February 2011 Vol. 25, No. 2

ILLINOIS STATE BAR ASSOCIATION

THE COUNSELOR

The newsletter of the Illinois State Bar Association's Section on Business Advice & Financial Planning

Breach Notification Laws—What every business owner needs to know

By Gary Zhao and Peter Maris

Breach Notification Laws—What they are

Identity theft and the theft of electronically stored personal information have dramatically increased in recent years, imposing financial harm and other costs on businesses and individuals.[1] The consequences of a breach are significant, and may include unwanted government investigations, consumer civil actions, adverse media attention, and damage to corporate reputation. According to the fifth annual U.S. Cost of a Data Breach Study, data breach incidents cost U.S. companies $204 per compromised customer record in 2009.[2]

There is no comprehensive regulatory scheme, state or federal, for securing consumer data and remedying breaches. Personal information protection law in the U.S. is rapidly evolving towards the reality that businesses have an obligation to provide appropriate security protections for personal information and an obligation to disclose a breach to affected consumers. More recently, however, the law has shifted to expand protections to personal information held by businesses across all industries and economic sectors. The Federal Trade Commission has begun to require stronger protections for consumers' personal information through more aggressive enforcement of Section 45 of the Federal Trade Commission Act.[3] Although only a handful of states require *ex ante* security measures for personal information or reasonable security laws, all but four states require that individuals be notified if their personal information is disclosed or accessed without authorization. These laws are known as "breach notification laws." As of October of 2010, the District of Columbia and every U.S. state except New Mexico, Kentucky, South Dakota, and Alabama had passed breach notification laws requiring that residents of the state be notified if their personal information security has been compromised.

Each state's breach notification law differs in certain respects. For the most part, these statutes do not penalize businesses for allowing the *data* breach itself to occur, but only provide penalties if a business fails (or is too slow in taking steps) to notify affected individuals. Generally, these laws define protected personal information as a person's first name and last name, in combination with any of the following: (1) social security number; (2) driver's license or I.D. card number; and (3) account, credit card, or debit card number, in combination with any required security access code or password.[4]

Breach Notification Law in Illinois

The Illinois Personal Information Protection Act (hereinafter PIPA or the Act) falls under the breach notification laws category.[5] PIPA requires businesses to notify individuals when a security breach results in their personal information being released to unauthorized parties. The Act specifies the notification steps businesses must follow in the event of a security breach.

The Act requires that any data collector notify a resident of a breach at no charge.[6] Notification must be given as expediently as possible, and without unreasonable delay, subject to any steps that must be taken to determine the scope of the breach and restore the system's security.[7] Notice can be written or electronic, provided the electronic notice complies with federal law regarding electronic writing and signatures.[8] Substitute notice can be provided if the data collector demonstrates that the cost of providing notice would exceed $250,000, more than 500,000 people would have to be notified, or the data collector does not have sufficient contact information for the affected people.[9] Substitute notice consists of e-mail, conspicuous posting on the data collector's Web site, or notification to major statewide media.[10]

Most states impose some type of civil liability for failing to comply with breach notification statutes. A violation of PIPA constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.[11] If an entity commits an unlawful practice under this act, the Attorney General or a State's Attorney may bring an action for injunctive relief, restitution, and civil penalties.[12] Individuals may also bring an action against a person who violates the Consumer Fraud and Deceptive Business Practices Act to recover any actual damages the plaintiff suffered as a result of a violation of the Act.[13]

Nuts And Bolts of Notification Compliance

Breach notification laws vary as to the lengths of time in which an entity must comply, with some imposing hard deadlines and others not. Complying with breach notification looks simple on paper: just promptly notify the affected customers by following your state's breach notification statute, right? However, the compliance process does not begin or end there. Good business practice requires a lot more. In addition to giving notice to customers, once a breach occurs, a business should also act quickly to determine the scope of the breach and potential notification duty and ensure that the breach

has been contained. Affected information systems must be isolated to prevent further breach and exposure.

The best way to comply with these laws is to prevent information security breaches in the first place. This can be accomplished by establishing an information security policy. It has been widely recognized that data security is an ongoing process that must be continually evaluated and changed. To remain effective, an information security policy should be based upon the size and type of business in question and the type of information involved. Most importantly, within a business, relevant employees or "first responders" must be educated about the basic tenets and responsibilities of data security.

Various governmental agencies have published guidelines for businesses to follow in establishing their respective information security policies. The Federal Trade Commission has adopted a process oriented approach in its guide.[14] The FTC's recommendations for compliance are built on 5 key principles: 1) determining what information the business has, 2) keeping only that information the business needs, 3) protecting the information the business needs and keeps, 4) disposing of what is no longer needed, and 5) creating a plan to respond to security incidents.[15]

The State of California Office of Privacy Protection has also issued a list of 13 recommended practices to minimize the risk of data breach. These practices include: 1) collecting the minimum amount of personal information necessary to complete the transaction, 2) creating an inventory of systems that contain personal information, 3) classifying personal information according to sensitivity, 4) using appropriate physical and technological safeguards, 5) paying particular attention to personal information stored on laptops and other portable devices, 6) not using data containing personal information in testing software or systems, 7) promoting awareness of security and privacy policies and procedures through ongoing employee training and communications, 8) requiring service providers and business partners to follow your security policies and procedures, 9) using intrusion detection technology and procedures to ensure rapid detection of unauthorized access to high-risk personal information, 10) when feasible, using data encryption in combination with host protection and access control, 11) disposing of records and equipment containing personal information, 12) reviewing a security plan at least annually, or whenever there is a material change in practices that implicates the security of personal information, and 13) health plans or health insurance providers should provide patients with regular explanation of benefits statements.[16]

Conclusion

While breach notification laws simply require an entity to alerts its customers if their personal information was improperly accessed, preventing such unauthorized access is the surest way to both comply with the law, and maintain a satisfied customer base and avoid costly breaches. All businesses are well advised to explore the information security threats they face and formulate a plan that is responsive to those threats. Fortunately, the law allows a substantial measure of flexibility in this area so that small businesses are not subject to the same security requirements as complex, multi-national corporations. On the other hand, this flexibility makes it difficult to know when an information security plan will comply with the laws in a given state. Not only must businesses comply with the laws in their home state, they must also comply with the laws in each state in which they have a customer or do business. For any multi-state or nationwide business, preventing information security breaches is most likely the easiest and cheapest way to comply with breach notification laws. ■

---

1. Janine S. Hiller, David L. Baumer, & Wade M. Chumney, *Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles*, 45 Idaho L. Rev. 283, 285 (2009).
2. *See*, *Ponemon Institute, U.S. Cost of a Data Breach Study*, 2010 at <http://www.ponemon.org/news-2/23>.
3. *Id*. at 289. *See also*, *In the Matter of Eli Lilly & Co*., 133 F.T.C. 763.
4. *See*, *e.g*., Wis. Stat. §134.98 (2010).
5. 815 ILCS 530/10 (2010).
6. *Id*.
7. *Id*.
8. *Id*.
9. *Id*.
10. *Id*.
11. 815 ILCS 530/20 (2010).
12. 815 ILCS 505/7 (2010).
13. 815 ILCS 505/10(a) (2010).
14. *See*, *Protecting Personal Information: A Guide for Business*, <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf>.
15. *Id.*
16. California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information*, <http://www.privacyprotection.ca.gov/res/docs/pdf/secbreach.pdf>.