Legal Briefs Data Security & PCI Compliance

Keep It Clean: Getting Compliant with Information Security Requirements will Help Avoid a Messy (and Expensive) Data Leak

Small businesses have a lot to worry about, so information security is typically not at the top of the list. Sometimes, it's not even on the list. Recent developments have, however, significantly raised the stakes for small businesses. Understanding the risks and requirements is your first step to dealing with the issues at hand. This article is intended to give you a flavor of some major requirements and issues in information security law, and why the risks of noncompliance are important to you.

Why Should You Care?

Because government agencies care (and, as described below, you have certain legal obligations to fulfill). The Federal Trade Commission has taken more than 20 actions alleging that inadequate information security constituted an unfair trade practice. These actions are typically settled with the offending entity, in which settlements require implementation of a comprehensive, written information security program and a third party audit of compliance with that program every other year for 10 or 20 years. Multiple state attorneys general have taken similar actions at the state level. In addition, Mississippi recently became the 46th state to enact a law requiring businesses experiencing a security breach to notify affected individuals if their personal information is impacted (North Carolina adopted its version in 2005). These laws mean that when certain personal information is either lost or stolen (e.g., an employee loses records containing financial account numbers, your system containing payment card numbers is hacked, etc.), you may have a legal obligation to send letters to each person affected (whether customer or employee) explaining what happened. That letter may be read with interest by regulators, plaintiffs' attorneys, the media, and, unfortunately, potential investors or customers. Whether you're responding to government enforcement or containing a security breach, productivity and cash flow will both be adversely affected.

What Are the Requirements?

• Security Breach Notification

As mentioned above, if something goes wrong with your information security program and personal information is adversely impacted, you may have a legal obligation to report that incident to the affected persons (e.g., your customers). In North Carolina, notification must also be made to the state attorney general who, not coincidentally, is the person authorized to charge you with an unfair business practice if it turns out your security was lax.

• PCI DSS

The Payment Card Industry Data Security Standard ("PCI DSS") is, for the most part, a privately-enforced set of security requirements issued by the major payment card brands (Am Ex, Visa, Discover, MasterCard and JCB). The PCI DSS requirements are typically applicable to merchants by way of their contracts with acquiring banks. The acquiring banks have an incentive to require compliance and enforce against noncompliance because the card brands will fine the banks in the event of data breaches that affect payment cards and necessitate reissuance of affected individuals' cards. There are a lot of costs associated with reissuing cards, and the point here is to downstream those costs to the merchant if their security was not sufficient. To the extent breaches were due to a merchant's failure to abide by PCI DSS, the consequences for the merchant can be fairly dramatic. The bank typically retains the right in the contract to withdraw funds directly from the merchants' account without much, if any, due process in the case of alleged PCI DSS noncompliance.

Although the majority of PCI DSS enforcement is private, three states have incorporated some or all of the standards into their laws and applied those requirements directly to merchants. Nevada is has incorporated PCI DSS in full such that any entity processing card data must fully comply as a matter of law. Washington and Minnesota apply PCI DSS less broadly than does Nevada, including some safe harbors, but the overall thrust is to hold merchants directly liable to banks for costs associated with breaches of card data.

Topics covered by PCI DSS include: firewall installation and maintenance; system passwords and other provider-supplied default security settings; access rights; anti-virus software; unique user IDs; physical security; system logging; testing; and written policies and procedures addressing information security.

• State Information Security Laws

Many states now require that businesses handling "personal information" implement certain information security measures. The definition of "personal information" will vary depending on the state and the law, but almost always includes Social Security numbers, driver's license or other state-issued ID numbers and financial account numbers (including payment card numbers). In North Carolina, there is a mandatory obligation to securely dispose of personal information, which is more broadly defined than is typical of state security laws and includes, for example, seemingly innocuous information like Internet account numbers and email

Continued on page 17

Legal Briefs Data Security & PCI Compliance

Continued from page 16

addresses as well as more sensitive information like biometric data and maiden names. Other states, like Massachusetts, are much more extensive in their requirements and go well beyond information disposal. Because these laws usually apply based on the residency of the individuals in question, you may have to worry about more than one state's law if you hold personal information about customers or employees in multiple states.

• **Federal Trade Commission Disposal Rule**

If you run credit checks or other types of background checks on employees or consumers, this federal regulation will require that you securely dispose of that information by cross-cut shredding or any other method that renders it unreadable and unusable.

• **Federal Trade Commission Red Flags Rule**

Without getting into the details, the fate of this federal regulation is as yet undetermined. As written, it will apply to your business if you qualify as a "creditor." That term is defined broadly, so if you allow customers (generally individuals, not businesses) to maintain a line of credit or otherwise provide service but allow them to pay for it later (such as invoice-based billing) the rule may apply to you. It requires creditors to take steps to curb identity theft, such as by implementing written procedures to ensure that the person requesting the service actually is the person they claim to be. An easy example would be requesting a photo ID prior to opening up the line of credit. The rule has, however, been challenged repeatedly in court and has been delayed multiple times by the Commission. The current enforcement deadline is December 31, 2010 unless an earlier date is specified by Congress in the meantime.

What Should You Do?

Here are a few steps you should take to mitigate risk in this area. This list is not exhaustive, but presents a good starting point:

• Carefully review your contracts with banks or service providers that play a role in your process for conducting payment card transactions. Consider questions like: What does the bank require of you? What happens if you don't comply (can they withdraw funds from your account as a fine)? Is your provider giving you a PCI-compliant processing solution? Did they guarantee that in your contract?

• Never retain full card data from the magnetic stripe, sometimes referred to as track data or magnetic stripe data. If you retain the full card number, secure it while your retain it and securely delete or destroy it as soon as the transaction clears.

• Get PCI DSS compliant if you are not already. What that means will vary depending on the volume of your payment card transactions. Each card brand sets and defines their own levels, but generally speaking there are four levels. Level 1 is the highest and carries the greatest burdens, such as submitting to a third party assessment. Level 4 is the smallest and typically requires an annual written self-assessment. Vulnerability scans may be required or only recommend, depending on the volume of card transactions.

• Apply reasonable security measures to personal information. Make sure access by your employees and others is limited on a need-to-know basis. Use physical security, like locking file cabinets, whenever possible. For electronic records, avoid storing personal information on any unencrypted portable device like a laptop, thumb drive, CD, PDA or smart phone. Document your security procedures, such as how you grant access rights, so that you can demonstrate them if called on to do so by a regulator or in litigation (and because PCI DSS and certain states require it).

• Ensure that all records containing personal information (even something innocuous like email address) are cross-cut shredded or otherwise disposed of so that they cannot be "practicably read or reconstructed." When it comes time to dispose of electronic records, degauss or wipe so that information cannot be resurrected. Remember that North Carolina requires a written policy documenting your information disposal process.

• Be careful of service providers that handle personal information on your behalf. You are responsible for their actions (or inaction). Some states require that you have an appropriate contract in place regarding the provider's information security. North Carolina requires such contracts with anyone engaged to dispose of personal information on your behalf. And, even if not required, a contract is a good idea to protect you against some of the risks described above.

Elizabeth Johnson is an attorney at the law firm Poyner Spruill LLP. She practices privacy and information security law, representing clients from many industries ranging in size from small businesses to Fortune 100 companies. She can be reached at 919-783-6400.