

Re-Assessing Data Security In 2010: A List Of Practical Action Items

**Alysa Z. Hutnik
and Christopher M. Loeffler**

KELLEY DRYE & WARREN LLP

The beginning of 2010 makes clear that data security's bottom line is unequivocal. Even in a down economy, businesses that handle personal information – whether customer or employee data – face a number of rigorous legal obligations. A recent wave of state laws – Massachusetts,¹ Nevada,² Washington,³ and others on the way – have mandated encryption and other specific types of data safeguards. Merchants are facing record fines and payment card reimbursement costs (often in the six figures, if not higher) for violations of the Payment Card Industry Data Security Standard (PCI-DSS). Congress is considering adding civil penalties for data security violations under pending legislation.⁴ And the Federal Trade Commission – the most active cop on the beat in this area – has announced 10- to 20-year settlements nearly every month over the past couple years with companies that the FTC alleges failed to sufficiently protect the personal data in their control.⁵

Clearly there is significant exposure for not taking these obligations seriously, but that's stating the obvious. What do these various legal (and contractual) data security obligations mean in a practical context? While there is no silver bullet answer, there are some common action items that are worth noting.

Alysa Z. Hutnik and Christopher M. Loeffler are attorneys in Kelley Drye & Warren's Washington, D.C. office. They specialize in privacy, data security, and advertising law. Ms. Hutnik is also the Chair of the American Bar Association's Privacy and Information Security Committee (within the Section of Antitrust).



**Alysa Z.
Hutnik**



**Christopher M.
Loeffler**

Implement A Written Information Security Program

Data security starts with a plan, and applicable law requires the plan be in writing and designed around the company's actual practices and risks. Some businesses have yet to implement a written information security program, and those that handle the personal information of Massachusetts residents may be working feverishly to develop the policies and procedures necessary to comply with the Massachusetts regulations that took effect in March 2010, which require such a program.

It's also worth noting that, should the FTC come knocking at your door (typically following a data breach), one of the first questions they will ask is to see a copy of your written information security program. Having nothing to provide, or an incomplete draft version, will not boost your defense.

A written information security program will typically include information security-related policies that holistically govern the business's data-handling practices. For example, the program may incorporate a written "umbrella" information security policy that lays out the overall mission of protecting the confidentiality, integrity, and security of confidential personal data. The program may also include:

- a physical and environmental security policy (detailing the physical security requirements for the business),
- an access control policy (documenting the policy safeguards restricting access to such data),

- a human resources security policy (addressing personnel safeguards),
- a Red Flags Rule / identity theft policy (if the company is subject to this regulation and/or otherwise uses such a policy to handle fraud),
- a records retention and disposal policy (designed, in part, to address secure disposal of personal and business data after the business need expires),
- a vendor security policy (to address risks associated with sharing data with service providers),
- an incident response policy (addressing security breaches), and
- a business continuity and disaster recovery policy.

The security program cannot just be on paper. It needs to be implemented, communicated to personnel with relevant training, carried out in contracts with third parties who will share or have access to personal data, and updated periodically to reflect the current business practices and corresponding risks.

Convene The Right Team

IT is no longer all technical. The right interdisciplinary "task force" is critical to ensuring that the business's data security program strikes the right balance in protecting data and complying with applicable laws, without sacrificing the business's mission or bottom line. Depending on the business, the team may involve representation from IT and legal, asset management, human resources, sales/marketing, and internal audit. Their collective input can be immensely valuable in deciding where to direct resources, and what risks are acceptable in deciding to implement (or not implement) certain safeguards – administrative, technical, and physical – while still maintaining an overall reasonable and compliant information security program.

Additionally, this interdisciplinary team will be critical in the event of a data security breach, as each representative will likely have an important role to play in investigating the scope of the incident and developing the business's response.

Please email the authors at ahutnik@kelleydrye.com or cloeffler@kelleydrye.com with questions about this article.

Know The Laws

No simple answer here – data security law is in flux, and there is no one uniform law that spells out all the requirements. The best bet is to know the legal federal and state landscape, and to keep track of how it's evolving – both in terms of the laws and regulations that get enacted, and how federal and state regulators and private litigants are enforcing such laws. Both assessments are critical to a company's risk assessment and compliance posture.

All in all, you're likely looking first to the state laws on privacy, data safeguards, breach notification, PCI-codification, and data disposal, which, in some contexts, can be fairly granular in their specificity. You then take a close look at how state attorneys general, the FTC and, if you handle health information, HHS have interpreted their enforcement authority on business practices involving personal data. There are plenty of examples to glean from their data security business guidance and settlements. Finally, to determine what is "reasonable" in today's data security world (and hence, the legal standard supporting most of these laws), have a good sense of the common industry best practices and recommended industry standards applicable to your business and the type of data in your control. These industry standards may include the PCI-DSS, ISO 27002, CoBIT, or NIST information technology and security standards. All of these requirements and principles outline an overall approach and framework for benchmarking a company's information security program.

Know The Trends

Given the frequency in which data breaches are publicized, it is no wonder that there is considerable scrutiny on business handling of personal data and enforcement by all parties who have a role in the protection of the data. In practical terms, this means that data security, as a compliance issue, is on the upswing. More laws are likely to be passed (and enforced). You're likely to see more rigorous contract language on data protection and detailed indemnity terms from business partners. Your potential exposure for non-compliance is larger given the active regulatory enforcement, private litigation, and PCI assessments and fines. This is not an issue that will go away quietly. As long as your business maintains or has access to personal data, you are likely to become intimately acquainted with why data security has a significant role in the business's set of priorities.

Know Where To Begin

The common starting point is typically focused on the type of personal data at issue. The more sensitive the data (i.e., Social Security numbers, payment card information, credit, health, and medical information, etc.), the more likely the most rigorous of the data security obligations will be triggered. But don't let your guard down on the slightly

less sensitive personal data. Privacy and data security laws often apply to those too (although the type of safeguard and handling restrictions may differ). The key is understanding what level of obligations are appropriate, depending on the type of information at issue, how it is used, stored, accessed, and shared.

Know Your Data

It is tough to do a data security risk assessment if you don't know where the business's personal data is stored and who can access it. For most companies, to perform this "data mapping" requires a fairly exhaustive examination of data collection that goes back years. It can be time and resource consuming, but is a critical component of ensuring that (1) you know what personal data you have, (2) you can securely dispose of personal data that the business no longer needs, and (3) you can tailor your information security safeguards to the actual (not hypothetical) flow of personal data within and outside the company.

Additionally, an evaluation of your business's current data-handling practices provides an opportunity to take stock of how much personal data your business collects and whether it makes sense to continue collecting all of this information. Historically, businesses have collected and stored as much data about customers and employees as possible. But your marketing practices or human resources practices may no longer require the collection and storage of vast amounts of personal information. Curtailing unnecessary data collection and storage practices is likely to materially reduce the company's security risk profile (as well as potential data storage costs).

Know Your Partners

You can invest heavily in your own data security, but if you freely hand off personal data to third parties without taking reasonable efforts to ensure they will protect the data, all that effort may become moot. Moreover, the context of potential third parties with whom your business may share personal data is likely broad. This list could involve companies you're thinking of acquiring or merging with, vendors or service providers who will be assisting your business (or vice versa), and/or franchisees.

Addressing the third-party issue in a data security program often includes a process, such as (1) a due diligence investigation during the selection process to confirm the status of the third party's existing data security program (and addressing any red flags that emerge from such analysis); (2) data security contract terms that sufficiently detail the expected obligations (and comply with applicable law), and indemnity language reflecting the company's informed decision-making about what risks it will take on and which ones should be owned by the third party; (3) controls in place to prevent com-

mon third-party lapses in data security (e.g., lost or stolen unencrypted data on mobile devices, improperly or untrained personnel handling data, insecure data disposal); and (4) an oversight and monitoring program, based on a risk assessment, to confirm that, during the period of the business relationship, the third parties are, in fact, reasonably protecting the personal data at issue.

Contractual provisions can provide monetary relief, but in the event of a data breach, your damages will likely extend to include harm to your business's reputation and goodwill. While data security contract terms should include appropriate monetary remedies, it is equally important to ensure that your company has appropriate controls in place in order to help prevent a data breach from occurring in the first place.

Know Your Insurance

Before your business faces a security crisis, it's helpful to have a good understanding of what costs (if any) your insurance policies may cover in the event of a data security breach, regulatory investigation, and/or related litigation. Some policies are generous; others cover very little, if anything. Moreover, even if coverage does apply, there are certain pre-conditions that will need to be met. Having a good understanding of these points will greatly assist the company when the need arises.

Conclusion

Understanding the patchwork of federal, state, and industry data security obligations and best practices can create challenges for businesses that handle personal information. While there is not a single solution to complying with the varied requirements, a holistic evaluation of a business's current information practices, along with application of these outlined security action items, can establish a framework that greatly reduces the company's risks associated with data security crises.

¹ 201 Mass. Code Regs 17.00 et seq. (implementing Mass. Gen. Laws ch. 93H, §2).

² Nev. Rev. Stat. § 603A.215.

³ Wash. H.B. 1149 (to be codified in Was. Rev. Code ch. 19.255).

⁴ See, e.g., *Data Accountability and Trust Act*, H.R. 2221, 111th Cong. (2009); *Data Breach Notification Act*, S. 139, 111th Cong. (2009); *Personal Data Privacy and Security Act of 2009*, S. 1490, 111th Cong. (2009).

⁵ See, e.g., *FTC, Press Release, Dave & Buster's Settles FTC Charges it Failed to Protect Consumers Information* (Mar. 25, 2010), available at <http://www.ftc.gov/opa/2010/03/davebusters.shtm>; *FTC, Press Release, Widespread Data Breaches Uncovered by FTC Probe* (Feb. 22, 2010), available at <http://www.ftc.gov/opa/2010/02/p2palert.shtm>; *FTC, Press Release, Mortgage Broker Who Dumped Computer Records Settles FTC Charges* (Jan. 20, 2010), available at <http://www.ftc.gov/opa/2010/01/navone.shtm>.