

# Privacy & Security Law Update

## Quantifying the Risks Privacy Law Enforcement

Recently-filed litigation as well as high-profile enforcement actions in the U.S. and Europe have raised an awareness of the consequences of privacy law violations.

Companies regularly try to estimate the exposure they may have as a result of non-compliance. If the exposure is material from a financial perspective, the company may have an obligation to disclose the risk to executive leadership, its auditors and shareholders. This article explores five of the most common and costly violations that companies face.

### 1. Security Incidents

While the websites that provide cost calculators for security breaches seem to grossly overstate the costs of most incidents, there



### IN THE SPOTLIGHT... Liability for Security Breaches

Many states are considering bills that would impose specific liability on companies for security breaches. Other states are considering changes to their security breach laws to add onerous new obligations on companies that have experienced a breach. If enacted, these bills could have significant impact on companies' response to a breach.

Massachusetts HB 123 would require retailers to reimburse banks for the costs associated with breaches, such as the costs of cancelling or reissuing payment cards, closing accounts and unauthorized transactions.

The Massachusetts Bankers Association strongly supports this bill because it believes that

is no question that a security breach is the easiest way to incur liability and expense.

For a "routine" breach, most companies estimate that they will spend approximately \$150 per record exposed. These costs include investigation/forensics costs, credit monitoring, consumer support (such as a call center) public relations, legal fees, regulatory notifications, and miscellaneous charges, such as printing and postage.

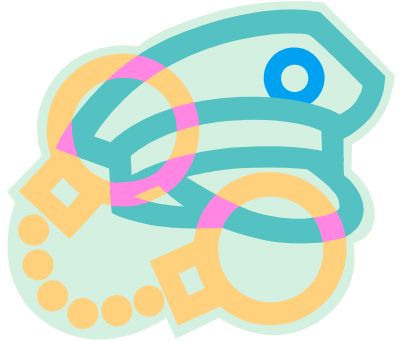
If the breach reveals a serious internal control weakness, the costs may escalate to include remediation, process changes, and additional training.

Additionally, if the breach results from a major violation of law or the PCI Data Security Standard, you may have litigation or regulatory costs. These costs can easily run in the millions or tens of millions of dollars, plus fines.

banks are unfairly bearing costs as a result of retailer failures to comply with the PCI Data Security Standard.

California AB 779 would permit companies to recover costs from third parties who were responsible for the breach. This bill would also limit the amount of time that retailers could retain sales transaction data to 90 days.

Texas HB 1262 would amend the existing security breach notification law to provide that entities that have a breach are "strictly liable" to the individuals whose data is compromised. The bill does not provide guidance, exposing companies to unspecified types of damages.



### 2. Asking for PI at POS in California

No matter how many alerts we publish, some companies are still asking consumers for their phone number, zip code or other personal information at point of sale in California. The mere request for this information violates the Song-Beverly Act, which has a private right of action.

Companies asking for personal information at point of sale in California should be prepared

*continued on page 2*

Kentucky's breach bill, HB 7, includes statutory damages of \$25,000 per violation and also permits courts to treble those damages for willful violations.

Illinois HB 0605 does not change the liability associated with a breach, but it would extend the notification law to paper records and require companies to notify individuals within 48 hours of a breach. This is, of course, an impossible standard.



## Enforcement Risks

to write a check for several tens of thousand of dollars to the plaintiff's lawyers and to provide coupons or gift cards to the consumers whose data you've collected in violation of the law.

### 3. FCRA Violations

The Fair Credit Reporting Act regulates the use of third party data—consumer

reports—for consumer lending, insurance underwriting and, most importantly, pre-employment screening. The law includes many process requirements, such as obtaining consents, giving consumers “adverse action notices” and it also limits the types of data you can consider.

Because the FCRA has a private right of action and sets statutory damages at \$1,000 per violation, plaintiff's lawyers

frequently allege FCRA violations. If you have not followed the letter of this complex law, you can expect to write a six figure check to settle.

Additionally, for egregious FCRA violations, you may also face regulatory action from the Federal Trade Commission or state authorities. The FTC's fines have exceeded \$2 million per company in several cases.

### 4. Telemarketing Violations

The FTC and the Federal Communications Commission vigorously enforce the laws regulating telemarketing, imposing almost \$20 million in fines since 2003. Common violations include:

- Inappropriate use of autodialers, which cannot be used to place calls to cell phones,
- Inappropriate use of prerecorded messages, which cannot be used to deliver sales messages, and
- Failure to check the Do Not Call Registry prior to making sales calls.

Additionally, over 40 states have their own laws regulating telemarketing. Companies regularly find themselves facing privacy lawsuits and state regulatory actions for violating these laws.

State laws often lack exceptions that exist under the Federal laws. Common violations include failures to respect state calling time restrictions and to scrub against state do-not-call registries

### 5. Data Protection Law Violations

European data protection authorities and functional regulators are engaged in spirited enforcement. This year, fines have ranged from 1,386€ (\$2,759) for sending 2 unsolicited emails, to 30,000€ (\$41,000) for inappropriate transfers of HR data to the US, to 980,000€ (\$1.9 million) for failure to secure consumer financial data properly.

## News Clips from Around the World



The **Bahamas Data Protection (Privacy of Personal Information) Act, 2003** took effect on April 2. This EU-style law applies to government and private sector entities. Elsewhere in **Latin America**, the Ministry of Economy in Peru is preparing a comprehensive data protection bill. Peru joins Venezuela, Ecuador, Mexico and Colombia, which are also considering EU-style laws.

Congratulations to **Jan Dhont**, Privacy Studio's “go to” colleague in Brussels, who has joined the international Lorenz law firm as a partner. Jan will continue to support our clients' EU needs at Lorenz, along with his partners. Jan's firm also has special expertise in Russian and Indian laws. Visit Jan online: [www.lorenz-law.com](http://www.lorenz-law.com).



The **Russian Data Protection** law's implementation has been delayed due to the reorganization of the federal agency that oversees compliance. According to an April 26 BNA report, the telecommunications supervisory agency, Rossvyaznadzor, has been merged with another agency. The merged agency will oversee data protection, but it is unlikely to establish a registry or issue guidance before June.

**Employee monitoring** continues to be a hot topic in Europe. On March 6, the Italian DPA issued a ruling that prohibits *any* monitoring of employee emails on employer-provided accounts. The new Czech Labor Code also contains specific requirements that must be met prior to conducting any employee monitoring, including electronic monitoring. These provisions took effect on January 1, but do attempt to balance worker privacy interests with employer needs.

**Information security** is also a concern in Europe. The Italian parliament has created an independent Authority for Information and Security Systems to serve as a counterpart to the established Data Protection Authority. Many EU countries have published formal security requirements for companies that process personal data.



Here at home, our dangerously cute panda cub, **Mei-Lan**, is now on public display at ZooAtlanta. If you are coming to Atlanta, let us know and we'll get tickets for you to meet the adorable, rambunctious, monochromatic fluff-ball. Or visit the PandaCam: [www.zooatlanta.org/animals\\_panda\\_cam.php4](http://www.zooatlanta.org/animals_panda_cam.php4)

This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email [tanya@privacystudio.com](mailto:tanya@privacystudio.com)—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.  
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339  
Phone: 404-914-1163  
[www.privacystudio.com](http://www.privacystudio.com)