

THIS WAY FORWARD

SMALL BUSINESS SOLUTIONS



Data Breach Responsibilities

>>> *What does the law require you to do when personal information is stolen?* By John D. Cromie and Monica Seth

It seems that the news is replete with incidents of identity theft. In today's cyber world, data protection and security are privacy concerns that are paramount issues for the business community. In an attempt to protect consumers when a business' computerized data has been compromised, New Jersey has enacted certain data breach security notification ("SBN") laws. Similar laws have been enacted throughout the country and continue to evolve. Interestingly, these widely adopted SBN laws rely in large part on the "public shaming" of businesses for effect. Clearly, no business wants that sort of negative publicity.

SBN laws are triggered by a security lapse. These laws require businesses to disseminate written notices to consumers when "personal information," as defined by SBN laws, has been stolen, compromised or attacked. Most SBN laws have notification requirements for third-party vendors

as well. The most common form of a breach is a stolen laptop containing sensitive business data, including consumer names, social security numbers, or other forms of "personal information." What is most troubling for a business involved in a breach is that not only is the business a target for bad publicity, but the business is also a target for litigation or class action suits related to the breach. Further, a data breach may also trigger an investigation by - and potentially give rise to - extensive settlement requirements with such regulatory agencies

> Interestingly, these widely adopted SBN laws rely in large part on the "public shaming" of businesses for effect. Clearly, no business wants that sort of negative publicity.

as the Federal Trade Commission and the Securities and Exchange Commission. Under SBN laws, businesses must disseminate written breach notices to all consumers affected by the breach. Notably, one study by the Ponemon Institute in February 2009 concluded that data breaches cost businesses \$202 per breached record. Of this figure, hard costs associated with data breaches, such as notifying customers of a breach, account for \$15, while \$139 is attributed to soft costs, such as "lost business." These costs can grow substantially where the data breach involves voluminous information.

Each state's definition of "personal information" varies, and depending on the locale of the customers affected by the data breach, multiple states' SBN laws may apply. New Jersey, in particular, defines "personal information," in relevant part, as follows, N.J.S. 56:8-161:

[A]n 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.

Given the potentially high costs associated with a data breach, if a business retains "personal information," a prudent company must ensure the security of this sensitive business data by maintaining up-to-date security measures. In fact, New Jersey's SBN laws provide a safe harbor for encrypted data. Although New Jersey's SBN laws do not require any particular level of encryption, some states recommend use of the National

Institute of Standards and Technology's Advanced Encryption Standard. Also, establishing an infrastructure for dealing with security issues may be important, because SBN laws require companies to take quick action when a breach occurs. For example, New Jersey's SBN laws require that written breach notices be dispatched to affected consumers "in the most expedient time possible and without unreasonable delay." As such, developing an established plan of action in the event of a breach is an essential element to ensure timely compliance with SBN laws. **NJB**

ABOUT THE AUTHOR

John Cromie, Esq. is a partner at the Rose-land office of Connell Foley, LLP and is chair of the firm's corporate and transactional practice group. Monica Seth, Esq. is an associate of the firm and is a member of its corporate and transactional practice group.