GLASER & WEINER, LLP

ATTORNEYS AT LAW

Toughened Data Security Law Proposed

New Data Security Requirements & Possible Safe Harbor Creation

Citing nearly 5,000 data breaches between 2006 and 2013 that affected over 22 million personal records of New Yorkers, Attorney General Eric Schneiderman recently announced that he would ask the State Legislature to introduce and consider a bill to strengthen New York's Information Security Breach and Notification Act (General Business Law Section 899-aa and State Technology Law Section 208). The law, which took effect in 2005, gives New York residents the right to know when "private information" has been compromised due to a "security breach."

Currently, private information is defined as "personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, 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." A security breach is an "unauthorized acquisition or acquisition without valid authorization 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 private information is not used or subject to unauthorized disclosure."

The Attorney General's proposed law would:

1. Expand the definition of private information to include:
    - Both email address and password combinations as well as email address and security question/answer combinations
    - Medical and health insurance information
2. Require any entity that collects and/or stores private information to have reasonable security measures in place, such as:
    - Administrative Safeguards to assess risks and train employees

- Technical Safeguards to identify risks, detect, prevent and respond to attacks, and regularly test and monitor systems controls and procedures
- Physical Safeguards for disposal and the areas where information is stored
- Annual independent third-party audits and certifications showing compliance, which could result in a rebuttable presumption of having reasonable data security in the event of a lawsuit

3. Create a safe harbor for entities that could potentially eliminate liability altogether for a data breach if certain steps have been met. These steps would include:
   - Categorize information systems based on the risk a breach imposes on the information stored
   - Implement an appropriate data security plan
   - Attain a certification
4. In the event of a data breach, encourage entities to share forensic reports with law enforcement officials so that the perpetrators can be caught. This could entail stating that the entity's legal privileges and protections would not be affected by such disclosure.

Recently, the State Legislature has been considering a number of proposed amendments to state law similar to the Attorney General's proposal. For example, the amendments would add medical information and health insurance information to the definition of both private information and identity theft. Medical information would be further defined to mean "any information regarding an individual medical history, mental or physical condition, or medical treatment of diagnosis by a health care professional." Health insurance information would be defined as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history, including, but not limited to, appeals history." These amendments would also require the development, implementation, and maintenance of a comprehensive information security program for the protection of personal information.