NEW JERSEY REGISTER
VOLUME 40, ISSUE 7
ISSUE DATE: APRIL 7, 2008
RULE ADOPTIONS
LAW AND PUBLIC SAFETY
DIVISION OF CONSUMER AFFAIRS

Adopted New Rules: N.J.A.C. 13:45F

Identity Theft

Proposed: April 16, 2007 at 39 N.J.R. 1397(a).

Adopted: February 21, 2008 by Lawrence DeMarzo, Acting Director, Division of Consumer Affairs, in consultation with Steven M. Goldman, Commissioner, Department of Banking and Insurance.

Filed March 3, 2008 as R.2008 d.80, with substantive and technical changes not requiring additional public notice or comment (N.J.A.C. 1:30-6.3) and with proposed N.J.A.C. 13:45F-3 and 5.2(b) not adopted.

Authority: N.J.S.A. 56:11-44 to 50 and 56:8-161 to 166.
Effective Date: April 7, 2008.
Expiration Date: April 7, 2013.

Summary of Agency-Initiated Change:

The Division has amended the language of N.J.A.C. 13:45F-4.1(g) (proposed (f)) to address a public entity's duty to affirmatively state the use to which a Social Security number will be put when requesting a Social Security number from an individual, rather than disclose the use only when requested to do so. The Division has made this change based on the requirements of the Federal Privacy Act at 5 U.S.C. ß552 note (b).

Federal Standards Statement

Certain Federal statutes and regulations have been cited in the Act and these rules. The rules do not exceed the Federal requirements. Rather, they cite to the Federal statutes and regulations and require that the cited provisions be followed. The Federal statutes cited in these rules include various provisions of the Fair Credit Reporting Act, 15 U.S.C. ßß1681 et seq. The rules of Subchapter 4 are not intended to obviate prohibitions in any Federal statutes or regulations.

Full text of the adopted new rules follows (additions to proposal indicated in boldface with asterisks *thus*; deletions from the proposal indicated in brackets with asterisks *[thus]*):

CHAPTER 45F
IDENTITY THEFT

SUBCHAPTER 1. PURPOSE, SCOPE AND DEFINITIONS

13:45F-1.1 Purpose

This chapter is promulgated by the Director under the Identity Theft Prevention Act (the ITPA), N.J.S.A. 56:11-44 et seq. The rules address the obligations of a consumer reporting agency to New Jersey consumers regarding placing, lifting or removing a security freeze on a consumer report under the ITPA at N.J.S.A. 56:11-46 et seq. *[In addition, the rules set forth the duties of businesses and public entities that are subject to the provisions of the ITPA governing breaches in computer security and destruction of records containing personal information under the ITPA at N.J.S.A. 56:8-161, 162 and 163.]* Further, the rules address prohibited uses of Social Security numbers and the manner in which Social Security numbers may be given in a public setting under the ITPA at N.J.S.A. 56:8-164. Finally, the rules address the

penalties for violations of the security freeze and breach of security provisions under the ITPA at N.J.S.A. 56:8-166 and 56:11-50.

13:45F-1.2 Scope

This chapter applies to consumer reporting agencies that maintain consumer reports on New Jersey residents*[, every business doing business in New Jersey and every New Jersey public entity that possesses the computerized personal information of New Jersey residents, every business or public entity that holds records containing personal information that are to be destroyed]* and any public or private entity or person who has access to the Social Security numbers of New Jersey residents.

13:45F-1.3 Definitions

For the purposes of this chapter, the following words and terms shall have the following meanings, unless the context clearly indicates otherwise:

*["Affected individual" means 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.

"Breach of security" means unauthorized access to electronic files, including those stored on laptops, MP3 players, personal digital assistants or any other high capacity storage device, media or data containing personal information that compromises the security, confidentiality, integrity or availability of personal information when access to personal information has not been secured by security measures at least meeting the standards set forth in N.J.A.C. 13:45F-3.2 or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an authorized employee or agent of a 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 and the authorized employee or agent is using the information for purposes for which it was provided.

"Business" means a sole proprietorship, partnership, corporation, association, or other entity however organized and whether or not organized to operate at a profit that does business in New Jersey and compiles or maintains computerized records that include personal information on New Jersey residents, 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 any other country, or the parent or the subsidiary of a financial institution. For purposes of N.J.A.C. 13:45F-3.5, the definition of business includes entities that possess either computerized records or other records, as defined in this section, containing personal information.]*

"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.

["Computerized records" means records stored in, or transmitted from, a computer and any materials produced from or organized by a computer as well as those maintained in storage devices related to computers, such as, but not limited to, hard drives, diskettes, memory sticks and flash memory cards.]

"Consumer" means an individual.

"Consumer report" 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 that 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:

1. Credit or insurance to be used primarily for personal, family or household purposes;

2. Employment purposes; or

3. Any other purpose authorized under the New Jersey Fair Credit Reporting Act, P.L. 1997, c. 172 ß4.

The term "consumer report" does not include:

1. Any report containing information solely on transactions or experiences between the consumer and the person making the report, communication of that information among persons related by common ownership or affiliated by corporate control, or 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;

2. Any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;

3. 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 or her 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. ß1681m, incorporated herein by reference as may be amended and supplemented; or

4. Communication excluded from the definition of consumer report pursuant to subsection (o) of section 603 of the Fair Credit Reporting Act, 15 U.S.C. ß1681a, incorporated herein by reference, as may be amended and supplemented.

"Consumer reporting agency" means all consumer reporting agencies that compile or maintain flies on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the Fair Credit Reporting Act, 15 U.S.C. ß1681a, incorporated herein by reference, as may be amended and supplemented.

["Customer" means an individual, including an employee of the business or public entity, who, directly or indirectly, through one or more intermediaries, has provided personal information to a business or about whom a public entity compiles or maintains personal information.]

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

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

*["Dissociated data" means data elements stored separately which, if linked, associates an individual's name with one or more elements of the individual's personal information.

"Encryption" means a process for converting information from its normal comprehensible form into an incomprehensible format that renders it unreadable without knowledge of a confidential code. For the purposes of this chapter, data will not be considered encrypted unless it meets the standard for encryption set forth in N.J.A.C. 13:45F-3.2.

"Hardware firewall" means a physical device to prevent unauthorized access to a system containing personal information.]*

"Individual" means a natural person.

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

"Official information" means individual's name, address, date of birth or Social Security number.

"Person" means a natural person, partnership, corporation, company, trust, firm, business entity or association.

*["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. A Social Security number;

2. A driver's license number or state identification card number; or

3. An account number or credit or debit card number in combination with any requited security code, access code, password security question, or authentication device that would permit access to an individual's bank account, investment account or other financial account.

Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data was accessed in connection with access to the dissociated data. For purposes of N.J.A.C. 13:45F-3, 4 and 5, personal information does 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.]*

"Plain language" means language presented in a simple, clear, understandable and easily readable manner.

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

"Public entity" means the State, any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State. *[For purposes of N.J.A.C. 13:45F-3 and 5, a public entity means the State, any county, municipality, district, public authority, public agency, and any other political subdivision or public body in the State that compiles or maintains computerized records that include personal information on a New Jersey resident.]* For purposes of this chapter, 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, digitized or electromagnetically transmitted. Records do not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed.]

"Security freeze" means a notice placed in a consumer's consumer report, at the request of the consumer that, subject to certain exceptions as set forth in N.J.S.A. 56:11-46(l), 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.

["Software firewall" means application-based protection to prevent unauthorized access to a system containing confidential information.]

SUBCHAPTER 2. SECURITY FREEZE PROVISIONS

13:45F-2.1 Providing information to consumers about a security freeze

(a) Each consumer reporting agency shall provide to consumers:

1. Complete, easily accessible information *presented* in plain *[English]* *language* about how to place, lift and remove a security freeze on a consumer report including:

i. All identifying information that the consumer reporting agency requires from a consumer to place,

temporarily lift or remove a security freeze on a consumer report;

ii. The methods by which a consumer can make a request to the consumer reporting agency to place, temporarily lift or remove a security freeze on a consumer report, which may be a written request by certified or overnight mail or secure electronic mail, or, where the freeze is being temporarily lifted or removed, by secure electronic media;

iii. A notice that a consumer must place a security freeze with each consumer reporting agency separately;

iv. The amount of any fee to temporarily lift or remove a security freeze and the methods of payment accepted by the consumer reporting agency; and

v. Information on the procedures to replace a lost personal identification number (PIN) or password; and

2. A toll-free telephone number that, if automated, includes a separate prompt on the menu for information about placing, lifting and removing a security freeze on a consumer report. This toll-free number must afford the consumer, during regular business hours, eastern time, access to a person who can supply any additional information needed by the consumer.

(b) Each consumer reporting agency shall place the information set forth in (a) above on its website, including *[an obvious]* *a conspicuous* link to that information on its home page. Each consumer reporting agency also shall *[supply the information to consumers in writing]* *mail the information in (a) above to consumers*, along with the notice "New Jersey Consumers Have the Right to Obtain a Security Freeze" set forth at N.J.S.A. 56:11-46i(1), when:

1. The consumer requests information about placement of a security freeze pursuant to N.J.S.A. 56:11-46i(2);

2. The consumer requests a copy of his or her *[credit]* *consumer* report; or

3. The consumer is entitled to receive a summary of rights required under ß609 of the Fair Credit Reporting Act, 15 U.S.C. ß1681g, incorporated herein by reference, as may be amended and supplemented.

(c) Each consumer reporting agency, *[(within 10 days of the effective date of this chapter)]* *by April 17, 2008*, shall send in writing, via e-mail to creditinfo@dca.lps.state.nj.us and regular mail to the Press Office, New Jersey Division of Consumer Affairs, 124 Halsey Street 7th floor, Newark, NJ 07101, the information required to be provided to consumers under (a)1i, ii, iv and v and 2 above.

(d) The consumer reporting agency shall communicate in writing, via e-mail and regular mail, any changes to the information supplied to the Division under (c) above within 10 days of implementation of the change.

13:45F-2.2 Placing a security freeze

(a) Upon receipt of a consumer's *written* request to place a security freeze on his or her consumer report made in accordance with the procedures provided in N.J.A.C. 13:45F-2.1(a), a consumer reporting agency shall, within five business days of receipt:

1. Place the security freeze on the consumer report;

2. Send a written confirmation of the security freeze to the consumer together with instructions on the procedures used by the consumer reporting agency to temporarily lift or remove a security freeze, and a toll-free number that a consumer may use for any further questions; *and*

3. Provide the consumer with a unique PIN or password, other than the consumer's Social Security number *[or portion thereof,]* *or any four or more consecutive numbers of the Social Security number* or data element comprising *[personal]* *identifying* information, to be used by the consumer when providing authorization for the release of his or her credit information for a specific party or period of time *[or for other communications with the consumer reporting agency such as, but not limited to, those set forth in

N.J.A.C. 13:45F-2.3, Temporarily lifting a security freeze; 2.4, Removing a security freeze; 2.5, Changing official information]* *or communications with the consumer reporting agency when temporarily lifting a security freeze (N.J.A.C. 13:45F-2.3), removing a security freeze (N.J.A.C. 13:45F-2.4) or changing official information (N.J.A.C. 13:45F-2.5).**[; and

4. Provide a copy of the notice "New Jersey Consumers Have the Right to Obtain a Security Freeze" set forth at N.J.S.A. 56:11-46i(1).]*

13:45F-2.3 Temporarily lifting a security freeze

(a) Upon receipt of a consumer's request to temporarily lift a freeze sent by certified or overnight mail or such system of secure electronic media as may be made available by the consumer reporting agency, the consumer reporting agency shall:

1. Lift the freeze if the consumer has properly supplied the following:

i. The information necessary for proper identification specified in the information given to the consumer pursuant to N.J.A.C. 13:45F-2.1; and

ii. The information to identify the specific third party granted access or the time period for which the consumer report is to be made available;

2. Supply a PIN to the consumer, other than the consumer's PIN, to be given to a third party where access is to be limited to a specified third party; *and*

3. Comply with the request as expeditiously as possible, but no later than three business days after receiving the request where the request has been made by certified or overnight mail and, when required under (b) below, within 15 minutes where the request has been made by any one of the methods made available to consumers*.**[; and

4. Provide to the consumer a copy of the information set forth in N.J.A.C. 13:45F-2.1(a)1 and 2.]*

(b) Each consumer reporting agency shall develop, within the time frame set forth below, secure procedures involving the use of telephone, fax, the Internet or other generally available electronic media to receive and process a request from a consumer to temporarily lift a security freeze on a consumer report. These procedures shall allow the lifting of a security freeze as expeditiously as possible, with the goal of lifting the security freeze within 15 minutes of receipt of the consumer's request.

1. *[(Within 60 days after the effective date of this chapter)]* *By June 6, 2008*, each consumer reporting agency shall provide to the Director, at the street address listed in N.J.A.C. 13:45F-2.1(c), a written plan that, when implemented, will allow the lifting of a security freeze within 15 minutes of receipt of the request to lift; and

2. *[(Within four months of the effective date of this chapter)]* *By August 7, 2008*, and in accordance with (b)1 above, each consumer reporting agency shall have technology in place to allow the lifting of a security freeze within 15 minutes of receipt of the request to lift.

(c) Any information that is provided to the Director under (b) above is confidential and proprietary information and shall not be considered a public or government record under the Open Public Records Act, N.J.S.A. 47:1A-1 et seq.

13:45F-2.4 Removing a security freeze

(a) Where a consumer reporting agency has received a request from the consumer to remove a security freeze it shall:

1. Remove the freeze if the consumer has supplied the information necessary for proper identification specified in the information given to the consumer pursuant to N.J.A.C. 13:45F-2.1(a)*1i* and the PIN

provided to the consumer pursuant to N.J.A.C. 13:45F-2.2(a)3; and

2. Comply with the request as expeditiously as possible, but no later than three business days after receiving the request.

(b) If a consumer reporting agency intends to remove a security freeze based on a material misrepresentation of fact by a consumer, the consumer reporting agency shall notify the consumer in writing in plain *[English]* *language* and shall wait at least five business days after mailing the notice before *[lifting]* *removing* the freeze. The notification to the consumer shall:

1. Be sent via first class mail to the consumer at the address on file with the consumer reporting agency;

2. State the basis upon which the consumer reporting agency has concluded that there was a material misrepresentation of fact;

3. State the action that the consumer reporting agency intends to take and the effective date of that action; and

4. Provide information for contacting the consumer reporting agency, including a telephone number, to dispute its findings.

13:45F-2.5 Changing official information

(a) Until a security freeze placed on a consumer report is removed, the consumer reporting agency shall not change any official information in the consumer report without first sending a written notice of the change to the consumer. The written notice shall be sent within 30 days of the posting of the intended change *to the official information* in the consumer *report* *[reporting agency's records]*. A consumer reporting agency shall wait at least 10 days after the written notice has been sent before finalizing the change in the consumer's report. The written notice of change shall:

1. State the type of official information that is being changed, without disclosing the actual information, and the reason for the change;

2. Advise the consumer that he or she must contact the consumer reporting agency*, in writing by mail or by any other method allowed by the consumer reporting agency,* within seven days of the date of the notice if the change in the official information is incorrect; and

3. Be sent to both the consumer's new and old address where the official information being changed is the consumer's address.

13:45F-2.6 Lost PIN or password

(a) Within 24 hours of notification that a consumer has lost his or her PIN or password, the consumer reporting agency shall:

1. Issue a new or reissue the original PIN or password if the consumer has supplied the information necessity for proper identification given to the consumer pursuant to N.J.A.C. 13:45F-2.1; and

2. Use a PIN or password, other than the consumer's Social Security number, or any portion thereof, or any data element comprising personal information, if issuing a new PIN or password.

13:45F-2.7 Fees

(a) A consumer reporting agency may charge the following fees:

1. Temporary lift or removal of a security freeze . . . . . up to $ 5.00; and

2. Replacement *or re-issuance* of a lost PIN or password . . up to $ 5.00.

(b) No fee may be charged for placing a security freeze on a consumer report.

SUBCHAPTER 3. *(RESERVED)* *[BREACH OF SECURITY PROVISIONS

13:45F-3.1 Duties of business or public entity in general

(a) Every business and every public entity shall maintain and keep on file for inspection by the Division, the following information, including any updates:

1. The analysis for the system developed by the business or public entity to meet the computer security requirements set forth in N.J.A.C. 13:45F-3.2; and

2. Notification procedures permitted under N.J.S.A. 56:8-163e and N.J.A.C. 13:45F-3.4(f), where the business or public entity maintains its own notification procedures.

(b) Every business and every public entity shall allow inspection by the Division of any records maintained under N.J.A.C. 13:45F-3.4(c), (d) and (g) and 3.5.

(c) Where there has been a breach of security, the business or public entity has a duty to mitigate any damage created by the breach of security, as expeditiously as possible. For example, where personal information has been posted to a website, the business or public entity shall contact the Internet service provider to have the personal information removed.

13:45F-3.2 Computer security system requirements

(a) Every business and every public entity shall maintain a security system and security measures covering its computers, including any wireless system, which, at a minimum, have the following elements:

1. Secure user authentication access for all system components containing personal information including:

i. Control of user IDs and other identifiers;

ii. A secure method of assigning and selecting passwords consisting of at least seven letters and numbers;

iii. Access restricted to active users and active user accounts only;

iv. Blocking access to user identification after not more than either six unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. Secure access control measures that:

i. Restrict access to files containing personal information to those who need such information to perform their job duties; and

ii. Assign a unique identification plus a logon or password, which is not vendor supplied, to each person with computer access;

3. Encryption of all stored or transmitted files containing personal information, including those in wireless environments and those containing personal information that will travel across public networks, and encryption of passwords for files containing personal information. The required encryption level is the Federal Information Processing Standard (FIPS) recommended standard, which is the Advanced Encryption Standard (AES) 128-bit to 256-bit or the FIPS recommended encryption standard in effect on (the effective date of this chapter). The FIPS recommended encryption standard is incorporated herein by reference, as may be amended and supplemented, and can be found at the National Institute of Standards and Technology website, www.nist.gov, specifically at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Encryption must be, at a minimum, 128-bit. If the FIPS standard changes, the encryption standard under this section shall be upgraded to that FIPS recommended standard within 30 days of the change to that

standard;

4. Secure storage of encryption keys and limitation of access keys to the fewest number of custodians necessary;

5. Management processes and procedures that are fully documented and implemented, to keep keys secure;

6. Periodic monitoring and testing of networks by conducting audits of individual user's access to personal information and recording the audit trails for users, events, dates, times and success or failure;

7. Periodic review of audit trails only by those with job-related need to view audit trail, and backing up audit trail files to a medium that is difficult to change;

8. Regular testing of security systems and processes;

9. A closed system not connected to the Internet for files containing personal information, or if connection to the Internet is necessary, software firewall protection with up-to-date patches and the latest firmware and, if the business or public entity has more than five computers, a system with hardware firewall protection. Workstations, servers, laptops or any mobile device used to access the business or public entity network where personal information is contained must have a software-based firewall;

10. Firewall configuration standards that include:

i. A current network diagram with all connections to confidential information, including any wireless networks;

ii. No system containing personal information that resides in a demilitarized zone (DMZ), bypassing the firewall. Prohibit direct public access between external networks and any system component that stores personal information;

iii. Justification and documentation for any risky protocols such as, but not limited to, File Transport Protocol (FTP); Hyper Text Transfer Protocol/Port 80 (HTTP);

iv. For businesses with more than five computers, a hardware firewall containing stateful packet inspection, or dynamic packet filtering, that allows only "established" connections into the network; and

v. Denial of all inbound and outbound traffic not allowed or when system is not in use;

11. The most current version of antispyware software, including up-to-date patches, or a version that still can be supported with up-to-date patches and which includes the following:

i. One antispyware program installed;

ii. Antispyware program running in memory to constantly monitor system integrity;

iii. Antispyware definitions updated daily; and

iv. Daily full system scans to ensure system integrity during off peak hours;

12. The most current version of antivirus software, including up-to-date patches, or up-to-date patches for a version that still can be supported and which includes daily virus definition update and weekly fill system scans during off-peak hours and the ability to generate audit logs;

13. Security patches on all systems and applications updated as follows:

i. Operating system patches/updates installed weekly; and

ii. All vendor supplied security patches installed within one month;

14. Secure encrypted tunnels and certificates to show it is a secure site;

15. Education and training of employees on the proper use of the computer security system and the importance of personal information security;

16. Restricted physical access to computerized records containing personal information, including a written procedure that sets forth the manner in which physical access to personal information is restricted. When notified of any unauthorized entry into a secure area by either an employee or any other unauthorized person, the integrity of the computerized records must be reviewed;

17. An information security policy for those businesses with more than five employees that addresses the security of computerized personal information and defines responsibilities for all employees, including a data retention and disposal policy;

18. A process by which unnecessary programs, services, and protocols from all systems that are not directly needed to perform the devices' specified function may be removed;

19. Encryption of all non-console administrative access;

20. A process to render stored personal information unreadable wherever stored, including portable media and wireless networks; and

21. Usage policies for critical employee-facing technologies, such as modems and wireless.

(b) In addition to the measures required under (a), every business and every public entity shall maintain the following computer security methods for wireless environments:

1. Enable WPA2 (Wi-Fi Protected Access version 2);

2. AES Encryption Standard as set forth in (a)3 above with rotation of AES keys quarterly or whenever there are personnel changes;

3. Hardcode Media Access Control (MAC) addresses that must be removed when they are no longer authorized to connect to the wireless network; and

4. Change wireless vendor defaults, to include, but not limited to:

i. Default router/access point passwords; and

ii. Unique Service Set Identifier Default (SSID) that will not be broadcast.

13:45F-3.3 Notification of possible breach of security to the Division of State Police

(a) Every business and every public entity shall disclose to the Division of State Police of the Department of Law and Public Safety (Division of State Police) any breach of security, regardless of the level of encryption or the presence of any security measures, within six hours following discovery or notification of the breach whether or not disclosure to affected individuals is ultimately required. A business or public entity shall notify the Division of State Police by calling 1-888-648-6007 within New Jersey or 1-609-963-6900 outside of New Jersey and following the instructions given by the Division of State Police.

13:45F-3.4 Disclosure of breach of security

(a) As expeditiously as possible, but not more than 24 hours after notification by the Division of State Police to the business or public entity that disclosure of a breach will not compromise any investigation, the business or public entity shall notify, in accordance with (d) below, any affected individual unless the business or public entity has determined, under (b) below, that disclosure is not required. In the case of

substitute notice under (d)3 below, if the next available publication or broadcast is not within the 24-hour period specified, then disclosure shall be made in the next available publication or broadcast after the 24-hour period has expired.

(b) Disclosure under (a) above is not required if, within 24 hours of the discovery or notification of a breach of security, the business or public entity establishes that misuse of the personal information accessed is not reasonably possible. It shall be conclusively presumed that misuse of accessed personal information is possible and the breach of security must be disclosed if the computer security requirements of N.J.A.C. 13:45F-3.2 have not been met by the business or public entity.

(c) A business or public entity that has had a breach of security and has determined that misuse of the personal information breached is not reasonably possible, shall document, maintain and make available for inspection by the Division for a period of not less than five years a written record of its findings that includes the following information:

1. How and by whom the investigation was performed;

2. The basis for the decision that misuse is not reasonably possible, including a summary of the information gathered in making the determination; and

3. The levels of security in place and compliance with N.J.A.C. 13:45F-3.2; and

4. The extent of the breach.

(d) A business or public entity that finds that misuse of the personal information breached is reasonably possible shall give notice to affected individuals by:

1. Written notice sent by regular first class mail and posted on the Internet if the company or public entity maintains a website;

2. Electronic notice that is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. ß7001, incorporated herein by reference, as may be amended and supplemented, if the affected individual has agreed to receive such notice; or

3. Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $ 250,000 or that the number of affected individuals to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information for the affected individuals. The determination that substitute notice is necessary must be documented in writing, maintained and made available for inspection by the Division for a period of not less than five years. Substitute notice shall consist of all of the following:

i. An e-mail notice to those affected individuals for whom the business or public entity has an e-mail address;

ii. A conspicuous posting of the notice on the Internet, if the business or public entity maintains a website; and

iii. A notification to all major Statewide media, which shall consist of newspapers of general circulation in each of the northern, central and southern areas of New Jersey, and radio and television stations broadcasting to each of the northern, central and southern New Jersey markets.

(e) The notification by a business or public entity under (d) above shall include:

1. A description of the categories of personal information that were, or are reasonably believed to have been, accessed by an unauthorized person, for example, Social Security numbers, driver's license or state identification card numbers, account numbers or debit or credit card numbers in combination with any required security code, access code or password that would permit access to an individual's financial

account and any other information that could be used to access personal financial data;

2. A toll-free number that may be used to contact the business or public entity with any questions and from which an affected individual can determine the types of information that the business or public entity maintained in general and the types of information maintained about that affected individual specifically;

3. The Federal Trade Commission's web site and its toll free number;

4. Information on how the affected individuals can protect themselves against, or limit the damage from, identity theft or financial harm, including information about placing a fraud alert on the affected individual's consumer report; and

5. Steps taken by the business or public entity if the personal information has been posted to a website.

(f) Notwithstanding the requirements of (d) above, 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 which is otherwise consistent with the requirements of (a), (b), (c) and (e) above, including any time frames set forth in those subsections, shall be deemed to be in compliance with the notification requirements of this provision, if the business or public entity notifies the affected individuals in accordance with its notification procedures, in the event of a breach of security.

(g) In any case where a breach of security has been disclosed by a business or public entity to either the Division of State Police alone or the Division of State Police and affected individuals, the business or public entity shall document, maintain and make available for inspection by the Division for a period of not less than five years, a record of the disclosure. The record of disclosure shall include the date, nature and purpose of each disclosure and the information set forth in (e) above. Where the breach is disclosed pursuant to N.J.S.A. 56:8-163d(1) or (2) or e and N.J.A.C. 13:45F-3.4(d)1 or 2 or (f), the record also shall include the names and addresses of all affected individuals whose personal information has been breached and to whom disclosure was made. When the breach is disclosed pursuant to N.J.S.A. 56:8-163d(3) or (e) or N.J.A.C. 13:45F-3.4(d)3 or (f) the record shall include a list of all media notified.

(h) In the event that a business or public entity is required to notify more than 1,000 affected individuals at one time, the business or public entity shall notify, at the same time, all consumer reporting agencies that compile or maintain files on consumers.

(i) Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity and does not use that personal information for its own purposes or in furtherance of its business immediately shall notify that business or public entity, which shall follow the notification requirements of this subchapter, 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.

(j) Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity and uses that information in furtherance of its own business is subject to all of the breach of security requirements of this subchapter if the business or public entity suffers a breach of security in which the personal information compiled or maintained on behalf of another business or public entity is accessed.

13:45F-3.5 Destruction of certain records

(a) A business or public entity shall destroy, or arrange for destruction of the original and all copies of records within its custody, direction or control containing personal information, if those records are 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. A business or public entity shall document, maintain and make available for inspection by the Division for a period of not less than five years a written record of all documents containing personal information that have been destroyed under this section. The written record shall

contain the types of records destroyed and the manner in which the records were destroyed.]*

SUBCHAPTER 4. SOCIAL SECURITY NUMBERS

13:45F-4.1 Restrictions on the communication of Social Security numbers

(a) No person, including a 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 person or public or private entity;

4. Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted *[under, at least, the standard set forth in N.J.A.C. 13:45F-3.2]*; or

5. Require an individual to use his or her Social Security number to access an Internet website, unless a password or unique PIN or other authentication device is also required to access the Internet web site.

(b) Nothing in this section shall prevent the collection, use or release of a Social Security number, as required by *or to comply with* State or Federal law nor shall this subchapter obviate any prohibition on the use of Social Security numbers found in any Federal or State statutes and regulations.

(c) A public or private entity may use a Social Security number for internal verification and administrative purposes, as 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.

(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 opened.

[(e) A person or public or private entity shall not refuse to provide services or products if an individual refuses to give his or her Social Security number, so long as the Social Security number is not necessary in order for the person or public or private entity to provide products or services.]

*(e) Nothing in this subchapter 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 subchapter 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 subchapter.*

[(f)] *(g)* Where a person or a *[public or]* private entity requests a Social Security number from an individual, the person *[or public]* or private entity, when asked by the individual, shall state the reason for requesting the individual's Social Security number. *Where a public entity requests a Social Security number from an individual, the public entity shall affirmatively state the use to which the Social Security number will be put.*

[(g)] *(h)* Where a person or a public or private entity requests a Social Security number from an individual, the person or public or private entity shall do so in conditions under which the Social Security number will remain confidential. *Nothing contained in this subsection shall prohibit a person or public or private entity from using or releasing the Social Security number if otherwise permitted to do so under the Act or any other applicable law.*

SUBCHAPTER 5. VIOLATIONS

13:45F-5.1 Violations of security freeze provisions

(a) Any consumer reporting agency that willfully fails to comply with the requirements of N.J.A.C. 13:45F-2 or N.J.S.A. 56:11-30 or 56:11-46 through 49 shall be liable to a consumer as provided in N.J.S.A. 56:11-38.

(b) Any consumer reporting agency that is negligent in failing to comply with the requirements of N.J.A.C. 13:45F-2 or N.J.S.A. 56:11-30 or 56:11-46 through 49 shall be liable to a consumer as provided in N.J.S.A. 56:11-39.

13:45F-5.2 Violations of breach of security provisions

[(a)] It shall be an unlawful practice and a violation of the Consumer Fraud Act, N.J.S.A. 56:8-1 et seq., to willfully, knowingly or recklessly violate N.J.S.A. 56:8-161 through 164.

*[(b) The following acts by a business or public entity shall be deemed to be a knowing, willful or reckless violation under N.J.S.A. 56:8-166, so as to constitute an unlawful practice and a violation of the Consumer Fraud Act, N.J.S.A. 56:8-1 et seq.:

1. Failure to comply with any time limits set forth in the breach of security provisions of the ITPA or this chapter;

2. Failure to develop and maintain documentation where it is required by the breach of security provisions of the ITPA or this chapter;

3. Failure to maintain a computer security system as required by N.J.A.C. 13:45F-3.2;

4. Failure to follow the procedures for notification and disclosure to the Division of State Police or affected individuals;

5. If over 1,000 people were affected by the breach of security, notification of all consumer reporting agencies as required by the breach of security provisions of the ITPA or this chapter; and

6. Wrongful use of Social Security numbers.]*