56:11-44

LEGISLATIVE HISTORY CHECKLIST
Compiled by the NJ State Law Library

LAWS OF: 2005 **CHAPTER:** 226

NJSA: 56:11-44 ("Identity Theft Prevention Act")

BILL NO: A4001 (Substituted for S1914/2154/2155/2440/2441/2524)

SPONSOR(S): Watson Coleman and others

DATE INTRODUCED: May 5, 2005

COMMITTEE: **ASSEMBLY:** Consumer Affairs
SENATE:

AMENDED DURING PASSAGE: Yes

DATE OF PASSAGE: **ASSEMBLY:** June 23, 2005

SENATE: June 23, 2005

DATE OF APPROVAL: September 22, 2005

FOLLOWING ARE ATTACHED IF AVAILABLE:

FINAL TEXT OF BILL (Assembly Committee Substitute (1R) for A4001 enacted)

A4001

SPONSOR'S STATEMENT: (Begins on page 15 of original bill) Yes

COMMITTEE STATEMENT: **ASSEMBLY**: Yes

SENATE: No

FLOOR AMENDMENT STATEMENT: Yes

LEGISLATIVE FISCAL ESTIMATE: No

S1914/2154/2155/2440/2441/2524

SPONSOR'S STATEMENT (S1914): (Begins on page 6 of original bill) Yes
SPONSOR'S STATEMENT (S2154): (Begins on page 2 of original bill) Yes
SPONSOR'S STATEMENT (S2155): (Begins on page 2 of original bill) Yes
SPONSOR'S STATEMENT (S2440): (Begins on page 4 of original bill) Yes
SPONSOR'S STATEMENT (S2441): (Begins on page 4 of original bill) Yes
SPONSOR'S STATEMENT (S2524): (Begins on page 3 of original bill Yes

COMMITTEE STATEMENT: **ASSEMBLY**: No

SENATE: Yes

FLOOR AMENDMENT STATEMENT: Yes

LEGISLATIVE FISCAL ESTIMATE: No

VETO MESSAGE: No

GOVERNOR'S PRESS RELEASE ON SIGNING: Yes

FOLLOWING WERE PRINTED:

To check for circulating copies, contact New Jersey State Government Publications at the State Library (609) 278-2640 ext. 103 or mailto:refdesk@njstatelib.org

REPORTS: No

HEARINGS: No

NEWSPAPER ARTICLES: Yes

"Tougher laws to combat ID theft," 9-23-2005 The Record, p.A5
"Codey signs laws to help combat identity theft," 9-23-2005 Philadelphia Inquirer, p. B2
"Codey signs identity theft measure," 9-23-2005 Star Ledger, p.50
"New NJ laws guard against identity theft," 9-23-2005 Asbury Park Press, p.A1

IS 11/8/07

§§1,2,5-9 -
C.56:11-44 to
56:11-50
§3 - C.2C:21-17.6
§§10-15 -
C.56:8-161 to
56:8-166
§16 - Note to §§1-15

P.L. 2005, CHAPTER 226, ***approved September 22, 2005***
Assembly Committee Substitute ***(First Reprint)*** for
Assembly, No. 4001

AN ACT concerning identity theft, amending P.L.1997, c.172 and supplementing various parts of the statutory law.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. (New section) This act shall be known and may be cited as the "Identity Theft Prevention Act."

2. (New section) 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

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.
Matter enclosed in superscript numerals has been adopted as follows:
[1] Assembly floor amendments adopted June 20, 2005.

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.

3. (New section) a. A person who reasonably believes or reasonably suspects that he has been the victim of identity theft in violation of 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 may contact the local law enforcement agency in the jurisdiction where he resides, which shall take a police report of the matter and provide the complainant with a copy of that report. Notwithstanding the fact that jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, the local law enforcement agency shall take the complaint and provide the complainant with a copy of the complaint and may refer the complaint to a law enforcement agency in that different jurisdiction.

b. Nothing in this section shall interfere with the discretion of a local law enforcement agency to allocate resources for investigations of crimes. A complaint filed under this section is not required to be counted as an open case for purposes such as compiling open case statistics.

4. Section 3 of P.L.1997, c.172 (C.56:11-30) is amended to read as follows:

3. As used in this act:

"Adverse action" has the same meaning as in subsection (k) of section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer" means an individual.

"Consumer report" (1) means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

(a) credit or insurance to be used primarily for personal, family or household purposes;

(b) employment purposes; or

(c) any other purpose authorized under section 4 of this act.

(2) The term "consumer report" does not include:

(a) any:

(i) report containing information solely on transactions or experiences between the consumer and the person making the report;

(ii) communication of that information among persons related by common ownership or affiliated by corporate control; or

(iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among those persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that the information not be communicated among those persons;

(b) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;

(c) any report in which a person, who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer, conveys his decision with respect to that request, if the third party advises the consumer of the name and address of the person to whom the request was made, and the person makes the disclosures to the consumer required under 15 U.S.C. s.1681m; or

(d) communication excluded from the definition of consumer report pursuant to subsection (o) of section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility for the purpose of preparing or furnishing consumer reports.

"Director" means the Director of the Division of Consumer Affairs in the Department of Law and Public Safety.

"Division" means the Division of Consumer Affairs in the Department of Law and Public Safety.

"Employment purposes" means, when used in connection with a consumer report, a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

"File" means, when used in connection with information on any consumer, all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

"Investigative consumer report" means a consumer report or a portion thereof in which information on a consumer's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with neighbors, friends or associates of the consumer who is the subject of the report or with others with whom the

consumer is acquainted or who may have knowledge concerning any of those items of information. However, this information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when the information was obtained directly from a creditor of the consumer or from the consumer.

"Medical information" means information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.

"Security freeze" means a notice placed in a consumer's consumer report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing the report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer report.

(cf: P.L.1997, c.172, s.3)

5. (New section) 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 [1]**[**.**]** ;[1]

(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; [1]**[**or**]**[1]

(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. [1]**;**

(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.[1]

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

(2) A consumer reporting agency may charge a reasonable fee, not to exceed $5, to a consumer who elects to remove or temporarily lift a security freeze on that consumer's consumer report.

(3) A consumer may be charged a reasonable fee, not to exceed $5, if the consumer fails to retain the original personal identification number provided by the consumer reporting agency and must be reissued the same or a new personal identification number.

6. (New section) 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.

7. (New section) 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.

8. (New section) 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.

9. (New section) 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).

10. (New section) As used in sections 10 through 15 of this amendatory and supplementary act:

"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; or (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. 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 this amendatory and supplementary act, 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 this amendatory and supplementary act, 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.

11. (New section) 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 nonreconstructable through generally available means.

12. (New section) 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 [1]**[**consumer**]** customer[1] 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.

13. (New section) 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.

14. (New section) 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.

15. (New section) 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.

16. This act shall take effect on [1][the 180th day after] January 1 next following[1] enactment, except that section 3 of this act shall take effect immediately.

The "Identity Theft Prevention Act"

ASSEMBLY, No. 4001

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED MAY 5, 2005

Sponsored by:
Assemblywoman BONNIE WATSON COLEMAN
District 15 (Mercer)
Assemblyman JOSEPH CRYAN
District 20 (Union)
Assemblyman REED GUSCIORA
District 15 (Mercer)
Assemblyman JOSEPH VAS
District 19 (Middlesex)

Co-Sponsored by:
Assemblymen McKeon, Mayer, Steele, Morgan, Panter, Payne, Prieto and Chivukula

SYNOPSIS

"Identity Theft Prevention Act."

CURRENT VERSION OF TEXT

As introduced.

(Sponsorship Updated As Of: 6/17/2005)

AN ACT concerning identity theft, amending and supplementing P.L.1997, c.172 and supplementing Title 2C of the New Jersey Statutes and Title 56 of the Revised Statutes.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. (New section) This act may be known and shall be cited as the "Identity Theft Protection Act."

2. (New section) a. A person who has learned or reasonably suspects that he has been the victim of identity theft in violation of 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 may contact the local law enforcement agency that has jurisdiction over his actual residence, which shall take a police report of the matter, and provide the complainant with a copy of that report. Notwithstanding the fact that jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, the local law enforcement agency shall take the complaint and provide the complainant with a copy of the complaint and may refer the complaint to a law enforcement agency in that different jurisdiction.

b. Nothing in this section interferes with the discretion of a local law enforcement agency to allocate resources for investigations of crimes. A complaint filed under this section is not required to be counted as an open case for purposes such as compiling open case statistics.

3. (New section) a. A person who reasonably believes that he is the victim of identity theft in violation of 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 may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move for an expedited judicial determination of his factual innocence, where a defendant was charged with, arrested for or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against a defendant in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and intended to be omitted in the law.

Matter underlined <u>thus</u> is new matter.

offense for which a defendant was arrested, charged, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.

b. After a court has issued a determination of factual innocence pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

c. Upon making a determination of factual innocence, the court must provide the victim written documentation of such order.

d. A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

e. The Administrative Office of the Courts shall develop a form for use in issuing an order pursuant to this section.

f. The Administrative Office of the Courts shall establish and maintain a data base of persons who have been victims of identity theft and that have received determinations of factual innocence. The Administrative Office of the Courts shall provide a victim of identity theft or his authorized representative access to the data base in order to establish that the person has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and any other persons and agencies authorized by the victims.

g. The Administrative Office of the Courts shall establish and maintain a toll-free number to provide access to information under subsection f. of this section.

h. In order for a victim of identity theft to be included in the data base established pursuant to subsection f. of this section, he shall submit to the Administrative Office of the Courts a court order, a full set of fingerprints and any other information prescribed by the Administrative Office of the Courts.

i. Upon receiving information pursuant to subsection h. of this section, the Administrative Office of the Courts shall verify the identity of the victim against any driver's license or other identification record maintained by the New Jersey Motor Vehicle Commission.

4. Section 3 of P.L.1997, c.172 (C.56:11-30) is amended to read as follows:

3. As used in this act:

"Adverse action" has the same meaning as in subsection (k) of

section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer" means an individual.

"Consumer report" (1) means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

(a) credit or insurance to be used primarily for personal, family or household purposes;

(b) employment purposes; or

(c) any other purpose authorized under section 4 of this act.

(2) The term "consumer report" does not include:

(a) any:

(i) report containing information solely on transactions or experiences between the consumer and the person making the report;

(ii) communication of that information among persons related by common ownership or affiliated by corporate control; or

(iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among those persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that the information not be communicated among those persons;

(b) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;

(c) any report in which a person, who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer, conveys his decision with respect to that request, if the third party advises the consumer of the name and address of the person to whom the request was made, and the person makes the disclosures to the consumer required under 15 U.S.C. s.1681m; or

(d) communication excluded from the definition of consumer report pursuant to subsection (o) of section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility for the purpose of preparing or furnishing consumer reports.

<u>"Credit header information" means written, oral or other</u>

communication of any information by a consumer reporting agency regarding the Social Security number of the consumer, or any derivative thereof, and any other personally identifiable information of the consumer, except the name, address and telephone number of the consumer if all are listed in a residential telephone directory available in the locality of the consumer.

"Director" means the Director of the Division of Consumer Affairs in the Department of Law and Public Safety.

"Division" means the Division of Consumer Affairs in the Department of Law and Public Safety.

"Employment purposes" means, when used in connection with a consumer report, a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

"File" means, when used in connection with information on any consumer, all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

"Investigative consumer report" means a consumer report or a portion thereof in which information on a consumer's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with neighbors, friends or associates of the consumer who is the subject of the report or with others with whom the consumer is acquainted or who may have knowledge concerning any of those items of information. However, this information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when the information was obtained directly from a creditor of the consumer or from the consumer.

"Medical information" means information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.

"Security freeze" means a notice placed in a consumer's consumer report, at the request of the consumer, that prohibits the consumer reporting agency from releasing the report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer report.

(cf: P.L.1997, c.172, s.3)

5. (New section) a. A consumer may elect to place a security freeze on his consumer report by:

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

(2) making a telephone request by providing certain personal identifying information to a consumer reporting agency; or

(3) 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 or telephone request from the consumer or three business days after receiving a secure electronic mail 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 the freeze and 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, request that the freeze be temporarily lifted, and provide 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 in writing sent by mail 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. (1) A consumer reporting agency shall, within one year of the effective date of this section, develop secure:

(a) procedures that enable a consumer to use the telephone to request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section, within 24 hours of the consumer's telephone request; and

(b) procedures that enable a consumer to use the Internet, and, in the consumer reporting agency's sole and absolute discretion, other electronic media to request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section within 24 hours of the consumer's Internet or other electronic media request.

(2) A consumer reporting agency shall, within two years of the effective date of this section, develop secure:

(a) procedures that enable a consumer to use the telephone to

request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section, within six hours of the consumer's telephone request; and

(b) procedures that enable a consumer to use the Internet, and, in the consumer reporting agency's sole and absolute discretion, other electronic media, to request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section, within six hours of the consumer's Internet or other electronic media request.

(3) A consumer reporting agency shall, within three years of the effective date of this section, develop secure:

(a) procedures that enable a consumer to use the telephone to request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section, within one hour of the consumer's telephone request; and

(b) procedures that enable a consumer to use the Internet, and, in the consumer reporting agency's sole and absolute discretion, other electronic media, to request that the consumer reporting agency temporarily lift a freeze on the consumer report pursuant to subsection d. of this section, within five minutes of the consumer's Internet or other electronic media 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 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 at no charge 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 after receiving the request.

A security freeze does not apply to circumstances where 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 information 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 a 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) A State or local child support enforcement agency;

(5) 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.;

(6) The New Jersey Department of Health and Senior Services or its agents or assigns acting to investigate fraud;

(7) The New Jersey Department of the Treasury or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities;

(8) A person for the purposes of prescreening as defined by the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681 et seq.;

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

(10) Any person or entity for the purpose of providing a consumer with a copy of his or her credit report upon the consumer’s request.

m. (1) A consumer shall not be charged for any security freeze services, including but not limited to, the placement or lifting of a security freeze.

(2) A consumer may be charged a reasonable fee, not to exceed $5, if the consumer fails to retain the original personal identification number provided by the consumer reporting agency and must be reissued the same or a new personal identification number. A consumer, however, shall not be charged for the first reissue of his lost personal identification number.

n. (1) If a consumer reporting agency negligently or willfully violates the security freeze by releasing credit information that has been placed under a security freeze, the affected consumer shall be entitled to:

(a) Notification within five business days of the release of the information, including specificity as to the information released and the third party recipient of the information;

(b) File a complaint with the Federal Trade Commission and the Attorney General; and

(c) Civil relief against the consumer reporting agency, including, but not limited to, injunctive relief to prevent or restrain further violation of the security freeze, and a civil penalty in an amount not to exceed $10,000 for each violation plus any damages available under other civil laws, and reasonable expenses, court costs, investigative costs and attorney's fees.

(2) Each violation of the security freeze shall be counted as a separate incident for purposes of imposing penalties under this subsection.

6. (New section) 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 and 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.

7. (New section) The provisions of sections 5 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.

8. (New section) 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, which issues 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.

9. (New section) A consumer reporting agency shall not provide a consumer's credit header information unless the requester has a permissible purpose to obtain the consumer's consumer report pursuant to section 604 of the federal "Fair Credit Reporting Act," 15 U.S.C. 1681b.

10. (New section) As used in sections 10 and 11 of this amendatory and supplementary act:

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

"Individual" means a natural person.

"Personal information" 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:

(1) Social Security number;

(2) Driver’s license number or State identification card number;

(3) Account number, credit or debit card number, if circumstances exist where that number could be used without additional identifying information, access codes, or passwords; or

(4) Account passwords or personal identification numbers (PINs) or other access codes.

Any item listed above shall also constitute personal information when not used in connection with the individual’s first name or first initial and last name if that information was compromised and would be sufficient to perform or attempt to perform identity theft against that individual.

Personal information shall not include publicly available information that is lawfully made available to the general public from federal, State or local government records.

"Security breach" means the unauthorized acquisition of any data that compromises the security and confidentiality, or integrity of personal information maintained by the consumer reporting agency.

Good faith acquisition of personal information by an employee or agent of the consumer reporting agency for a legitimate purpose of the agency is not a security breach, provided that the personal information is not used for a purpose unrelated to the agency or subject to further unauthorized disclosure. A security breach of non-computerized data may include, but is not limited to, unauthorized photocopying, facsimiles or other paper-based transmittal of documents.

11. (New section) a. Except as provided in subsection b. of this section, any data collector that owns or uses personal information in any form that includes personal information concerning a New Jersey resident shall notify the resident that there has been a security breach related to that data following discovery or notification of the security breach, without regard for whether or not the data has or has not been accessed by an unauthorized third party for legal or illegal purposes. If the data collector does not own the information whose security was breached, the data collector shall notify the owner or licensee of the information of the security breach. The disclosure notifications 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 b. of this section, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data system.

b. The notification required by this section may be delayed if a law enforcement agency determines that the notification may impede a criminal investigation. The notification shall only be made after the law enforcement agency determines that it will not compromise the investigation.

c. 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 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 information. Substitute notice shall consist of all of the following:

(a) E-mail notice when the data collector has an e-mail address for the New Jersey resident whose personal information was affected by the breach;

(b) Conspicuous posting of the notice on the website page of the data collector, if the data collector maintains one; and

(c) Notification to major statewide media.

d. Any waiver of the provisions of this act is contrary to public policy, and is void and unenforceable.

e. Any individual injured by a violation of this section may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this section may be enjoined. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

12. (New section) As used in section 12 through 15 of this amendatory and supplementary act:

"Business" means sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity that destroys records.

"Dispose" means the discarding or abandonment of records containing personal information, and the sale, donation, discarding or transfer of any medium, including computer equipment, or computer media, containing records of personal information, or other non-paper media upon which records of personal information is stored, or other equipment for non-paper storage of information.

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, a name, signature, Social Security number, fingerprint, photograph or computerized image, physical characteristics or description, address, telephone number, passport number, driver's license or State identification card number, date of birth, medical information, bank account number, credit card number, debit card number or any other financial information.

"Records" means any material on which written, drawn, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics. Records do not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

13. (New section) Any business that conducts business in New Jersey and any business that maintains or otherwise possesses personal information of residents of New Jersey shall take all reasonable measures to protect against unauthorized access to or use of that information in connection with, or after its disposal. The reasonable measures shall include, but may not be limited to:

a. Implementing and monitoring compliance with polices and procedures that require the burning, pulverizing or shredding of papers containing

personal information so that the information cannot practicably be read or reconstructed;

b. Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other non-paper media containing personal information so that the information cannot practicably be read or reconstructed;

c. After due diligence, entering into and monitoring compliance with a written contract with another party engaged in the business of record destruction to dispose of personal information in a manner consistent with this amendatory and supplementary act. Due diligence should ordinarily include, but may not be limited to, one or more of the following: reviewing an independent audit of the disposal company's operations and its compliance with this amendatory and supplementary act; obtaining information about the disposal company from several references or other reliable sources and requiring that the disposal company be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal company; and

d. For disposal companies explicitly hired to dispose of records containing personal information: implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of personal information during or after the collection and transportation and disposing of such information in accordance with subsections a. and b. of this section.

14. (New section) Procedures relating to the adequate destruction or proper disposal of personal records must be comprehensively described and classified as official policy in the writings of the business entity, including corporate and employee handbooks and similar corporate documents.

15. (New section) a. Any person or business that violates the provisions of sections 12, 13 or 14 of this amendatory and supplementary act shall be liable for a civil penalty not to exceed $3,000 for each violation.

b. Any individual aggrieved by a violation of sections 12, 13 or 14 of this amendatory and supplementary act may bring a civil action in this State to enjoin further violations and to recover actual damages, costs and reasonable attorney's fees.

16. (New section) a. Except as provided in subsection b. of this section, no person, including any public or private entity, shall:

(1) Intentionally communicate or otherwise make available to the public an individual's Social Security number.

(2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person.

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

encrypted.

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

(5) 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.

(6) Sell, lease, loan, trade, rent, or otherwise disclose an individual's Social Security number to a third party for any purpose without written consent to the disclosure from the individual.

(7) Refuse to do business with an individual because the individual will not consent to the receipt by that person of the Social Security number of that individual, unless that person is expressly required under State or federal law, in connection with doing business with an individual, to submit to the State or federal government, as applicable, that individual's Social Security number.

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

17. (New section) a. Any person who negligently violates section 16 of this amendatory and supplementary act shall be liable for a civil penalty not to exceed $3,000 for each violation.

b. Any person who knowingly violates section 16 of this amendatory and supplementary act shall be guilty of a crime of the fourth degree and, notwithstanding the provisions of N.J.S.2C:43-3 and N.J.S.2C:43-6, punishable by imprisonment of not more than 15 days or a fine of not more than $5,000, or both.

c. A person aggrieved by a violation of section 16 of this amendatory and supplementary act may bring a civil action against the violator for recovery of actual damages or $5,000, whichever is greater, plus reasonable attorney's fees and court costs.

18. This act shall take effect on the 180th day after enactment, except that section 2 of this act shall take effect immediately.

STATEMENT

This bill allows victims of identity theft to obtain an official incident record from their local law enforcement agency if the victim has learned or reasonably suspects that he has been a victim of identity theft. The victim may contact their local law enforcement agency to make a complaint and provide the victim with a police report.

In addition, this bill establishes a procedure whereby a victim of

identity theft could obtain a factual determination of innocence and access a Statewide identity theft registry. Under the provisions of the bill, if a person reasonably believes that he is a victim of identity theft that person, or the court on its motion or upon application by the prosecuting attorney, may move for an expedited judicial determination of his factual innocence if a defendant has been arrested for, charged with or convicted of a crime under the victim's identity or where a criminal complaint has been filed against a defendant in the victim's name or if the victim's identity has been mistakenly associated with a record of criminal conviction. If the court determines that the petition or motion is meritorious and that the victim has not committed the offense, the court shall issue a judicial determination of factual innocence. After an order has been issued, the court may order that the name and personal identifying information of the victim contained in court records, files and indexes be deleted, sealed or labeled to show that the data is impersonated and does not reflect the defendant's identity.

This bill also requires the Administrative Office of the Courts (AOC) to establish and maintain a data base of persons who have been victims of identity theft and that have received determinations of factual innocence. Access to the data base would be limited to criminal justice agencies, victims of identity theft and any other persons and agencies authorized by the victims. The AOC would also be required to establish a toll-free number to provide access information to victims of identity theft.

This bill also amends and supplements the "New Jersey Fair Credit Reporting Act," to require that a consumer reporting agency place a security freeze on a consumer credit report within five business days of receiving a request to do so either in writing by certified mail or by a telephone request with certain accompanying personal identifying information; or within three business days of receiving a secure electronic mail request, and prohibits the release of information from the report while the freeze is in place, except as provided by the bill.

As defined in the bill, "security freeze" means a notice placed in a consumer's credit report, at the request of the consumer, that prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

The bill also provides that the consumer reporting agency shall provide notice to a consumer of the availability and mechanics of the security freeze in a notice, the form of which is provided in the bill, at any time a consumer is required to receive a summary of rights under section 609 of the federal "Fair Credit Reporting Act."

The bill requires a consumer reporting agency to provide a

consumer with an identification number to be used for temporarily lifting a freeze upon a consumer credit report or authorizing the subsequent release of information from a consumer credit report that is subject to a security freeze. Further, the bill stipulates that a security freeze shall remain in place until either the consumer requests to have the security freeze removed, or upon discovery by the consumer reporting agency that the consumer's credit report was frozen due to a material misrepresentation by the consumer. Also, if a third party requests access to a consumer credit report on which a security freeze is in effect, and this request is in connection with an application for credit or any other benefit, and the consumer does not allow the report to be accessed, the third party may treat the application as incomplete.

A consumer reporting agency shall be required to lift the security freeze within three business days of receiving a written request to do so. However, within one year of the effective date of this bill, a consumer reporting agency must have mechanisms in place to allow a consumer to lift the freeze by either use of the telephone or the Internet. If the telephone or Internet is used, the consumer reporting agency must lift the freeze within 24 hours of receiving the request. Within two years of the bill's effective date, the freeze must be lifted within six hours of a telephone or Internet request. Finally, within three years of the bill's effective date, a consumer reporting agency must lift the freeze within one hour of a telephone request and five minutes of an Internet request.

The bill also provides that when a security freeze is in place, a consumer reporting agency shall not modify any of the consumer's basic identifying information in the report without sending a written confirmation of the change to the consumer, including, in the case of an address change, a written confirmation sent to both the new and the former address. Also, the bill prohibits a consumer reporting agency from charging any fees to freeze, remove a freeze, or temporarily lift a freeze regarding access to a consumer credit report. However, a consumer reporting agency may charge up to $5 if a consumer fails to retain his personal identification number, but shall not charge for the first reissue of that number.

A consumer reporting agency that negligently or willfully violates the security freeze sections of the bill shall notify the consumer of the misconduct within five business days and may be subject to civil and injunctive penalties.

Any data collector that owns or uses personal information concerning a New Jersey resident shall notify the resident that there has been a security breach related to the data following discovery or notification of the breach. The disclosure notifications shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. The

disclosure may be delayed, however, if a law enforcement agency determines that notification will impede a criminal investigation.

Any data collector that maintains computerized data that includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery.

For purposes of this bill, notice may be written or electronic. 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 information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the data collector has an e-mail address; (2) conspicuous posting of the notice on the website page of the data collector, if the data collector maintains one; and (3) notification to major statewide media.

Any individual injured by a violation of the security breach section of the bill may institute a civil action to recover damages or injunctive relief.

This bill also requires any business that conducts business in New Jersey and any business that maintains or otherwise possesses personal information of New Jersey residents must take all reasonable measures to protect against unauthorized access to or use of that information in connection with or after its disposal. Further, the procedures used in the destruction and disposal of the personal records must be comprehensively described and classified as official policy in the writings of the business entity.

A violation of the destruction of records provisions of the bill shall be punishable by a civil penalty not to exceed $3,000 for each violation, injunctive relief and actual damages, costs and reasonable attorney's fees.

The bill also prohibits any person, including a public or private entity from: (1) intentionally communicating or otherwise making available to the public an individual's Social Security number; (2) printing an individual's Social Security number on any card required for the individual to access products or services provided by the person; (3) requiring an individual to transmit his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; (4) requiring an individual to use his Social Security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website; (5) printing 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; (6) selling, leasing, loaning, trading, renting, or otherwise disclosing an individual's Social Security number to a third party for any purpose

without written consent to the disclosure from the individual; or (7) refusing to do business with an individual because the individual will not consent to the receipt by that person of the Social Security number of that individual, unless that person is expressly required under State or federal law, in connection with doing business with an individual, to submit to the State or federal government, as applicable, that individual's Social Security number.

Unauthorized use of a Social Security number is punishable by a $3,000 fine for a negligent violation, and a $5,000 fine or up to 15 days imprisonment, or both, for knowingly violating this section. An aggrieved individual may recover actual damages or $5,000, whichever is greater, plus reasonable attorney's fees and court costs.

ASSEMBLY CONSUMER AFFAIRS COMMITTEE

STATEMENT TO

ASSEMBLY COMMITTEE SUBSTITUTE FOR
ASSEMBLY, No. 4001

STATE OF NEW JERSEY

DATED: JUNE 16, 2005

The Assembly Consumer Affairs Committee reports favorably an Assembly Committee Substitute for Assembly Bill No. 4001.

This Assembly Committee Substitute for Assembly Bill Number 4001, entitled the "Identity Theft Prevention Act," contains various provisions intended to combat identity theft and provide remedies for victims of identity theft.

This committee substitute allows victims of identity theft to obtain an official incident record from their local law enforcement agency if the victim reasonably believes or reasonably suspects that he has been a victim of identity theft. The victim may contact his local law enforcement agency to make a complaint. When a complaint is filed a copy of the complaint must be given to the victim.

This bill also amends and supplements the "New Jersey Fair Credit Reporting Act," to require that a consumer reporting agency place a security freeze on a consumer credit report within five business days of receiving a request to do so, and prohibits the release of information from the report while the freeze is in place, except as provided by the bill. As defined in the bill, "security freeze" means a notice placed in a consumer's credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

The bill further requires a consumer reporting agency to provide a consumer with an identification number to be used for temporarily lifting a freeze upon a consumer credit report or authorizing the subsequent release of information from a consumer credit report that is subject to a security freeze. Further, the bill stipulates that a security freeze shall remain in place until either the consumer requests to have the security freeze removed, or upon discovery by the consumer reporting agency that the consumer's credit report was frozen due to a material misrepresentation by the consumer. Also, if a third party requests access to a consumer credit report on which a

security freeze is in effect, and this request is in connection with an application for credit or any other benefit, and the consumer does not allow the report to be accessed, the third party may treat the application as incomplete.

If a consumer requests information about a security freeze or at any time a consumer is required to receive a summary of rights, as required under the federal "Fair Credit Reporting Act," the consumer shall be provided with the form notice provided in the substitute.

The bill also provides that when a security freeze is in place, a consumer reporting agency shall not modify any of the consumer's basic identifying information in the report without sending a written confirmation of the change to the consumer, including, in the case of an address change, a written confirmation sent to both the new and the former address.

Any business that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information must disclose any breach of security of those computerized records to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The substitute also provides that any business or public entity that compiles or maintains computerized records on behalf of another business or public entity shall notify that business or public entity, who must then notify its New Jersey customers of the breach.

This bill is not identical to the Senate Committee Substitute for Senate Bill Nos. 1914, 2154, 2155, 2400, 2441 and 2524, in that the Assembly Consumer Affairs Committee changed the language to specify that disclosure of a breach of security is not required if the business or public entity establishes that misuse of the information is not reasonably possible. This change also requires any such determinations to be documented in writing and retained for five years.

However, these disclosures may be delayed if a law enforcement agency determines that notification will impede a criminal or civil investigation. Further, any business or public entity required to disclose a breach of security of computerized records must first report the breach of security to the Division of State Police in the Department of Law and Public Safety for investigation on handling before disclosing to the customer.

For purposes of this bill, notice may be written or electronic. If the business 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 does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major Statewide media. However, a business 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 the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

In addition to any other disclosure or notification required under the bill, in the event that a business or public entity discovers circumstances requiring notification 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.

A business shall also be required to take all reasonable steps to destroy customer records, including paper records, within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means.

This bill also prohibits any person, or public or private entity, from using an individual's Social Security number in certain ways including: (1) publicly posting or publicly displaying an individual's Social Security number, or any four or more consecutive numbers contained in the individual's Social Security number; (2) printing 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) printing an individual's Social Security number on any card required for the individual to access products or services provided by the entity; (4) intentionally communicating or otherwise making available to the general public an individual's Social Security number; (5) requiring 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) requiring 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.

This bill does not 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 authorized or allowed by law or the release of a Social Security number, as required by State or federal law.

Social Security numbers may also 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 bill 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.

The bill's Social Security provisions do not apply to documents that are recorded or required to be open to the public pursuant to Title 47 of the Revised Statutes. That section of the bill also does 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.

Failure to comply with the security freeze provisions of this bill will be considered a failure to comply with the "New Jersey Fair Credit Reporting Act" and thus will be subject to the liability provisions of that act. A violation of the security breach or Social Security number provisions shall be an unlawful practice subject to the penalties applicable to a violation of the consumer fraud law pursuant to N.J.S.A.56:8-13. Under N.J.S.A.56:8-13, any business which violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.

Finally, the bill authorizes 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, to promulgate regulations to effectuate the provisions of this bill.

STATEMENT TO

ASSEMBLY COMMITTEE SUBSTITUTE FOR

ASSEMBLY, No. 4001

with Assembly Floor Amendments
(Proposed By Assemblywoman WATSON COLEMAN)

ADOPTED: JUNE 20, 2005

The Assembly Consumer Affairs Committee Substitute for Assembly Bill No. 4001 enacts the "Identity Theft Prevention Act."

These floor amendments would specify that a security freeze would not apply to a:

- person or entity administering a credit file monitoring subscription service to which the consumer has subscribed; or
- person or entity for the purpose of providing a consumer with a copy of the consumer's credit report upon the consumer's request.

These amendments also make a technical change which clarifies that the required disclosure is to be made to the customer. Finally, the amendments change the effective date from the 180th day after enactment to January 1 next following enactment.

SENATE, No. 1914

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED OCTOBER 4, 2004

Sponsored by:
Senator SHIRLEY K. TURNER
District 15 (Mercer)

Co-Sponsored by:
Senator Karcher

SYNOPSIS

Permits security freezes upon consumer credit reports.

CURRENT VERSION OF TEXT

As introduced.

(Sponsorship Updated As Of: 6/10/2005)

AN ACT concerning consumer credit reports, amending and supplementing P.L.1997, c.172.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. Section 3 of P.L.1997, c.172 (C.56:11-30) is amended to read as follows:

3. As used in this act:

"Adverse action" has the same meaning as in subsection (k) of section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer" means an individual.

"Consumer report" (1) means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

(a) credit or insurance to be used primarily for personal, family or household purposes;

(b) employment purposes; or

(c) any other purpose authorized under section 4 of this act.

(2) The term "consumer report" does not include:

(a) any:

(i) report containing information solely on transactions or experiences between the consumer and the person making the report;

(ii) communication of that information among persons related by common ownership or affiliated by corporate control; or

(iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among those persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that the information not be communicated among those persons;

(b) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;

(c) any report in which a person, who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer, conveys his decision with respect to that request, if the third party advises the consumer of the name and address of the person

EXPLANATION - Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and intended to be omitted in the law.

Matter underlined <u>thus</u> is new matter.

to whom the request was made, and the person makes the disclosures to the consumer required under 15 U.S.C. s.1681m; or

(d) communication excluded from the definition of consumer report pursuant to subsection (o) of section 603 of the federal "Fair Credit Reporting Act," 15 U.S.C. s.1681a.

"Consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility for the purpose of preparing or furnishing consumer reports.

"Director" means the Director of the Division of Consumer Affairs in the Department of Law and Public Safety.

"Division" means the Division of Consumer Affairs in the Department of Law and Public Safety.

"Employment purposes" means, when used in connection with a consumer report, a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

"File" means, when used in connection with information on any consumer, all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

"Investigative consumer report" means a consumer report or a portion thereof in which information on a consumer's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with neighbors, friends or associates of the consumer who is the subject of the report or with others with whom the consumer is acquainted or who may have knowledge concerning any of those items of information. However, this information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when the information was obtained directly from a creditor of the consumer or from the consumer.

"Medical information" means information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.

<u>"Security freeze" means a notice placed in a consumer's consumer report, at the request of the consumer, that prohibits the consumer reporting agency from releasing the report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that</u>

a security freeze is in effect with respect to the consumer report.
(cf: P.L.1997, c.172, s.3)

2. (New section) a. A consumer may elect to place a security freeze on his consumer report by making a request in writing by certified mail to a 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 10 business days and 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, request that the freeze be temporarily lifted, and provide 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 may 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.

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 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. If a consumer requests a security freeze, the consumer reporting agency shall disclose the process of placing and temporarily lifting a freeze, and the process for allowing access to information from the consumer report for a specific party or period of time while the freeze is in place.

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) A State or local child support enforcement agency; or

(5) 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.

m. Nothing in this act shall prevent a consumer reporting agency

from charging a reasonable fee, not to exceed $10, to a consumer who elects to freeze, remove the freeze, or temporarily lift the freeze regarding access to a consumer report.

3. (New section) 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 and 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.

4. (New section) The provisions of this 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.

5. (New section) The following entities are not required to place a security freeze in a consumer report, pursuant to section 2 of this act:

a. A check services company, which issues 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.

6. This act shall take effect on the 180th day following enactment.

STATEMENT

This bill amends and supplements the "New Jersey Fair Credit Reporting Act," to require that a consumer reporting agency place a

security freeze on a consumer credit report within five business days of receiving a request to do so in writing by certified mail, and prohibits the release of information from the report while the freeze is in place, except as provided by the bill. As defined in the bill, "security freeze" means a notice placed in a consumer's credit report, at the request of the consumer, that prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

The bill requires a consumer reporting agency to provide a consumer an identification number to be used for temporarily lifting a freeze upon a consumer credit report or authorizing the subsequent release of information from a consumer credit report that is subject to a security freeze. Further, the bill stipulates that a security freeze shall remain in place until either the consumer requests to have the security freeze removed, or upon discovery by the consumer reporting agency that the consumer's credit report was frozen due to a material misrepresentation by the consumer. Also, if a third party requests access to a consumer credit report on which a security freeze is in effect, and this request is in connection with an application for credit or any other benefit, and the consumer does not allow the report to be accessed, the third party may treat the application as incomplete.

The bill provides that when a security freeze is in place, a consumer reporting agency shall not modify any of the consumer's basic identifying information in the report without sending a written confirmation of the change to the consumer, including, in the case of an address change, a written confirmation sent to both the new and the former address. Also, the bill permits a consumer reporting agency to charge a reasonable fee to freeze, remove a freeze, or temporarily lift a freeze regarding access to a consumer credit report.

SENATE, No. 2154

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED DECEMBER 13, 2004

Sponsored by:
Senator WALTER J. KAVANAUGH
District 16 (Morris and Somerset)
Senator ANDREW R. CIESLA
District 10 (Monmouth and Ocean)

Co-Sponsored by:
Senator Singer

SYNOPSIS

Prohibits use of Social Security numbers for identification purposes except for internal verification.

CURRENT VERSION OF TEXT

As introduced.

AN ACT prohibiting the use of Social Security numbers for identification purposes under certain circumstances.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. For purposes of this act:

"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.

2. a. No person, including any public or private entity, shall require any individual to print or display in any manner that individual's Social Security number on any document, including but not limited to a license, permit, pass or certificate, for identification purposes, unless otherwise required in accordance with applicable State or federal law.

b. No person, including any public or private entity, shall require any individual to provide that individual's Social Security number over the telephone, Internet or via electronic mail, unless otherwise required to do so in accordance with applicable State or federal law.

c. 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 result in, or require the release of, the Social Security number to persons not designated by the public or private entity to perform associated functions authorized by law.

3. This act shall take effect on the 60th day following enactment.

STATEMENT

This bill prohibits any person, including any public or private entity, from requiring any individual to print or display in any manner that individual's Social Security number on any document, including but not limited to a license, permit, pass or certificate, for identification purposes. The bill further prohibits a public or private entity from requiring any individual to provide that individual's Social Security number over the telephone, Internet or via electronic mail unless otherwise required to do so in accordance with applicable State or federal law. The bill does not prevent a public or private entity from using a Social Security number for internal verification, so long as the

use does not result in, or require the release of, the Social Security number to persons not designated by the public or private entity to perform associated functions authorized by law.

SENATE, No. 2155

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED DECEMBER 13, 2004

Sponsored by:
Senator WALTER J. KAVANAUGH
District 16 (Morris and Somerset)
Senator ANDREW R. CIESLA
District 10 (Monmouth and Ocean)

Co-Sponsored by:
Senator Singer

SYNOPSIS

Prohibits business entities or institutions of higher education from using or displaying certain social security numbers under certain circumstances.

CURRENT VERSION OF TEXT

As introduced.

AN ACT prohibiting the use or display of social security numbers by business entities or institutions of higher education under certain circumstances.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. a. No business entity in the State shall assign an individual identification number to an individual which is identical to or incorporates the individual's social security number.

b. No business entity in the State shall allow the public display or use of an individual's social security number, or any four or more consecutive numbers contained in the individual's social security number.

c. Nothing in this section shall prohibit a business entity's use of an individual's social security number when required by applicable State or federal law.

2. a. No public or independent institution of higher education in the State shall assign an individual identification number to a student which is identical to or incorporates the student's social security number.

b. No public or independent institution of higher education in the State shall allow the public display or use of a student's social security number, or any four or more consecutive numbers contained in the student's social security number.

c. Nothing in this section shall prohibit a public or independent institution of higher education's use of a student's social security number when required by applicable State or federal law.

3. This act shall take effect on the 180th day after enactment.

STATEMENT

This bill prohibits a business entity in the State from assigning an individual identification number to an individual which is identical to or incorporates the individual's social security number. The bill also prohibits these business entities from allowing the public display or use of an individual's social security number, or any four or more consecutive numbers contained in the individual's social security number. In addition, the bill prohibits a public or independent institution of higher education in the State from assigning an individual identification number to a student which is identical to or incorporates the student's social security number. The bill also prohibits these institutions of higher education from allowing the public display or

use of a student's social security number, or any four or more consecutive numbers contained in the student's social security number.

SENATE, No. 2440

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED MARCH 21, 2005

Sponsored by:
Senator SHIRLEY K. TURNER
District 15 (Mercer)

SYNOPSIS

Requires businesses to disclose any breach of security of computer systems to customers and to destroy certain personal information no longer retained.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning the security of personal information retained by businesses.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. As used in this act:

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

"Business" means a sole proprietorship, partnership, corporation, association, or other group, 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.

"Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

"Individual" means a natural person.

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or non-driver identification card number, insurance policy number, education, employment history, bank account number, credit card number, debit card number, or any other financial information.

"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.

2. A business shall take all reasonable steps to 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, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

3. a. Any business that conducts business in New Jersey, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system within 15 days following discovery or notification of the breach in the security of the data to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be 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.

b. Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

c. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation.

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 15 U.S.C. § 7001; or

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

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

(b) Conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and

(c) Notification to major statewide media.

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

4. A violation of any provisions of this act shall be an unlawful practice subject to the penalties applicable pursuant to section 1 of P.L.1966, c.39 (C.56:8-13).

5. This act shall take effect on the 120th day following enactment.

STATEMENT

This bill requires a business to take all reasonable steps to destroy customer records within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means.

In addition, any business that conducts business in New Jersey and owns or licenses computerized data that includes personal information must disclose any breach of the security of the computer system within 15 days to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the disclosure may be delayed if a law enforcement agency determines that notification will impede a criminal investigation.

Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

For purposes of this bill, notice may be written or electronic. If the business 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 does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major Statewide media. However, a business 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 the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Finally, a violation of any provisions of this bill shall be an unlawful practice subject to the penalties applicable to a violation of the

consumer fraud law pursuant to N.J.S.A. 56:8-13. Under N.J.S.A. 56:8-13, any business who violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.

SENATE, No. 2441

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED MARCH 21, 2005

Sponsored by:
Senator BYRON M. BAER
District 37 (Bergen)

SYNOPSIS

Prohibits the use and display of Social Security numbers for certain identification purposes by public or private entities.

CURRENT VERSION OF TEXT

As introduced.

AN ACT prohibiting the use and display of Social Security numbers for certain identification purposes by public or private entities.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. The Legislature finds and declares that:

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

b. Computer records have replaced paper filing systems in most organizations. Since more than one person may share the same name, accurate retrieval of information works best if each file is assigned a unique number. Many businesses and government agencies believe the Social Security number is tailor-made for this purpose. However, with the rise in the crime of identity theft and other illegitimate uses of the Social Security number, this assumption is not valid; and

c. The crime of identity theft is increasing at epidemic proportions. With the Social Security number accessible to so many people, it is relatively easy for someone to fraudulently use a Social Security number to assume an individual's identity and gain access to their bank account, credit accounts, utilities records, and other sources of personal information; and

d. 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; therefore,

e. It is 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 thereby further the public safety.

2. For purposes of this act:

"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.

"Dispose" means the sale or transfer of a record for value to a company or business engaged in the business of record destruction.

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

"Personal information" means personally identifiable data about an individual's medical condition, if the data are not generally considered to be public knowledge; personally identifiable data which contain an

individual's account or identification number, account balance, balance owing, credit balance, or credit limit, if the data relate to an individual's account or transaction with a business; personally identifiable data provided by an individual to a business upon opening an account or applying for a loan or credit; or personally identifiable data about an individual's federal, State, or local income tax return.

"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 in the State. For purposes of this act, 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.

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

(1) Assign an individual identification number to an individual which is identical to or incorporates the individual's Social Security number.

(2) Publicly post or publicly display an individual's Social Security number, or any four or more consecutive numbers contained in the individual's Social Security number.

(3) 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.

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

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

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

(7) 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 result in, or require the release of, the Social Security number to persons not designated by the entity to perform associated functions authorized by law.

c. 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 entity takes all reasonable efforts to ensure that the individual's Social Security number is not released to the general public, including but not limited to, through the improper disposal or discarding of records.

d. An entity shall not discard or dispose of a record containing an individual's Social Security number unless the entity:

(1) Shreds the individual's record before discarding the record, or renders the record unreadable or irretrievable before discarding the device which contained the record; or

(2) Erases the personal information contained in the individual's record before discarding the record; or

(3) Modifies the individual's record to make the personal information unreadable before discarding the record; or

(4) Takes actions that it believes reasonable, and that is in conformance with industry standards, if any, to ensure that no unauthorized person will have access to the personal information contained in the individual's record.

4. It shall be an unlawful practice and a violation of P.L.1960, c.39 (C.56:8-1 et seq.) to violate any provision of this act.

5. This act shall take effect on the 180th day after enactment.

STATEMENT

This bill prohibits any person or public or private entity, from using an individual's Social security number in certain ways including: (1) assigning an individual identification number to an individual which is identical to or incorporates the individual's Social Security number; (2) publicly posting or publicly displaying an individual's Social Security number, or any four or more consecutive numbers contained in the individual's Social Security number; (3) printing 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; (4) printing an individual's Social Security number on any card required for the individual to access products or services provided by the entity; (5) intentionally communicating or otherwise making available to the general public an individual's Social Security number; (6) requiring an individual to transmit his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or (7) requiring 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.

The bill further requires an entity to take all reasonable efforts to ensure that an individual's Social Security number is not released to the general public, including but not limited to, through the improper disposal or discarding of records.

The bill requires that an entity must not discard or dispose of a record containing an individual's Social Security number unless it:

(1) shreds the individual's record before discarding the record, or renders the record unreadable or irretrievable before discarding the device which contained the record; or

(2) erases the personal information contained in the individual's record before discarding the record; or

(3) modifies the individual's record to make the personal information unreadable before discarding the record; or

(4) takes actions that it believes reasonable, and that is in conformance with industry standards, if any, to ensure that no unauthorized person will have access to the personal information contained in the individual's record.

SENATE, No. 2524

STATE OF NEW JERSEY

211th LEGISLATURE

INTRODUCED MAY 12, 2005

Sponsored by:
Senator JOSEPH F. VITALE
District 19 (Middlesex)

SYNOPSIS

Allows identity theft victims to apply for police incident record and judicial determination of factual innocence.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning identity theft and supplementing Title 2C of the New Jersey Statutes.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. a. A person who reasonably believes or reasonably suspects that he has been the victim of identity theft in violation of N.J.S. 2C:21-1, section 1 of P.L.1983, c. 565 (2C:21-2.1) or N.J.S.2C:21-17 may contact the local law enforcement agency in the jurisdiction where he resides, which shall take a police report of the matter and provide the complainant with a copy of that report. Notwithstanding the fact that jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, the local law enforcement agency shall take the complaint and provide the complainant with a copy of the complaint and may refer the complaint to a law enforcement agency in that different jurisdiction.

b. Nothing in this section shall interfere with the discretion of a local law enforcement agency to allocate resources for investigations of crimes. A complaint filed under this section is not required to be counted as an open case for purposes such as compiling open case statistics.

2. a. A person who reasonably believes that he is the victim of identity theft in violation of N.J.S. 2C:21-1, section 1 of P.L.1983, c. 565 (2C:21-2.1) or N.J.S.2C:21-17 may petition a court, or the court, on its own motion or upon application of the prosecuting attorney, may move for an expedited judicial determination of his factual innocence, where a defendant was charged with, arrested for or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against a defendant in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant and reliable information submitted by the parties or ordered to be part of the record by the court. Where the court determines that the petition or motion is meritorious and that there is no reasonable cause to believe that the victim committed the offense for which a defendant was arrested, charged, convicted, or subject to a criminal complaint in the victim's name, or that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.

b. After a court has issued a determination of factual innocence

pursuant to this section, the court may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public be deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

c. Upon making a determination of factual innocence, the court shall provide the victim written documentation of such order.

d. A court that has issued a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

e. The Administrative Office of the Courts shall develop a form for use in issuing an order pursuant to this section.

f. The Administrative Office of the Courts shall establish and maintain a database of persons who have been victims of identity theft and that have received determinations of factual innocence. The Administrative Office of the Courts shall provide a victim of identity theft or his authorized representative access to the database in order to establish that the person has been a victim of identity theft. Access to the database shall be limited to criminal justice agencies, victims of identity theft, and any other persons and agencies authorized by the victims.

g. The Administrative Office of the Courts shall establish and maintain a toll free number to provide access to information under subsection f of this section.

h. In order for a victim of identity theft to be included in the database established pursuant to subsection f. of this section, he shall submit to the Administrative Office of the Courts a court order, a full set of fingerprints and any other information prescribed by the Administrative Office of the Courts.

i. Upon receiving information pursuant to subsection h. of this section, the Administrative Office of the Courts shall verify the identity of the victim against any driver's license or other identification record maintained by the Department of Motor Vehicles.

3. This act shall take effect immediately.

STATEMENT

This bill would allow victims of identity theft to obtain an official incident record from their local law enforcement agency if the victim reasonably believes or reasonably suspects that he has been a victim of identity theft. The victim may contact his local law enforcement agency to make a complaint and provide the victim with a police report.

In addition, this bill would establish a procedure whereby a victim of identity theft could obtain a factual determination of innocence. The bill would also create a Statewide identity theft registry. Under the provisions of the bill, if a person reasonably believes that he is a victim of identity theft that person, or the court on its motion or upon application by the prosecuting attorney, may move for an expedited judicial determination of his factual innocence if a defendant has been arrested for, charged with or convicted of a crime under the victims identity or where a criminal complaint has been filed against a defendant in the victim's name or if the victim's identity has been mistakenly associated with a record of criminal conviction. If the court determines that the petition or motion is meritorious and that the victim has not committed the offense, the court shall issue a judicial determination of factual innocence. After an order has been issued, the court may order that the name and personal identifying information of the victim contained in court records, files and indexes be deleted, sealed or labeled to show that the data is impersonated and does not reflect the defendant's identity.

This bill would also require the Administrative Office of the Courts (AOC) to establish and maintain a database of persons who have been victims of identity theft and that have received determinations of factual innocence. Access to the database would be limited to criminal justice agencies, victims of identity theft and any other persons and agencies authorized by the victims. The AOC would also be required to establish a toll free number to provide access information to victims of identity theft.

SENATE COMMERCE COMMITTEE

STATEMENT TO

SENATE COMMITTEE SUBSTITUTE FOR

SENATE, Nos. 1914, 2154, 2155, 2440, 2441 and 2524

STATE OF NEW JERSEY

DATED: MAY 26, 2005

The Senate Commerce Committee reports favorably Senate Committee Substitute for Senate Bill Nos. 1914, 2154, 2155, 2440, 2441 and 2524.

This bill, a committee substitute entitled the "Identity Theft Prevention Act," contains various provisions intended to combat identity theft and provide remedies for victims of identity theft.

This committee substitute allows victims of identity theft to obtain an official incident record from their local law enforcement agency if the victim reasonably believes or reasonably suspects that he has been a victim of identity theft. The victim may contact his local law enforcement agency to make a complaint and provide the victim with a police report.

This bill also amends and supplements the "New Jersey Fair Credit Reporting Act," to require that a consumer reporting agency place a security freeze on a consumer credit report within five business days of receiving a request to do so, and prohibits the release of information from the report while the freeze is in place, except as provided by the bill. As defined in the bill, "security freeze" means a notice placed in a consumer's credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer, but does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

The bill further requires a consumer reporting agency to provide a consumer with an identification number to be used for temporarily lifting a freeze upon a consumer credit report or authorizing the subsequent release of information from a consumer credit report that is subject to a security freeze. Further, the bill stipulates that a security freeze shall remain in place until either the consumer requests to have the security freeze removed, or upon discovery by the consumer reporting agency that the consumer's credit report was frozen due to a material misrepresentation by the consumer. Also, if a third party requests access to a consumer credit report on which a

security freeze is in effect, and this request is in connection with an application for credit or any other benefit, and the consumer does not allow the report to be accessed, the third party may treat the application as incomplete.

If a consumer requests information about a security freeze or at any time a consumer is required to receive a summary of rights, as required under the federal "Fair Credit Reporting Act," the consumer shall be provided with the form notice provided in the substitute.

The bill also provides that when a security freeze is in place, a consumer reporting agency shall not modify any of the consumer's basic identifying information in the report without sending a written confirmation of the change to the consumer, including, in the case of an address change, a written confirmation sent to both the new and the former address.

Any business that conducts business in New Jersey or any public entity that compiles or maintains computerized records that include personal information must disclose any breach of security of those computerized records to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The substitute also provides that any business or public entity that compiles or maintains computerized records on behalf of another business or public entity shall notify that business or public entity, who must then notify its New Jersey customers of the breach.

However, these disclosures may be delayed if a law enforcement agency determines that notification will impede a criminal or civil investigation. Further, any business or public entity required to disclose a breach of security of computerized records must first report the breach of security to the Division of State Police in the Department of Law and Public Safety for investigation on handling before disclosing to the customer.

For purposes of this bill, notice may be written or electronic. If the business 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 does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major Statewide media. However, a business 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 the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

In addition to any other disclosure or notification required under the bill, in the event that a business or public entity discovers

circumstances requiring notification 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.

A business shall also be required to take all reasonable steps to destroy customer records, including paper records, within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means.

This bill also prohibits any person, or public or private entity, from using an individual's Social Security number in certain ways including: (1) publicly posting or publicly displaying an individual's Social Security number, or any four or more consecutive numbers contained in the individual's Social Security number; (2) printing 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) printing an individual's Social Security number on any card required for the individual to access products or services provided by the entity; (4) intentionally communicating or otherwise making available to the general public an individual's Social Security number; (5) requiring 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) requiring 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.

This bill does not 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 authorized or allowed by law or the release of a Social Security number, as required by State or federal law.

Social Security numbers may also 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 bill 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.

The bill's Social Security provisions do not apply to documents that are recorded or required to be open to the public pursuant to Title 47 of the Revised Statutes. That section of the bill also does 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.

Failure to comply with security freeze provisions of this bill will be considered a failure to comply with the "New Jersey Fair Credit Reporting Act" and thus will be subject to the liability provisions of that act. A violation of the security breach or Social Security number provisions shall be an unlawful practice subject to the penalties applicable to a violation of the consumer fraud law pursuant to N.J.S.A.56:8-13. Under N.J.S.A.56:8-13, any business which violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.

Finally, the bill authorizes 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, to promulgate regulations to effectuate the provisions of this bill.

STATEMENT TO

SENATE COMMITTEE SUBSTITUTE FOR

SENATE, Nos. 1914, 2154, 2155, 2440, 2441 and 2524

with Senate Floor Amendments
(Proposed By Senators BAER and TURNER)

ADOPTED: JUNE 20, 2005

These amendments remove language from the definition of "breach of security" in section 10 of the substitute bill, which provided that the acquisition of personal information or access thereto is not a breach of security if the business or public entity establishes, after a thorough investigation, that misuse of the information has not occurred and is not reasonably possible.

Instead, similar language was added to section 12 of the bill, which is the operative section that provides the steps a business or public entity must undertake if a breach of security occurs. The revised language provides that disclosure of a breach of security shall not be required if the business or public entity establishes that misuse of the information is not reasonably possible. In both cases, any determination by a business or public entity that a breach of security did not occur shall be documented in writing and retained for five years.

The amendments also exempt two additional entities from complying with the security freeze provisions of the bill. The exemption covers: (1) any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed; or (2) 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.

The amendments also make a technical amendment to the substitute to provide that a fraud prevention services company, which issues reports on incidents of fraud is not required to place a security freeze in a consumer report. While the substitute exempted a fraud prevention services company from being required to place a security freeze in a consumer report, it did not include the carve out "which issues reports on incidents of fraud."

Finally, the amendments provide that the effective date of the bill will be January 1 next following enactment.

PO BOX 004
TRENTON, NJ 08625

Contact: Kelley Heck
609-777-2600

RELEASE: September 22, 2005

Codey Signs Identity Theft Prevention Into Law

Bills help protect Social Security numbers, "good name" of state residents

(TRENTON) – Acting Governor Richard J. Codey today signed A4001/S1914, A2768 and A2769/S2617, bills that give consumers safeguards against identity theft.

"At the end of the day, New Jersey residents should feel assured that they are working for their families – not shameless impersonators who have targeted their nest egg," said Codey. "A good name is always worth protecting."

Codey signed the bills during a public ceremony at the Governor's Outer Office in the State House. Bill sponsors who joined the Acting Governor included Assembly members Bonnie Watson Coleman (D-Mercer), Reed Gusciora (D-Mercer), Joseph Vas (D-Middlesex) and Senators Shirley K. Turner (D-Mercer), Byron M. Baer (D-Bergen), Joseph F. Vitale (D-Middlesex) and Andrew R. Ciesla (R-Monmouth, Ocean). Other bill sponsors include Assemblymen Joseph Cryan (D-Union), Jeff Van Drew (D-Cape May, Cumberland), John S. Wisniewski (D-Middlesex), Neil M. Cohen (D-Union), Patrick Diegnan Jr. (D-Middlesex), Brian Stack (D-Hudson) and Senators Stephen M. Sweeney (D-Gloucester, Cumberland, Salem), Fred H. Madden (D-Camden, Gloucester) and Walter J. Kavanaugh (R-Somerset).

Bills A4001/S1914 – the "New Jersey Identity Theft Prevention Act" – would provide the following safeguards:

- Allow consumers to request that a reporting agency place a security freeze on their consumer credit report
- Affirm an individual's right to file and receive a copy of a police report concerning suspected identity theft
- Require any company that lawfully collects and maintains computerized records containing consumer's personal information to notify affected consumers in the event that personal data is compromised
- Limit use of a consumer's Social Security number as an identifier and prohibit public display and usage of the number on printed materials except where required by law
- Require businesses to destroy records containing a customer's personal information

that is no longer needed

The law will go into effect Jan. 1, 2006.

"The risk of identity theft continues to rise as weaknesses in data reporting and storage are exploited on a daily basis," said Watson Coleman. "Recent media headlines concerning lost information and security breaches affecting millions of consumers clearly illustrate why we need to take a stand and protect consumers against the fastest growing threat to their financial security and quality of life."

"So many people in our country don't know the power of their own Social Security numbers, but in the wrong hands, the economic impact can be extensive and lasting," said Turner. "Identity theft is insidious, invasive, and indiscriminate, striking at the young and old with equal voracity and in some cases causing irreparable damage to one's credit history. However, with greater oversight on how our identifying information is being handled in New Jersey, and the appropriate legal tools to prove a consumer's innocence, we can protect New Jersey's residents from identity theft."

"Particularly in light of the CitiGroup, North Jersey and BJ's incidents, we must provide New Jersey's consumers with the tools they need to protect themselves and the business community with guidelines to follow so they can prevent these devastating financial crimes," said Cryan.

"New incidents of security breaches and lost consumer data are constantly being reported in the media," said Gusciora. "We have an obligation to provide New Jersey residents and businesses with every tool possible to safeguard sensitive personal and credit information from unscrupulous individuals."

"The security of Social Security numbers and credit information is no laughing matter," said Vas. "As technology improves a would-be thief's chances of stealing someone's identity, we should empower consumers and businesses with a new and improved law to help mitigate the situation."

"With the spread of e-commerce and the passage of vulnerable identifying information over unsecured data lines, identity theft has grown from a minor occurrence to a lucrative criminal trade," said Vitale. "New Jersey needs to take every appropriate action to ensure that the innocent are not held culpable for the actions of an imposter. Under these new guidelines, it will be harder for criminals to steal someone's identity, and easier for innocent consumers to protect their good names."

"Identity theft is now the fastest-growing financial crime in our country, with nearly ten million Americans victimized in 2003 alone," said Kim Ricketts, Director of the Division of Consumer Affairs, the agency charged with enforcement of this statute. "The Identity Theft Prevent Act the Governor is signing today is the most comprehensive and easy-to-use identity theft prevention law in the nation, and I applaud Governor Codey for giving consumers the tools they need to protect their financial well-being."

Bill A2768 will expand the state's identity theft laws to include the selling, manufacturing possession or exhibiting of false birth certificates. The new measure will make it a second-degree crime to sell, offer to sell, or possess with the intent of selling a forged birth certificate. Convictions will be punishable by up to 10 years in prison and $150,000 in fines. The statute for forging a birth certificate would be consistent with punishment for manufacturing a false driver's license or other government documents. The law will go into effect immediately.

Bills A2769/S2617 will protect consumers from having their credit or ATM card information unwittingly taken from them. The new measure will prohibit the unauthorized use of scanning devices or re-encoders to access or scan the encoded information on any ATM, debit, credit or other payment card. The bill would also make it a crime to use a re-encoder to place the information encoded on the magnetic strip onto a different card without permission. A re-encoder is a device that places encoded information from the magnetic strip of a payment card onto the magnetic strip or stripe of a different payment card. The law will go into effect immediately.

"Anyone who gets their hands on a re-encoder can become an identity thief; it could be a gas station attendant or a server at your favorite restaurant," said Sweeney. " By banning re-encoders we are working to help eliminate identity theft while saving consumers millions of dollars in fraudulent debt."

"Consumers deserve to be able to shop without the fear of identity theft," said Madden. "This law will help combat credit card fraud by making it more difficult for thieves to use re-encoders to steal identities, and help give consumers peace of mind while they are shopping."