Legal Insight

K&L GATES

www.klgates.com

March 6, 2012

Practice Group:

Technology Transactions & Data Protection

Illinois Attorney General Issues Guidance on Newly Amended Personal Information Protection Act

By Christopher A. Bloom

In the wake of amendments to the Illinois Personal Information Protection Act, 815 ILCS 530 *et seq.*, Illinois Attorney General Lisa Madigan has issued an *Information Security and Security Breach Notification Guidance* (the "Guidance"). The amendments and Guidance are aimed at curtailing identity theft and fraud which occur as a result of security breaches. In the announcement accompanying the Guidance, Lisa Madigan focused on the problems of identity theft citing reports that more than 550 breaches involving more than 30 million records occurred in 2011. The Guidance encourages businesses and government agencies "to understand the scope of the personal information they collect and to train employees on how to properly maintain and handle information to prevent security breaches which in turn can help prevent identity theft." This is advisable not only because of Illinois state law, but also because of obligations on businesses under federal law regarding identity theft prevention and claims handling.[1]

Illinois' Personal Information Protection Act was originally adopted in 2005 in response to an October 2004 incident involving Georgia-based ChoicePoint. ChoicePoint reportedly had sold the personal information of more than 145,000 people, including 5,000 Illinois residents, to identity thieves who pretended to be legitimate businesses. As originally enacted, the Personal Information Protection Act focused on requiring notice of data breaches to consumers. Notice was required by the Act when there was "unauthorized acquisition of computerized data that compromised the security, confidentiality or integrity of personal information maintained by a data collector." The Act defines "personal information" consistent with the core of other states' laws as an individual's name in combination with the individual's Social Security number, driver's license number or financial account number (such as a bank account, credit or debit card number) in combination with any required security code or password that would permit access to that account.[2]

The amendments to the Illinois Personal Information Protection Act were effective January 1, 2012 (the "2012 Amendments"). As explained in the Guidance, the 2012 Amendments expand the content requirements for data breach notices affecting Illinois residents and broaden responsibility for reporting data breaches to include companies that "store or maintain" data for others. The 2012

---

[1] For example, some businesses must have "red flag" identity theft prevention programs. FTC rules are at 16 CFR Part 681; the SEC and the Commodity Futures Trading Commission just jointly issued proposed rules (see http://www.sec.gov/news/press/2012/2012-34.htm). Many businesses must also timely respond to requests for information made by persons claiming to be victims of identity theft tied to transactions relating to the business. See 15 USC 1681g(e)(12).

[2] "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number.
(2) Driver's license number or State Identification card number.
(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

815 ILCS 530/5.

Amendments also mandate destruction and proper disposal of all records that contain personal information. Below are some of the key points in the Illinois Attorney General's Guidance and the 2012 Amendments.

Additional Notice Requirements

The 2012 Amendments expand the content requirement of the data breach notice under Illinois law. As has been described elsewhere in "Check Your Local Listings: California and Illinois Data Breach Law Amendments Highlight Varying State Compliance Obligations," Illinois law now requires that the notice include at a minimum: contact information for consumer reporting agencies which are listed in the Guidance; contact information for the Federal Trade Commission; and an express statement that the individual "can obtain information from these sources about fraud alerts and security freezes." The 2012 Amendments expressly prohibit the notice from including "information concerning the number of Illinois residents affected by the breach," which places the Illinois law directly in opposition to laws of some other states.

At this time, no single federal law or regulation covers data breaches of all types of sensitive personal information, and at least 45 states have enacted their own legislation requiring notification of security breaches involving personal information.[3] As a result, companies that collect and store personal information must comply with a matrix of different and sometimes inconsistent state laws throughout the United States. This becomes especially critical when a data security breach occurs and immediate, appropriate action is required.

Data Storage Companies Covered

The 2012 Amendments broaden the companies responsible for reporting data breaches under Illinois law. The 2005 Act placed responsibility solely on a data collector that "owns or licenses" personal information. The 2012 Amendments expand coverage to any company that "maintains or stores but does not own or license" computerized data which includes personal information. Companies which provide "cloud" and other information storage functions for data collectors are now required, by the Act, to notify the owner or licensee of the information of any breach of security of the data immediately following discovery. The Act requires such parties to cooperate with the owner or licensee of the computerized data in matters related to the breach.

Destruction and Disposal of Records

The 2012 Amendments require every individual, company and state agency to "dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable and undecipherable." Prior to disposal, as the Guidance states, electronic media and other non-paper media such as computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones or any other electronic media or hardware containing personal information must be destroyed or erased so that this personal information cannot be read or reconstructed.

The Act empowers the Attorney General to levy civil fines of up to $50,000 for each instance of improper disposal of materials containing personal information. Because of the potential harm and legal liability resulting from improper disposal, the Guidance recommends that companies "[consider]

[3] U.S. Congressional Research Service. *Federal Information and Security and Data Breach Notifications Laws* (RL34120; January 28, 2010), by Gina Stevens.

designating or hiring a records retention manager to supervise the disposal of records containing [such] information."

Enforcement

The Personal Information Protection Act expressly provides that violation of the Act constitutes an "unlawful practice" under the Consumer Fraud and Deceptive Business Practices Act.[4] Thus, a violation of the notice and destruction provisions of the Act is subject to all of the remedies provided under the Consumer Fraud and Deceptive Business Practices Act. This includes the ability of persons who are injured by a violation to bring a private cause of action. The Attorney General can also sue and levy fines for violations. As a result, companies ignore the newly amended Personal Information Protection Act at their peril.

Because a data security breach can be costly, the Attorney General's Guidance focuses on "preventing, preparing for, and responding to breaches of information security." It encourages companies that "collect, maintain, store, use and ultimately dispose of personal information" to take steps to protect that information and reduce the risk of suffering a security breach.

The full text of the Guidance can be found here.

Author:

Christopher A. Bloom
christopher.bloom@klgates.com
+1. 312.807.4370

[4] 815 ILCS 530/20