1 of 5 DOCUMENTS

NEW JERSEY REGISTER

VOLUME 40, ISSUE 24

ISSUE DATE: DECEMBER 15, 2008

RULE PROPOSALS

LAW AND PUBLIC SAFETY
DIVISION OF CONSUMER AFFAIRS

40 N.J.R. 6926(a)

Pre-Proposed New Rules: N.J.A.C. 13:45F-3

Pre-Proposed Amendments: N.J.A.C. 13:45F-1.1, 1.2, 1.3 and 5.2

Click here to view Interested Persons Statement

Notice of Pre-Proposal

Identity Theft, Written Security Programs and Violations

Authorized By: David Szuchman, Director, Division of Consumer Affairs.

Authority: N.J.S.A. 56:8-165.

Pre-Proposal Number: PPR 2008-3.

Take notice that on April 16, 2007, the Division of Consumer Affairs proposed rules on Identity Theft at 39 N.J.R. 1397(a), pursuant to the Identity Theft Prevention Act (IPTA), P.L. 2005, c. 226, N.J.S.A. 56:11-44 et seq. The comment period for that proposal closed on June 15, 2007. The Division received a number of comments that addressed the provisions of Subchapter 3, and the definitions and violations related to Subchapter 3.

Take further notice that after reviewing those comments, the Division decided to reconsider the rules implementing the provisions of the ITPA related to the security of personal information found at N.J.S.A. 56:8-161 to 163. The Division adopted the remainder of N.J.A.C. 13:45F, which was published on April 7, 2008 at 40 N.J.R. 1898(a).

Take further notice that after review of the comments received, further research, and input from various groups, the Division has developed a new Subchapter 3 and has included appropriate amendments to Subchapters 1 and 5 of N.J.A.C. 13:45F to effectuate Subchapter 3. The Division finds it appropriate to submit this draft proposal as a pre-proposal to allow interested parties to submit comments and suggestions prior to formally proposing this rule.

Submit written comments on the pre-proposal by February 13, 2009 to:
David Szuchman, Director
Division of Consumer Affairs
124 Halsey Street
PO Box 45027
Newark, NJ 07101

Full text of the pre-proposed new rules and amendments follows (additions indicated in boldface **thus**; deletions indicated in brackets [thus]):

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 regarding 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

(a) This chapter applies to**:**

1. [consumer] **Consumer** reporting agencies that maintain consumer reports on New Jersey residents**;**

2. Every business doing business in New Jersey and every New Jersey public entity that possesses the computerized personal information of New Jersey residents;

3. Every business or public entity that holds records of New Jersey residents containing personal information that are to be destroyed; and

4. [any] **Any** public or private entity or person who has access to the Social Security numbers of New Jersey residents.

(b) N.J.A.C. 13:45F-3.2 shall not apply to any business doing business in New Jersey or any New Jersey public entity that is required to comply with a Federal or State statutory or regulatory scheme that would satisfy the requirements of N.J.A.C. 13:45F-3.2(a).

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 set forth in the comprehensive written information security program of the business or public entity as required by 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.

"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-3.4, the definition of business includes entities that possess either computerized records or other records, as defined in this section, containing personal information.

"Computerized records" means records stored in, or transmitted from, 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.

. . .

"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.

. . .

"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 required 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.

[page=6927] **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.**

. . .

"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.

. . .

"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.

. . .

SUBCHAPTER 3. 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. A synopsis of the comprehensive written information security program developed by the business or public entity to show that the business or public entity has met the requirements of N.J.A.C. 13:45F-3.2(a); and

2. Notification procedures permitted under N.J.S.A. 56:8-163e and N.J.A.C. 13:45F-3.3(g), 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-3.3(d), (e) and (h).

(c) Where there has been a breach of security, the business or public entity shall make all reasonable efforts as expeditiously as possible to prevent further release of or access to the personal information that has been accessed. 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 Comprehensive written information security program

(a) Every business and every public entity shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of personal information appropriate to the size and complexity of the business or public entity, the nature and scope of its activities, and the sensitivity of the personal information. This information security program shall be designed to:

1. Ensure the security and confidentiality of personal information;

2. Protect against any anticipated threats or hazards to the security or integrity of the personal information; and

3. Protect against unauthorized access to or use of customers' personal information that could result in substantial harm or inconvenience to any customer.

(b) The actions and procedures described in this subsection are examples of methods of implementation of the requirements of (a) above that businesses and public entities may follow. These examples of non-exclusive illustrations of actions and procedures are as follows:

1. Assessment of the risk by:

i. Identifying reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of personal information or personal information systems;

ii. Assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer/personal information; and

iii. Assessing the sufficiency of policies, procedures, customer/personal information systems and other safeguards in place to control risks;

2. Management and control of risk by:

i. Designing an information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the activities of the business or public entity;

ii. Training staff, as appropriate, to implement the information security program of the business or public entity;

iii. Regularly testing or otherwise regularly monitoring the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the risk assessment performed by the business or public entity; and

iv. Implementing a record destruction program;

3. Review of service provider agreements by:

i. Exercising appropriate due diligence in selecting service providers;

ii. Requiring service providers to implement appropriate measures designed to meet the objectives of this subchapter; and

iii. Taking appropriate steps to confirm that its service providers have satisfied these obligations, when indicated by the risk assessment of the business or public entity; and

4. Adjustment of the program by monitoring, evaluating and adjusting, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the changing business arrangements of the business or public entity, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

(c) Businesses and public entities that are required by this section to implement a comprehensive written information security program shall implement that program within one year of the date of the adoption of these rules.

13:45F-3.3 Disclosure and notification of breach of security

(a) Every business and every public entity required to disclose a breach of security under N.J.S.A. 56:8-163 to affected individuals shall in advance of the disclosure notify the Division of State Police of the Department of Law and Public Safety (Division of State Police) by calling 1-888-648-6007 within New Jersey or 1-609-963-6900 outside of New Jersey and follow the instructions given by the Division of State Police.

(b) As expeditiously as possible 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 (e) below, any affected individual unless the business or public entity has determined, under (c) below, that disclosure is not required.

(c) Disclosure under (a) and (b) above is not required if the business or public entity establishes that misuse of the personal information accessed is not reasonably possible.

(d) A business or public entity that has had a breach of security and has determined that misuse of the personal information accessed 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; and

2. A brief description of the facts and circumstances that form the basis for the decision that misuse is not reasonably possible.

[page=6928] **(e) A business or public entity that finds that misuse of the personal information accessed through the breach is reasonably possible shall give notice to affected individuals by:**

1. Written notice sent by regular first class mail;

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. §7001, 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 determines 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 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.

(f) The notification by a business or public entity under (e) 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 or other means, which is of no cost to the consumer, 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 to comply with N.J.A.C. 13:45F-3.1(c), if applicable.

(g) Notwithstanding the requirements of (e) 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 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.

(h) In any case where a breach of security has been disclosed by a business or public entity to 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 a description of the categories of affected individuals. When the breach is disclosed pursuant to N.J.S.A. 56:8-163d(3) or (e) or N.J.A.C. 13:45F-3.3(e)3 or (g), the record shall include a list of all media notified.

(i) 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, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers.

(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 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.

(k) 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 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-3.4 Destruction of certain records

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 under the entity's record retention policy, by shredding, erasing or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable through generally available means.

SUBCHAPTER 5. VIOLATIONS

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) It shall be a rebuttable presumption that the following acts by a business or public entity are 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 Identity Theft Prevention Act, N.J.S.A. 56:11-44 et seq., (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 follow the procedures for notification and disclosure to the Division of State Police or affected individuals; or

4. A violation of N.J.S.A. 56:8-164(a)(1), (3), (5) or (6) or a violation of N.J.A.C. 13:45F-4.1(a)1, 3, 4, or 5.