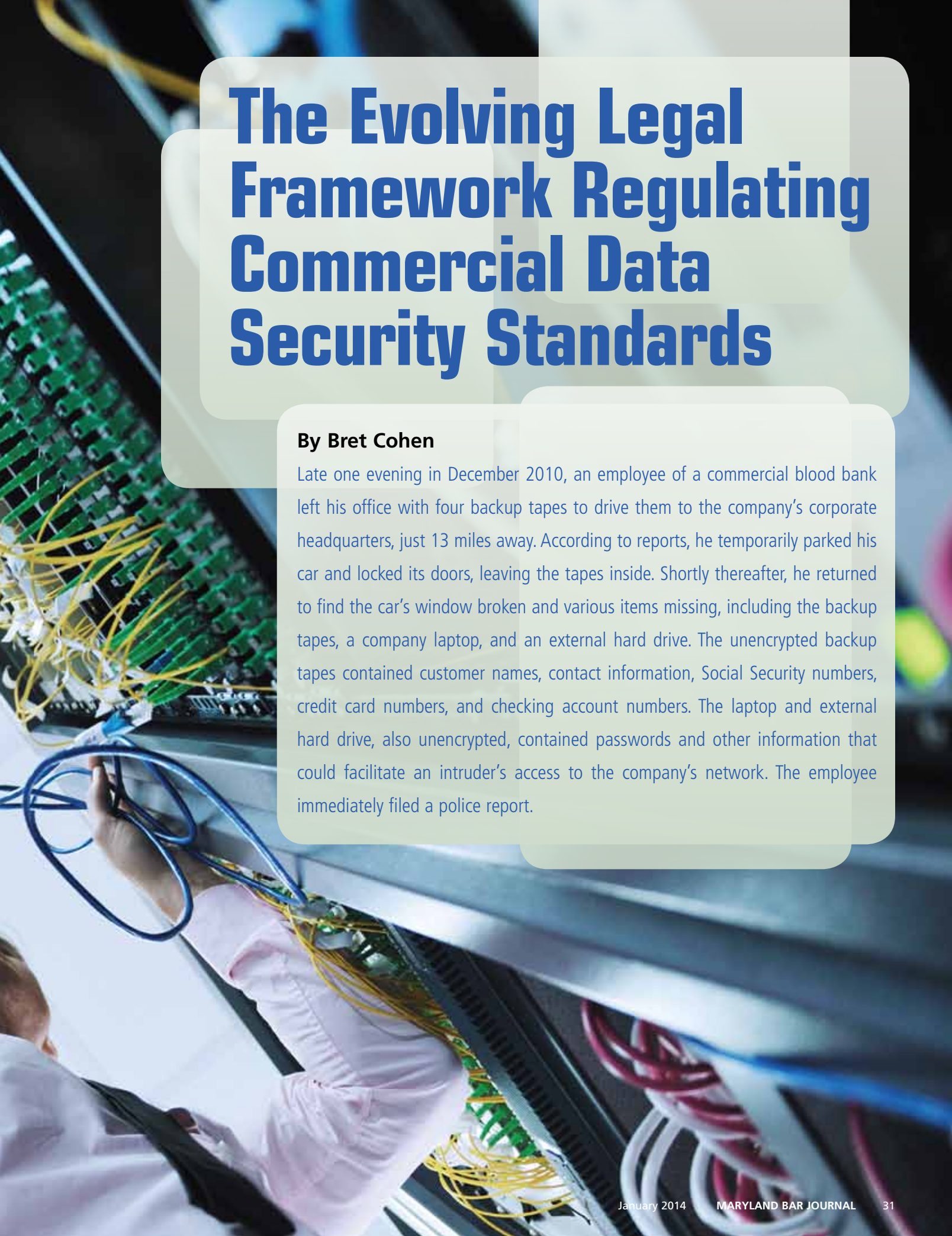

The Evolving Legal Framework Regulating Commercial Data Security Standards

By Bret Cohen

Late one evening in December 2010, an employee of a commercial blood bank left his office with four backup tapes to drive them to the company's corporate headquarters, just 13 miles away. According to reports, he temporarily parked his car and locked its doors, leaving the tapes inside. Shortly thereafter, he returned to find the car's window broken and various items missing, including the backup tapes, a company laptop, and an external hard drive. The unencrypted backup tapes contained customer names, contact information, Social Security numbers, credit card numbers, and checking account numbers. The laptop and external hard drive, also unencrypted, contained passwords and other information that could facilitate an intruder's access to the company's network. The employee immediately filed a police report.

This was just the beginning of the company's data breach saga. Soon after the breach, the company was investigated by the Federal Trade Commission (FTC), which alleged that it had violated federal law when it "failed to use reasonable and appropriate procedures for handling customers' personal information." In a settlement with the FTC, the company agreed to establish and maintain a comprehensive information security program and to submit to security audits by an independent auditor every other year for 20 years. *See In re Cbr Systems, Inc.*, FTC File No. 112 3120 (2013).

Around the same time, one of the company's customers filed a class action lawsuit on behalf of almost 300,000 customers whose information resided on the backup tapes. After over a year of litigation, the company settled the suit by providing a two-year subscription to a credit monitoring service (worth approximately $112 million, if fully utilized), cash reimbursements for demonstrated identity theft losses, and enhanced security measures. The company also agreed to pay $600,000 in attorneys' fees and costs. *Johansson-Dohrmann v. Cbr Systems, Inc.*, No. 12-cv-1115-MMA (BGS), 2013 WL 3864341 (S.D. Cal. July 24, 2013).

Data breach stories like this have become increasingly common. In response, a diverse legal framework has emerged to regulate commercial data security practices, driven by developments in four areas: federal and state enforcement of general consumer protection laws; state attorney general enforcement of a growing body of security-specific laws; federal sectoral regulation of specific categories of personal information, most prominently health and financial information; and consumer class action litigation.

General Consumer Protection Laws

At the federal level, the FTC brings enforcement actions against businesses that suffer breaches of certain sensitive categories of information – typically, those that can lead to consumer fraud or identity theft, such as Social Security numbers and credit card numbers – through its authority under Section 5 of the FTC Act to police "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45. The Commission typically proceeds under one of two theories. First, a business that fails to adopt industry-standard security measures to protect these types of information commits an "unfair" practice causing harm to consumers. Second, a business that makes a promise that it will keep data secure but then suffers a breach through inadequate safeguards commits a "deceptive" practice. Typically, an FTC investigation is precipitated by news of a data security breach, but often is not limited to the breach and comprehends an organization's entire data security program. Similarly, many states have so-called "little FTC Acts" which give them parallel and co-extensive enforcement authority.

As in the case of the blood bank, the FTC has resolved all public investigations to date by entering into settlements requiring companies to establish a comprehensive data security program and to conduct and file biannual, independent audits for 20 years. Although these settlements are not accompanied by any financial penalty, any failure to comply with the settlement agreement over the next 20 years, including through another data breach due to a security lapse, can result in a penalty of $16,000 per record breached. As Google learned, as it paid a $22.5 million penalty in 2012 to settle its second Section 5 complaint in two years. *See* Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://ftc.gov/opa/2012/08/google.shtm.

The FTC has not promulgated any formal regulations formally defining those data security practices that satisfy the FTC Act. Instead, it issues complaints along with its settlements that indicate which of the settling organization's practices it considered to be inadequate. It then encourages businesses to avoid these practices to avoid enforcement. Although not under the guise of formal regulation, the Commission has published guidance materials that provide the general steps it expects businesses to take to protect consumer information. *See* FTC, *Protecting Personal Information: A Guide for Business*, http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

State Data Security Laws

In addition to the significant authority wielded by the FTC, states have adopted a number of laws that impose security obligations on organizations that handle personal information. Perhaps the single greatest factor influencing the scrutiny of organizational data security over the past decade is state enactment of breach notification laws. Starting with California in 2003, 50 U.S. states and territories have adopted laws that typically require organizations that own or license certain sensitive categories of computerized information to notify individuals of any unauthorized acquisition of their information. For example, Maryland's law

requires notification "as soon as reasonably practicable" after conducting an initial investigation if the breached information includes a resident's name combined with an unencrypted Social Security number, driver's license number, financial account number, or individual taxpayer identification number. Md. Code, Com. Law § 14-3504. Like a number of other states, Maryland also requires notification to the Office of the Attorney General. These notices, which often are picked up by the media, invite regulatory scrutiny and motivate organizations to take proactive steps to improve their security practices and avoid the reputational harm and expense of a breach.

Other state laws more directly regulate security practices. Maryland, similar to the FTC standard, requires businesses that own or license sensitive categories of personal information to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations," and to enter into contracts holding service providers to the same standard. *Id.* § 14-3503. And when destroying customer records containing sensitive personal information, businesses must "take reasonable steps to protect against unauthorized access to or use of the personal information." *Id.* § 14-3502.

The Maryland Attorney General has enforced these laws. In 2009, the AG's office, along with 41 other attorneys general, entered into a $9.75 million settlement with retailer TJX Companies based on a breach that allowed hackers to steal customers' unencrypted credit card information. *See* Press Release, Md. Att'y Gen., Attorney General Gansler Reaches Settlement with TJX Companies, Inc. (June 23, 2009), *available at* http://oag.state.md.us/Press/2009/062309.htm. Smaller businesses have not been overlooked; in 2010, Mid Atlantic Processing entered into a $20,000 settlement for discarding business records containing Social Security numbers, cancelled checks, and other sensitive personal information in a Dumpster rather than using more secure methods. *See* Press Release, Md. Att'y Gen., Attorney General Settles with Mid Atlantic Processing (May 10, 2010), *available at* http://oag.state.md.us/Press/2010/051010.htm. Most recently, in August 2013, CVS Pharmacy agreed to pay $250,000 to settle claims that, among other things, it improperly disposed of records containing sensitive health information in open Dumpsters. *See* Press Release, Md. Att'y Gen., AG Gansler Reaches Settlement with CVS Pharmacy over Improper Disposal of Patient Records, Inappropriate Sale of Expired Products (Aug. 28, 2013), *available at* http://oag.state.md.us/Press/2013/082813.html.

Some states have adopted more granular data security regulations. The most far-reaching are the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, which became effective in 2010. 201 CMR § 17.00. The Massachusetts Standards are significantly more detailed than other state laws or regulations that merely require businesses to implement "reasonable security procedures and practices," such as Maryland's, containing sector-neutral data security requirements consistent with FTC guidance.

Under the regulation, entities that own or license sensitive categories of personal information of Massachusetts residents – defined similarly to the information covered under Maryland's data security laws – are required to document and implement a comprehensive information security program to protect hard copy and electronic records. While the security program can be tailored to the size and scope of business, the program must meet certain minimum requirements. These include designating an employee in charge, conducting regular risk assessments, overseeing service providers, and adopting certain technical security requirements such as encrypting all covered information stored on laptops or other portable devices. The state can seek an injunction, the reasonable costs of investigation and litigation, and a civil penalty of up to $5,000 per violation.

The Massachusetts Attorney General takes the position that the Standards apply to companies located outside of the state who collect personal information from Massachusetts residents. Therefore, non-Massachusetts organizations still may be subject to the regulations if they collect information about Massachusetts residents, although to date the regulations have not been enforced outside of the state. As with Calfornia's first-in-class breach notification law, the Massachusetts Standards may be the template for future regulation in other states, and in any event they generally align with the FTC's de facto data security standards. Therefore, even non-Massachusetts organizations should think consider designing a data security program compliant with the Massachusetts Standards.

Federal Sectoral Laws

A handful of federal laws regulate commercial data security in specific industry sectors, but the most comprehensive ones are those embodied in the Health Insurance Portability

and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA).

HIPAA directly regulates the collection and use of health information by health plans, health care providers, and health care clearinghouses. Among HIPAA's requirements is its Security Rule, which prescribes specific administrative, physical, and technical measures that covered entities must adopt to protect electronic health information. 45 C.F.R. Part 164, Subpart C. The Security Rule is the most comprehensive data security regulation in the United States, and generally reflects specific industry-leading data security standards. Regulated entities that violate the Security Rule are subject to tiered penalties of $100 to $50,000 per violation depending on their level of knowledge or willfulness, with a cap of $1.5 million per calendar year for multiple violations of identical provisions. In addition, similar to the state breach notification laws, HIPAA's Breach Notification Rule requires notification following a breach of unsecured protected health information. *Id.* Subpart D.

While HIPAA primarily focuses on the regulation of entities in the health care industry, a recent overhaul of its regulations greatly expands the statute's reach to health care providers' business associates. As of September 23, 2013, most persons or businesses that provide services to HIPAA-covered entities involving access to or storage of protected health information are directly subject to the Security Rule and the Breach Notification Rule. This includes, for example, attorneys and accountants who access or store protected health information in their provision of services, and providers of passive data storage solutions. These business associates now must, among other new requirements, perform periodic HIPAA security risk assessments, adopt HIPAA security policies and procedures, and enter into written agreements with subcontractors incorporating similar HIPAA requirements.

GLBA requires covered "financial institutions" – organizations that offer consumer financial products or services such as loans, financial or investment advice, or insurance – to adopt a comprehensive data security program. 15 U.S.C. § 6801(b). Specific requirements are detailed in the rules of the many federal and state regulators with authority over covered institutions. But similar to HIPAA, all generally require that financial institutions implement administrative, technical, and physical safeguards to secure customer information.

Banks, insurers, and other traditional financial institutions are not the only entities subject to GLBA; the data security requirements also apply to other individuals or organizations based on

the offering of financial products or services to consumers. This includes check-cashing businesses, mortgage brokers, real estate appraisers, retailers that issue credit cards, and the lending arms of universities and vehicle manufacturers.

Consumer Class Action Litigation

Perhaps the biggest source of data security legal risk in the last couple of years has been consumer class action litigation. It is not particularly controversial that organizations may be liable for fraud or identity theft damages directly resulting from a data breach. Those types of claims, however, typically have not translated to the class action context, given the need to prove individualized damages. Even so, the past few years have seen a dramatic increase in the number of class action lawsuits filed against businesses who report a breach. Most of these claims are not based on any theory that the purported class suffered any actual damages, but rather that they are entitled to some sort of compensation for the loss of their personal information, or because they incurred costs to protect against possible fraud or identity theft that might result.

The majority of class actions based on data security breaches have been dismissed, for lack of standing or failure to state a claim, because the plaintiffs could not allege that they were harmed by the breach. *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). Some more recent opinions, however, have begun to chip away at that reasoning. For example, courts have held that plaintiffs can proceed in data breach suits based on arguments that subscriber fees incorporated unfulfilled data security benefits, or that costs to mitigate the risk of identity theft were reasonable in light of demonstrated identity theft affecting others. *See Resnick v. Avmed, Inc.*, 693 F.3d 1317 (11th Cir. 2012); *Anderson v. Hannaford Bros.*, 659 F.3d 151 (1st Cir. 2011). Once plaintiffs are able to defeat a motion to dismiss, defendants are more likely to settle, which in turn increases the incentive to bring claims based on just about any data breach. Therefore, any organization preparing to report an incident under the breach notification laws should prepare itself for the possibility of a lawsuit.

Data security strategies used to focus on protecting the crown jewels: an organization's intellectual property, trade secrets, and business records. While that still should be a primary goal of any security program, the significant legal risks related to the protection of regulated personal information need to be considered as well. As a starting point, here are five steps organizations can take to mitigate these risks:

1. **Take an inventory of regulated information**. The first step to determining what risks exist is knowing what information the organization maintains, and where that information is located.

2. **Design and conduct regular security risk assessments**. A common thread of all of the security-related legal requirements is the ongoing assessment and management of risk. While it may require an initial investment, proactive identification of and reaction to these risks is much cheaper than handling breaches after the fact. For smaller organizations without vast stores of regulated data, this does not need to be a significant undertaking; there are off-the-shelf materials and audit criteria that can help guide assessment efforts. But regardless of size, organizations should consider conducting these assessments under the direction of counsel, to preserve privilege in case the assessment reveals any risk that later leads to a breach.

3. **Regularly train employees on data security**. While IT staff responsible for security operations should receive the most robust training, countless breaches have occurred through the actions of normal employees, from clicking on a virus in an email to losing a thumb drive containing sensitive information. Therefore, employees should be trained on the company's data security policies when they first join the organization and then on a periodic basis thereafter.

4. **Incorporate data security into vendor management procedures**. Organizations are increasingly outsourcing data processing operations to service providers, so a key to maintaining an acceptable level of risk is conducting reasonable diligence of these providers, and including security-specific terms into contracts.

5. **Consider cyber risk insurance**. Despite best intentions, some data security breaches cannot be avoided and may not be covered under standard Commercial General Liability policies. Therefore, companies should speak with their brokers about the availability of cyber risk insurance, which can help fill some of the gaps in coverage.

Mr. Cohen practices in the Privacy and Information Management group at the law firm of Hogan Lovells and blogs about data privacy and cybersecurity issues at hldataprotection.com. He may be reached at bret.cohen@hoganlovells.com.