DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

Consider the security-breach notice rules adopted by 45 U.S. states. These laws generally make the retailer responsible for security breaches at service providers who are holding or processing information on behalf of the retailer and provide no exception for PCI compliance.

Prior to Data Loss, Check That Contract

When a security breach happens, retailers are alone on the hook unless they have carefully crafted their agreements with third-party service providers, say Tom Bell and Susan Lyon.

Tom Bell is a partner in the Privacy & Security and E-Commerce Practice Groups at the Seattle-based law firm Perkins Coie LLP. Susan Lyon is of counsel in the Privacy & Security and E-Commerce Practice Groups at Perkins Coie.

It's 4:30 p.m. on Friday when you, the retailer, receive a call reporting a data-security breach at your service provider (e.g., call center, customer support, processor, etc.). The breach includes personal information from your customers. You think back six months to when you finalized the contract with the service provider and recall that the service provider agreed to comply with the Payment Card Industry data-security standard (PCI). Does that protect you from all claims? If not, what claims are you subject to and who will pay them?

Since January 2005, over 245 million data records of U.S. residents have been exposed in security breaches, according to privacyrights.org. The bottom line: security breaches can occur in any organization.

Courts have routinely denied recovery of damages from retailers and other collectors of personal information in most breach cases. Those courts have so far found lack of a contractual duty or insufficient evidence of harm to support a claim of judgment in favor of plaintiffs (e.g., banks issuing compromised cards or consumers).

Absent actual identity theft or other harm, such as with the disclosure of sensitive medical data, past cases indicate that U.S. courts are not likely to make a retailer pay affected banks or individuals for mere data exposure. Does that mean the retailer or other collector of personal information will have no liability for the security breach at the service provider?

Focused on the Breach

On the contrary, security breaches cost companies an average of $197 per record, according to the Poneman Institute's 2007 Annual Study: Cost of a Data Breach. With courts denying liability against retailers who suffer the security breach, what are those costs?

Ponemon's research concluded that lost business due to churn (including customer reacquisition) accounted for 56% of the costs. Customer contacts and notifications (inbound, outbound, and PR) were 14%. Investigations, audit, and consulting services added 15%. Legal defense costs were 8%.

Whose systems allowed the breaches, and therefore the costs, to happen? Third parties (like the service provider) accounted for 40% of security breaches. Perhaps more relevant to the retailer and service provider, the average cost for a security breach at a third party was $238 per record versus an internal security breach cost of $171.

Going back to our Friday afternoon call, is the PCI-compliant service provider obliged to cover those costs? The short answer is likely, "No."

Consider the security-breach notice rules adopted by 45 U.S. states. Those rules require the retailer or other data collector to notify customers of security breaches. These laws generally make the retailer responsible for security breaches at service providers who are holding or processing information on behalf of the retailer and provide no exception for PCI compliance.

Why? PCI is a standard promulgated by the credit card payment brands and is binding based on contractual arrangements in the credit card regime. States and government regulators are not bound by it. When it comes to notification obligations, they are focused on the breach, not on how it occurred or whether a security standard was followed.

What should a retailer do to protect itself? The Federal Trade Commission's (FTC) 2005 case against BJ's Wholesale Club provides a good starting place. BJ's suffered a significant security breach. The FTC looked to PCI standards when investigating whether BJ's used reasonable care in securing the data, but concluded that by failing to provide adequate security BJ's violated the Federal Trade Commission Act.

The FTC required BJ's to implement a written program with "administrative, technical, and physical safeguards appropriate" to the information collected and its size and complexity. The FTC mandated that minimum safeguards must include:

- Designation of an employee in charge of the data-security program;
- Identification of material risks (internal and external);
- Reasonable safeguards to control the identified risks; and
- Updating the security program in light of changed circumstances.

Given the significant percentage of security breaches that occur at service providers, and given that those third-party breaches are more costly, the prudent retailer will take service providers (and any party it shares information with) into account in its security program. The provider's compliance with PCI should reduce the risk that a breach will occur, but it will not prevent a security breach or shelter the retailer from the associated costs. Neither state regulators nor the FTC are likely to accept the defense that "I (or my service provider) complied with PCI."

Third parties account for 40% of security breaches—at an average cost of $238 vs. $171 for an internal breach.

The prudent retailer will take service providers into account in its security program.

Rules for Third Parties

Prior to sharing personal information with a service provider, the retailer should carefully consider:

1. Due diligence. Ask the service provider about prior security breaches at its facilities. Ask for and review recent security audits, or at least certifications and descriptions of those audits. Review the service provider's security program.

2. Contract provisions. Consider these issues in the service provider contract:

- **Define the issue.** Confidentiality clauses are not enough. Neither is PCI. Broadly define personal information. Require that the service provider commit to a security program and consider whether it should encrypt all personal data.
- **Notice.** Require that the service provider give the retailer immediate notice of any security breach of personal information.
- **Cooperation.** The retailer will need the service provider's cooperation to investigate and fix the security breach, notify customers, and deal with law enforcement. Have the service provider appoint a 24/7 security contact.
- **Responsibility.** The retailer will be first in line to pay the costs described above. If the security breach is caused by the service provider, define what the service provider should pay. Make sure the damages cap is high enough to cover those costs.

3. Monitor. Monitor the service provider's compliance. At a minimum, require that the service provider report the results of its own internal security audits. Consider a separate right to regularly audit the service provider's security practices.

The risks and costs briefly summarized above have surfaced over the last three to five years. Banks, processors, consumer advocates, and regulators continue to consider other costs (e.g. credit card replacement fees and fraudulent charges) and how those should be allocated. Retailers need to be part of that process. Otherwise, as in our example, they will pay costs caused by another party. DT