major statewide media.

(c) Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency sha11 also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681 a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(e) Notice to Attorney General. Any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including:

(A) The types of personal information compromised in the breach.
(B) The number of Illinois residents affected by such incident at the time of notification.
(C) Any steps the State agency has taken or plans to take relating to notification of the breach to consumers.
(D) The date and timeframe of the breach, if known at the time notification is provided. Such notification must be made within 45 days of the State agency's discovery of the security breach or when the State agency provides any notice to consumers required by this Section, whichever is sooner, unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the State agency shall send the Attorney General the date or timeframe of the breach as soon as possible.

(f) In addition to the report required by Section 25 of this Act, if the State agency that suffers a breach determines the identity of the actor who perpetrated the breach, then the State agency shall report this information, within *5* days after the determination, to the General Assembly, provided that such report would not jeopardize the security of Illinois residents or compromise a security investigation.

(g) A State agency directly responsible to the Governor that has been subject to or has reason to believe it has been subject to a single breach of the security of the data concerning the personal information of more than 250 Illinois residents or an instance of aggravated computer tampering, as defined in Section 17-53 of the Criminal Code of 2012, shall notify the Office of the Chief Information Security Officer of the Illinois Department oflnnovation and Technology and the Attorney General regarding the breach or instance of aggravated computer tampering. The notification shall be made without delay, but no later than 72 hours following the discovery of the incident.

Upon receiving notification of such incident, the Chief Information Security Officer shall without delay take necessary and reasonable actions to:

(i) assess the incident to determine the potential impact on the overall confidentiality, security, and availability of State of Illinois data and information systems;
(ii) ensure the security incident is contained to minimize additional impact and risk to the State;
(iii) identify the root cause of the incident;
(iv) provide recommendations to the impacted State agency to assist with eradicating the threat and removing and mitigating any vulnerabilities to reduce the risk of further compromise; and
(v) assist the impacted State agency in any necessary recovery efforts to ensure effective return to a state of normal operations.

The Department oflnnovation and Technology may agree to submit the reports required in subsections (e) and (f) of this Section and in Section 25 in lieu of the impacted agency.

(h) Upon receiving notification from a State agency of a breach of personal information or from the Department of Innovation and Technology in lieu of the impacted agency, the Attorney General may publish the name of the State agency that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.
(Source: P.A. 99-503, eff. 1-1-17; 100-412, eff. 8-25.17.)

(815 ILCS 530/15)
Sec. 15. Waiver. Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable.
(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/20)
Sec. 20. Violation. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.
(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/25)
Sec, 25. Annual reporting. Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the bleach 10 the General Assembly listing (he breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.
(Source: P.A. 94-947. eff 6-27-06.)

(815 [LCS 530/30)
Sec. 30. disposal of information. Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material.
(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/40)
Sec. 40. Disposal of materials containing personal information; Attorney General

a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:

    i) Paper documents containing personal infonnation may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

    ii) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.

c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third-party

hat contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit authorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposa] of materia]s containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any pena]ty imposed under this Section.

e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

f) A financial institution under 15 US.C. 6801 et. seq. or any person subject to 15 U.S.C. 6801 is exempt from this Section.
(Source: **P.A.** 97-483. Eff. 1-1-12.)

(815 ILCS 530/45)
Sec. 45. Data security.

(a) A data collector that owns, or licenses, or maintains, or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(b) A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(c) If a state or federal law requires a data collector to provide greater protection to records that contain persona] information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

(d) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section. (Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/50)
Sec. 50. Entities subject to the federal Health Insurance Portability and Accountability Act of 1996.

Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health infonnation established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Hea1th Act shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within *5* business days of notifying the Secretary. (Source: P.A. 99-503, eff. 1-1-17.)

(815 ILCS 530/900)
Sec. 900. (Amendatory provisions: text omitted). VIII

REVISION HISTORY

•Created: August 2014
•Revised: November 2019
•Reviewed: August 2022
•Effective: November 2019