PLEASE READ

The official text of New Jersey Statutes can be found through the home page of the New Jersey Legislature **http://www.njleg.state.nj.us/**

New Jersey Statutes Annotated (N.J.S.A.), published by Thomson West, provides the official annotated statutes for New Jersey.

The statutes in PDF form provided on this website by the Division of Consumer Affairs are unofficial courtesy copies, which may differ from the official text. Although every effort is made to ensure that the text of the courtesy copies is identical to the official version, if any discrepancies exist between the text on this website and the official version, the official version will govern.

Identity Theft Prevention Act
Table of Contents

56:8-161. Definitions relative to security of personal information.

As used in sections 10 through 15 of P.L.2005, c.226 (C.56:8-161 through C.56:8-166):

"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

"Business" means a sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.

"Communicate" means to send a written or other tangible record or to transmit a record by any means agreed upon by the persons sending and receiving the record.

"Customer" means an individual who provides personal information to a business.

"Individual" means a natural person.

"Internet" means the international computer network of both federal and non-federal interoperable packet switched data networks.

"Personal information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

For the purposes of sections 10 through 15 of P.L.2005, c.226 (C.56:8-161 through C.56:8-166), personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.

"Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, other than a public entity.

"Public entity" includes the State, and any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. For the purposes of sections 10 through 15 of P.L.2005, c.226 (C.56:8-161 through C.56:8-166), public entity does not include the federal government.

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

"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed, or electromagnetically transmitted. Records does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.

L.2005, c.226, s.10; amended 2019, c.95, s.1.

56:8-162. Methods of destruction of certain customer records.

A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable through generally available means.

L.2005, c.226, s.11.

56:8-163. Disclosure of breach of security to customers.

a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

d. For purposes of this section, notice may be provided by one of the following methods:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001); or

(3) Substitute notice, if the business or public entity 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 business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) E-mail notice when the business or public entity has an e-mail address;

(b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and

(c) Notification to major Statewide media.

e. Notwithstanding subsection d. of this section, a business or public entity 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 requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system.

f. In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s.1681a), of the timing, distribution and content of the notices.

g. (1) Notwithstanding subsection d. of this section, in the case of a breach of security involving a user name or password, in combination with any password or security question and answer that would permit access to an online account, and no other personal information as defined in section 10 of P.L.2005, c.226 (C.56:8-161), the business or public entity may provide the notification in electronic or other form that directs the customer whose personal information has been breached to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business or public entity and all other online accounts for which the customer uses the same user name or email address and password or security question or answer.

(2) Any business or public entity that furnishes an email account shall not provide notification to the email account that is subject to a security breach. The business or public entity shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the customer online when the customer is connected to the online account from an Internet Protocol address or online location from which the business or public entity knows the customer customarily accesses the account.

L.2005, c.226, s.12; amended 2019, c.95, s.2.

56:8-164. Prohibited actions relative to display of social security numbers.

a. No person, including any public or private entity, shall:

(1) Publicly post or publicly display an individual's Social Security number, or any four or more consecutive numbers taken from the individual's Social Security number;

(2) Print an individual's Social Security number on any materials that are mailed to the individual, unless State or federal law requires the Social Security number to be on the document to be mailed;

(3) Print an individual's Social Security number on any card required for the individual to access products or services provided by the entity;

(4) Intentionally communicate or otherwise make available to the general public an individual's Social Security number;

(5) Require an individual to transmit his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or

(6) Require an individual to use his Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site.

b. Nothing in this section shall prevent a public or private entity from using a Social Security number for internal verification and administrative purposes, so long as the use does not require the release of the Social Security number to persons not designated by the entity to perform associated functions allowed or authorized by law.

c. Nothing in this section shall prevent the collection, use or release of a Social Security number, as required by State or federal law.

d. Notwithstanding this section, Social Security numbers may be included in applications and forms sent by mail, including 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 is permitted to be mailed under this subsection may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been open.

e. Nothing in this section shall apply to documents that are recorded or required to be open to the public pursuant to Title 47 of the Revised Statutes. This section shall not apply to records that are required by statute, case law, or New Jersey Court Rules, to be made available to the public by entities provided for in Article VI of the New Jersey Constitution.

f. Nothing in this section shall apply to the interactive computer service provider's transmissions or routing or intermediate temporary storage or caching of an image, information or data that is otherwise subject to this section.

L.2005, c.226, s.13.

56:8-165. Regulations concerning security of personal information.

The Director of the Division of Consumer Affairs in the Department of Law and Public Safety, in consultation with the Commissioner of Banking and Insurance, shall promulgate regulations pursuant to the "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et seq.), necessary to effectuate sections 4 through 15 of this amendatory and supplementary act.

L.2005, c.226, s.14.

56:8-166. Unlawful practice, violation.

It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

L.2005, c.226, s.15.

56:8-166.1. Person, business, association prohibited from publishing certain information on the Internet.

a. A person, business, or association shall not disclose on the Internet the home address or unpublished home telephone number of a law enforcement officer or retired law enforcement officer under circumstances in which a reasonable person would believe that providing that information would expose another to harassment or risk of harm to life or property.

b. A person, business, or association that violates subsection a. of this section shall be liable to the law enforcement officer, retired law enforcement officer, or any other person residing at the home address of the law enforcement officer or retired law enforcement officer, who may bring a civil action in the Superior Court.

c. The court may award:

(1) actual damages, but not less than liquidated damages computed at the rate of $1,000 for each violation of this act;

(2) punitive damages upon proof of willful or reckless disregard of the law;

(3) reasonable attorney's fees and other litigation costs reasonably incurred; and

(4) any other preliminary and equitable relief as the court determines to be appropriate.

d. For the purposes of this section, "disclose" shall mean to solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, disseminate, present, exhibit, advertise or offer.

L.2015, c.226, s.3.

56:11-44. Short title.

This act shall be known and may be cited as the "Identity Theft Prevention Act."

L.2005, c.226, s.1.

56:11-45. Findings, declarations relative to identity theft.

The Legislature finds and declares that:

a. The crime of identity theft has become one of the major law enforcement challenges of the new economy, as vast quantities of sensitive, personal information are now vulnerable to criminal interception and misuse; and

b. A number of indicators reveal that, despite increased public awareness of the crime, incidents of identity theft continue to rise; and

c. An integral part of many identity crimes involves the interception of personal financial data or the fraudulent acquisition of credit cards or other financial products in another person's name; and

d. Identity theft is an act that violates the privacy of our citizens and ruins their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories; and

e. Credit reporting agencies and issuers of credit should have uniform reporting requirements and effective fraud alerts to assist identity theft victims in repairing and protecting their credit; and

f. The Social Security number is the most frequently used record keeping number in the United States. Social Security numbers are used for employee files, medical records, health insurance accounts, credit and banking accounts, university ID cards and many other purposes; and

g. Social Security numbers are frequently used as identification numbers in many computer files, giving access to information an individual may want kept private and allowing an easy way of linking data bases. Therefore, it is wise to limit access to an individual's Social Security number whenever possible; and

h. It is therefore a valid public purpose for the New Jersey Legislature to ensure that the Social Security numbers of the citizens of the State of New Jersey are less accessible in order to detect and prevent identity theft and to enact certain other protections and remedies related thereto and thereby further the public safety.

L.2005, c.226, s.2.

56:11-46. Election of placement of security freeze on consumer report, procedure.

a. A consumer may elect to place a security freeze on his consumer report by:

(1) making a request in writing by certified mail or overnight mail to a consumer reporting agency; or

(2) making a request directly to the consumer reporting agency through a secure electronic mail connection, if an electronic mail connection is provided by the consumer reporting agency.

b. A consumer reporting agency shall place a security freeze on a consumer report no later than five business days after receiving a written request from the consumer.

c. The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within five business days of placing the freeze and at the same time shall provide the

consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time.

d. If the consumer wishes to allow his consumer report to be accessed for a specific party or period of time while a freeze is in place, he shall contact the consumer reporting agency via certified or overnight mail or secure electronic mail and request that the freeze be temporarily lifted, and provide all of the following:

(1) Information generally deemed sufficient to identify a person;

(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection c. of this section; and

(3) The proper information regarding the third party who is to receive the consumer report or the time period for which the consumer report shall be available to users of the consumer report.

e. A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a consumer report pursuant to subsection d. of this section shall comply with the request no later than three business days after receiving the request.

f. A consumer reporting agency shall develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a consumer report pursuant to subsection d. of this section in an expedited manner. The director shall promulgate regulations necessary to allow the use of electronic media to receive and process a request from a consumer to temporarily lift a security freeze pursuant to subsection d. of this section as quickly as possible, with the goal of processing a request within 15 minutes of that request.

g. A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer report only in the following cases:

(1) Upon consumer request, pursuant to subsection d. or j. of this section; or

(2) If the consumer report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a consumer report pursuant to this paragraph, the consumer reporting agency shall notify the consumer in writing at least five business days prior to removing the freeze on the consumer report.

h. If a third party requests access to a consumer report on which a security freeze is in effect, and this request is in connection with an application for credit or any other use, and the consumer does not allow his consumer report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

i. (1) At any time that a consumer is required to receive a summary of rights required under section 609 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681g, the following notice shall be included:

New Jersey Consumers Have the Right to Obtain a Security Freeze

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to New Jersey law.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific party, parties or period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(i) The unique personal identification number or password provided by the consumer reporting agency;

(ii) Proper identification to verify your identity; and

(iii) The proper information regarding the third party or parties who are to receive the credit report or the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days or less, as provided by regulation, after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around, or specifically for a certain creditor, a few days before actually applying for new credit.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

(2) If a consumer requests information about a security freeze, he shall be provided with the notice provided in paragraph (1) of this subsection and with any other information, as prescribed by the director by regulation, about how to place, temporarily lift and permanently lift a security freeze.

j. A security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides the following:

(1) Proper identification; and

(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection c. of this section.

k. A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

l. The provisions of this section do not apply to the use of a consumer report by the following:

(1) A person, or subsidiary, affiliate, or agent of that person, or an assignee of a financial obligation owing by the consumer to that person, or a prospective assignee of a financial obligation owing by the consumer to that person in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument. For purposes of this paragraph, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements;

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection d. of this section, for purposes of facilitating the extension of credit or other permissible use;

(3) Any State or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, or subpoena;

(4) The Division of Taxation in the Department of the Treasury for the purpose of enforcing the tax laws of this State;

(5) A State or local child support enforcement agency;

(6) The use of credit information for the purposes of prescreening as provided for by the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681 et seq.;

(7) Any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed; or

(8) Any person or entity for the purpose of providing a consumer with a copy of the consumer's credit report upon the consumer's request.

m. (1) A consumer reporting agency shall not charge a consumer any fee to place a security freeze on that consumer's consumer report, or to remove or temporarily lift a security freeze on that consumer's consumer report.

(2) (Deleted by amendment, P.L.2018, c.153)

(3) (Deleted by amendment, P.L.2018, c.153)

L.2005, c.226, s.5; amended 2018, c.153, s.1.

56:11-47. Actions of consumer reporting agency relative to security freeze.

If a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a consumer report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file: name; date of birth; Social Security number; or address. Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or

transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and to the former address.

L.2005, c.226, s.6.

56:11-48. Inapplicability of sections 4 through 9 of act of resellers.

The provisions of sections 4 through 9 of this amendatory and supplementary act shall not apply to a consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the data base of another consumer reporting agency or multiple consumer reporting agencies, and does not maintain a permanent data base of credit information from which new consumer reports are produced, except that such a reseller of credit information shall honor any security freeze placed on a consumer report by another consumer reporting agency.

L.2005, c.226, s.7.

56:11-49. Entities not required to place security freeze in consumer report.

The following entities are not required to place a security freeze in a consumer report, pursuant to section 5 of this amendatory and supplementary act:

a. A check services company or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments; and

b. A demand deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a demand deposit account at the inquiring bank or financial institution.

L.2005, c.226, s.8.

56:11-50. Noncompliance, liability.

a. Any person who willfully fails to comply with the requirements of sections 4 through 9 of this amendatory and supplementary act shall be liable to a consumer as provided in section 11 of P.L.1997, c.172 (C.56:11-38).

b. Any person who is negligent in failing to comply with the requirements of sections 4 through 9 of this amendatory and supplementary act shall be liable to a consumer as provided in section 12 of P.L.1997, c.172 (C.56:11-39).

L.2005, c.226, s.9.

56:11-51. Denial, reduction of credit to victims of identity theft, certain, prohibited.

a. A creditor shall not deny credit to, or reduce the credit limit of, an individual solely because that individual was a victim of identity theft pursuant to N.J.S.2C:21-1, section 1 of P.L.1983, c.565 (C.2C:21-2.1) or N.J.S.2C:21-17. For purposes of this section, "victim of identity theft" means any

individual who, prior to or at the time of applying for credit, or for increasing the individual's credit limit, presents to a creditor:

(1) a copy of a police report filed pursuant to section 3 of P.L.2005, c.226 (C.2C:21-17.6); or

(2) either:

(a) a properly completed copy of a standardized affidavit of identity theft, as established by the Federal Trade Commission pursuant to section 609 of the federal "Fair Credit Reporting Act," Pub.L.91-508 (15 U.S.C. s.1681g); or

(b) a similar, duly executed affidavit concerning the victim's identity theft.

b. The provisions of subsection a. of this section shall not abrogate the right of a creditor to deny credit to, or reduce the credit limit of, a victim of identity theft for any other reason authorized by law.

L.2007, c.33, s.1.

56:11-52. Violations, penalties.

Any creditor who violates any provision of this act shall be liable for a penalty of not more than $5,000 for each violation, to be collected by and in the name of the Commissioner of Banking and Insurance in a summary proceeding pursuant to the "Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.).

L.2007, c.33, s.2.