

Privacy and Security Bulletin

May 2006

RECENTLY ENACTED STATE INFORMATION SECURITY BREACH LAWS

A 2005 survey of over 850 organizations indicated that nearly 60% had experienced a major security breach in the prior six months that resulted in the loss of confidential information or interruption in operations.¹ In response to high-profile cases of identity theft and data breaches, nearly half of the states have enacted legislation that places the onus on businesses that are victims of such security breaches to notify the individuals whose personal information may have been compromised. New York, Connecticut and Pennsylvania have enacted such legislation, and many more states have security breach legislation pending. These laws expose businesses to serious reputational risk. Prudence requires that companies plan not only to minimize the risk of a security breach of their own or a subcontractor's computer system, but also how to react when one occurs, to reduce both the negative publicity and the possibility of legal liability. This bulletin analyzes and compares the security breach laws recently enacted in New York, Connecticut and Pennsylvania.

Summary of New York Information Security Breach and Notification Act

In December 2005, the Information Security Breach and Notification Act (the "Act") took effect in New York State. It amends the New York General Business Law and New York State Technology Law by requiring New York "state entities"² and persons conducting business in New York to provide notice to affected

persons whenever the private information of New York residents has been unlawfully acquired due to a security breach.

The Act is a response to increases in security breaches and identity theft both on the state and national levels highlighted when the data broker ChoicePoint inadvertently exposed thousands of individuals' personal information to identity theft.³ This breach was discovered in early 2005 because of a 2003 California law that requires notification to victims of a personal information security breach. At that time no New York law required such notification. The Act fills the gap in New York law: it imposes stringent notification requirements on state entities and businesses.

The Act amends the State Technology Law by requiring that New York state entities that own or license computerized data that includes private information⁴ disclose any breach in the security protecting this information to each New York resident whose private information was acquired, or is reasonably believed to have been acquired, without valid authorization. For state entities that maintain but do not own or license computerized data that includes private information, the Act requires disclosure of any breach in the security of this information to the owner or the licensee of this information, if the private information was, or is reasonably

believed to have been acquired by a person without valid authorization. Thus, if an entity that maintains but does not own or license certain data discloses a security breach to the owner, the owner must, in turn, notify all New York residents who are affected by such breach. The Act requires written notification unless a person affected by the security breach has expressly consented to receiving notice via electronic communication or the quantity or cost of providing such written notice is excessive. It also requires that state entities notify the state Attorney General, the State Office of Cyber Security and Critical Infrastructure Coordination, and the Consumer Protection Board. Under the Act, state entities are required to notify consumer reporting agencies (e.g. Equifax, Experian, and TransUnion) when more than five thousand New York residents may have been affected by such a breach. Finally, the Act amends the State Technology Law by requiring that local governments either develop policies or adopt laws consistent with the Act no more than one hundred twenty days after its enactment.

The Act's amendments to the General Business Law are similar to its amendments to the State Technology Law. Pursuant to these amendments, entities doing business in New York that own or license computerized data that includes private information must

disclose any breach in the security of this information to any New York resident whose private information was acquired, or is reasonably believed to have been acquired, without valid authorization. The Act also provides that any entity doing business in New York that maintains but does not own computerized data that includes private information must disclose any breach in the security of this information to the owner or the licensee of this information, if the private information was, or is reasonably believed to have been acquired by a person without valid authorization. Therefore, just as is the case with state entities, if a business is notified by a subcontractor that maintains its computerized data that a security breach compromising the data has occurred, the business must disclose this breach to affected New York residents. The Act requires written or telephone notification unless a person affected by the security breach has expressly consented to receiving notice via electronic communication or the quantity or cost of providing such written or telephone notice is excessive. It also allows for the state Attorney General to bring an action against a business violating the Act (by failing to notify residents affected by a security breach of its information system) to secure an injunction against such business and for damages for actual costs or losses incurred by persons affected by such violations. A business which knowingly or recklessly violates the Act may be

subject to civil penalties of up to \$150,000. Finally, the Act requires that businesses notify the state Attorney General, the State Office of Cyber Security and Critical Infrastructure Coordination, and the Consumer Protection Board. Under the Act, businesses are required to notify consumer reporting agencies when more than five thousand New York residents may have been affected by such a breach.

While the Act's amendments to the General Business Law are focused on protecting consumer information, the Act makes no distinction between the private information of consumers (who are New York residents) maintained by businesses and that of New York-resident employees of the business whose security has been breached.

Although one of the Act's sponsors in the New York State Assembly has indicated that this legislation is only intended to cover electronic records, the legislation is silent as to whether paper print-outs of electronic records are covered. Without further guidance from state regulators, this is a matter that could cause some confusion or potential litigation.

Other State Laws

At least twenty-two other states have enacted security breach notification laws in the past few years, many of which are similar to the New York Act. For example, Pennsylvania recently passed the Breach of Personal Information Notification Act (effective by July

1, 2006), which tracks much of New York law on this subject. Comparable to New York law, Pennsylvania law applies to state government entities and businesses doing business in Pennsylvania and protects state residents. Pennsylvania law, however, expands what constitutes a security breach to unauthorized *access* and acquisition of computerized data (New York law only contemplates acquisition), and limits a security breach to that which *materially* compromises the security or confidentiality of personal information maintained by an entity and that has caused or will cause loss or injury to any Pennsylvania resident. Connecticut law, which applies to persons who conduct business in Connecticut, now also mandates notification of residents whose personal information has been or is reasonably believed to have been improperly acquired. Yet it also slightly differs from New York law, providing for a "security freeze" by which a consumer may freeze his or her credit report and contains both less and more stringent notification requirements for when a security breach occurs. For example, unlike New York law, Connecticut law states that notification of a security breach shall not be required if, after appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the business in question reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Similar to

Pennsylvania, the Connecticut statute also expands the definition of a security breach to mean unauthorized access to, and acquisition of, computerized data. Although the New York, Pennsylvania and Connecticut statutes all apply to persons or entities who “conduct business” in each respective state, these statutes do not explicitly define what it means to “conduct business.” Therefore, application of these statutes does not appear to be limited to businesses physically located in the state. Furthermore, it is possible, absent further clarification and guidance from state regulators, that a business located in New York, but which also “conducts business” in Connecticut and Pennsylvania, may be subject to the laws of all three states.

Conclusion

The passage of the New York Information Security Breach and Notification Act and similar laws in other states means that individuals are entitled to be alerted to security breaches that may result in identity theft. It also means that businesses and state entities must be increasingly vigilant about detecting and reporting breaches of information security protocols. The obligation to disclose information security breaches poses a significant reputational risk for an entity, thereby encouraging preventative measures to mitigate against such breaches. To limit their potential liability, state entities and businesses should ensure that all of their employees are notified

about and comply with changes in information security law in the states in which they have customers or operate. State entities and businesses may want to set up protocols in advance for dealing with security breaches, rather than waiting for a breach to occur and reacting in “crisis mode”. Moreover, if they choose to have outside vendors maintain their computerized data, they should be especially careful to select reputable vendors that have reliable data protection systems in place and make sure to obtain warranties from them. State entities and businesses should also consider revising or amending certain of their internal documents and contracts with subcontractors and outside vendors to ensure compliance with the new state information security breach laws.

If you have any questions regarding this Privacy and Security Bulletin please contact:

Eric P. Bergner
(212) 554-7855
ebergner@mosessinger.com

Elizabeth A. Corradino
(212) 554-7892
ecorradino@mosessinger.com

Howard R. Herman
(212) 554-7847
hherman@mosessinger.com

Alan Kolod
(212) 554-7866
akolod@mosessinger.com

Linda A. Malek
(212) 554-7814
lmalek@mosessinger.com

Jay Meisel
(212) 554-7823
jmeisel@mosessinger.com

David Rabinowitz
(212) 554-7815
drabinowitz@mosessinger.com

Peter S. Smedresman
(212) 554-7869
psmedresman@mosessinger.com

Alexandre G. Simon
(212) 554-7861
asimon@mosessinger.com

1 Survey conducted by the Computing Technology Industry Association, 2005.

2 “State Entity” is defined under the Act as: “any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the State of New York except for the judiciary and cities, municipalities, villages, towns, and other local agencies.”

3 On January 26, 2006, ChoicePoint was fined \$15 million by the Federal Trade Commission for this security breach.

4 “Private Information” is defined under the Act as personal information that is not encrypted or for which an encryption key has been acquired in combination with a social security number, a driver’s license number or non-driver identification card number, and/or debit/credit card or account number combined with a password or access code which would permit access to a financial account. The definition excludes publicly available information from government records.

MOSES & SINGER LLP

Disclaimer

This Privacy and Security Bulletin is a general comment on recent developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the Firm on the legal issues described.

To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

This message is being sent from a Law Firm and may contain CONFIDENTIAL or PRIVILEGED information. If you are not the intended recipient, do not printout, copy or distribute this message. Advise the sender immediately by reply e-mail, and delete this message and attachments without retaining a copy.

Viewing this email or contacting Moses & Singer LLP by e-mail does not create an attorney-client relationship.

ADVERTISING MATERIAL

Under the ethics rules of certain state bar associations, this email may be construed as an advertisement or solicitation.

To stop receiving future privacy and security email bulletins from Moses & Singer LLP, please reply to optoutprivacy@mosessinger.com.

Copyright © 2006 Moses & Singer LLP
All Rights Reserved