

New Jersey Publishes Pre-Proposal of Rules Protecting Personal Information

LISA J. SOTTO, ELIZABETH H. JOHNSON, AND MASON A. WEISZ

New Jersey is considering rules to protect the personal information of its residents. According to the author, the rules would: (1) require the implementation of a comprehensive written security program; (2) impose security breach response requirements (including new breach-notification procedures); and (3) alter existing record disposal obligations.

The New Jersey Division of Consumer Affairs has published a pre-proposal of rules relating to the protection of personal information (“PPR”) and accepted comments on the proposal. A formal proposal will follow. The PPR comes nearly a year after the state withdrew earlier proposed rules (the “Original Proposal”) that drew fire from the business community for the burdens they would have imposed. Among other obligations, the PPR would: (1) require implementation of a comprehensive written security program; (2) impose security breach response requirements (including new breach-notification procedures); and (3) alter existing record disposal obligations.

Lisa J. Sotto, partner and head of the Privacy and information Management Practice at Hunton & Williams LLP, focuses her practice on privacy, data security, and information management issues and assists clients in identifying and managing risks in these areas. Elizabeth H. Johnson and Mason A. Weisz are associates in the firm’s Privacy and information Management Practice. The authors can be reached at lsotto@hunton.com, ehjohnson@hunton.com, and mweisz@hunton.com, respectively.

SCOPE OF THE PERSONAL PROTECTION RULES

The PPR would apply to:

- Every organization 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, in any medium, of New Jersey residents containing personal information that are to be destroyed;
- Any public or private entity or person who has access to the Social Security numbers of New Jersey residents; and
- Consumer reporting agencies that maintain consumer reports on New Jersey residents.

The PPR defines “personal information” as 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. Dissociated data that, if linked, would constitute personal information is deemed “personal information” if the means to link the dissociated data was accessed in connection with access to the dissociated data.

WRITTEN INFORMATION SECURITY PROGRAM REQUIRED

The PPR would require every covered entity to 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 entity, the nature and scope of its activities, and the sensitivity of the personal information. The program must be designed to: (1) ensure the security and confidentiality of personal information; (2) protect against any anticipated threats or haz-

ards 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. Significantly, the term "customer" is defined to include employees.

The Original Proposal required a covered entity to develop a "security system and security measures covering its computers" and imposed a detailed and lengthy list of technical requirements that, in many aspects, were more onerous and complex than the requirements of the recently promulgated Massachusetts information security regulations. The Original Proposal's detailed requirements have been replaced with a list of "examples of non-exclusive illustrations" of methods to implement a comprehensive written information security program that are strongly reminiscent of the FTC's Gramm-Leach-Bliley Act Safeguards Rule.

Judging from the "non-exclusive illustrations" provided in the PPR, a program that meets the requirements of the Massachusetts information security regulations would also appear to meet the requirements of the PPR if the program encompasses the PPR's definition of "personal information."

CHANGES TO BREACH RESPONSE REQUIREMENTS

The Original Proposal stated that an entity suffering a security breach "has a duty to mitigate any damage created by the breach of security, as expeditiously as possible." In response to critics who feared that this language would create undue liability, the provision has been changed to state that relevant entities "shall make all reasonable efforts as expeditiously as possible to prevent further release of or access to the personal information that has been accessed." Like the Original Proposal, the PPR still illustrates this provision by stating, as an example of a mitigating act, that where personal information has been posted to a web site, the business must contact the Internet service provider to have it removed.

CHANGES TO BREACH NOTIFICATION PROCEDURES

New Jersey is one of a minority of states that require notification to a state agency in the event of a data breach. Specifically, N.J. Statute §

56:8-163 requires that, prior to notifying affected citizens, the entity suffering the breach must notify the Division of State Police in the Department of Law and Public Safety. The law does not impose specific timing requirements with respect to this notification, and a security incident may not constitute a reportable breach if the information was encrypted. Moreover, neither the state police nor citizens need be notified if the affected entity establishes that misuse of the information is not reasonably possible. The Original Proposal required notification to the state police, regardless of the level of encryption or the presence of any security measures, within six hours following discovery of the breach, whether or not disclosure to affected individuals was ultimately required. Where disclosure to affected individuals would have been required, the Original Proposal mandated that such disclosure be made within 24 hours of determination by the state police that disclosure would not compromise an investigation.

Those proposed regulatory requirements have been replaced with provisions in the PPR. The PPR specifies that, prior to notifying customers, an affected entity must: (1) notify the Division of State Police by telephone; (2) follow the instructions given by the state police; and (3) refrain from notifying customers until the state police determines that such disclosure would not compromise an investigation. Unlike the statute, the PPR requires entities to obtain an affirmative indication from the state police that notifying individuals would not impede their investigation.

In addition, the PPR would establish a specific procedure for entities that avail themselves of a statutory exception to breach-notification requirements. N.J. Statute § 56:8-163 provides that an entity suffering a breach need not notify customers if it: (1) determines that misuse of the information is not reasonably possible and (2) documents that determination and maintains the documentation for five years. The PPR would give the state police the right to inspect such documentation and would require that the documentation describe: (1) how and by whom the investigation was performed and (2) the facts and circumstances that form the basis for the decision that misuse is not reasonably possible.

CHANGES TO RECORD RETENTION REQUIREMENTS

N.J. Statute § 56:8-162 already requires entities to destroy customer records containing personal information (by shredding or other secure method) when those records will no longer be retained. No reported cases construe that statutory section, but it appears to apply only to records if and when they are slated for disposal. The PPR would change the nature of this requirement by mandating destruction of such records when they are no longer to be retained “under the entity’s record retention policy.” This change, combined with the PPR’s mention of “[i]mplementing a record destruction program” in the list of “examples of non-exclusive illustrations” of methods to implement a comprehensive written information security program, may imply that covered entities would need to develop and implement a formal records management program and dispose of records pursuant to that program to ensure compliance with the PPR.