PUBLICATION

Does Your POS Comply with PCI and New State Statutes?

December 22, 2009

What's a good New Year's resolution for any business in the hospitality or retail industry? Take a look to make sure your Point of Sale (POS) systems are PCI-DSS (Payment Card Industry- Data Security Standard) compliant.[1]

According to a recent report by Verizon, 20% of data security breaches occur in the hospitality and food/beverage industry, with POS system attacks being the most frequent.[2] Most businesses rely upon third-party software and support of their POS systems, assuming the third-party technology experts will install and maintain the systems that will protect important customer financial information captured by the POS and are compliant with applicable governmental and industry standards.

But owners can't make assumptions in this regard, as merchants in Louisiana and Mississippi discovered. In a suit filed by several restaurants in Louisiana and Mississippi against a local POS supplier, the merchants allege that Georgia-based Radiant Systems' Aloha POS solution stored all of the information captured from customer bank card magnetic stripes in an unencrypted format (including card verification and PIN data) after customer transactions.[3] The complaint alleges the vendor failed to comply with PCI-DSS by storing (a) excessive amounts of customer financial account information and (b) storing that information in unencrypted form. The complaint also alleges the vendor used sloppy administrative controls in maintaining the system. Computer World, the exclusive provider of the Aloha system within the restaurants' territory, installed remote access software on the POS system to fix problems off-site. The log-in and password Computer World technicians allegedly used was the same for all 200 of its Louisiana customer locations, and both the login and the password were the "defaults" that came with the system and were listed in the program documentation. In this case, the default login was "administrator" and the default password was "computer"!

The result? A Romanian hacker accessed the POS systems of over a dozen businesses and installed malicious software to capture all of the POS customer credit card information.[4] The security attack was discovered by one of the restaurant employees and so far has resulted in thousands of dollars of chargebacks from customers, credit card company fines and costs related to computer audits. [5]

According to Charles Hoff, general counsel of the Georgia Restaurant Association, this type of hack is just the tip of the iceberg for POS security breaches. Mr. Hoff indicated that most of the time technology vendors settle security incident complaints like this one rather than risk public exposure through a court case. [6]

Another popular breach method for POS systems involves a hacker gaining access to the system of a third-party supporting POS installations to steal log-in credentials. With these credentials, the hacker can use what appear to be "legitimate" usernames and passwords to access the merchants' POS terminals and servers. Many third-party support organizations, like the maintenance provider for the Aloha POS system, may use the same username and password for all of their POS merchant installations, making such attacks easier.

So how do you protect your POS systems from such blatant attacks? First, make sure your POS vendor is PCI-DSS compliant and has the latest patches for security issues that have arisen since release of the POS software version you have installed.[7] Have the vendor provide a representation and warranty to that effect in your contract for the POS system (or an addendum, schedule or similar supplement or amendment to the contract) and create an ongoing obligation in the contract that the vendor will warn you of security threats or notices from any party if the specific system installed at your business fails PCI compliance or is subject to a security incident. You might also want to include a contract provision for security audit rights or add specific attachments to the contract that spell out how the vendor handles security procedures (from resetting default passwords[8] to background checks on vendor employees who will have access to log-in information).

Second, make sure you have adequate internal controls on your POS system. A sound practice is to make sure your POS system isn't continuously connected to an open network (like the internet) or that a proper "firewall" is in place to screen unauthorized access. Make sure that any financial information that is stored on the system is encrypted. Don't store customer data for any period longer than absolutely necessary. Purge credit card numbers, PINs and card verification data as soon as possible after the transaction is complete.

Many times companies look at the "cost" of a deal as the purchase price for the POS system. But in the POS acquisition environment, the real cost isn't what you pay the vendor – it's the total cumulative liability you could be incurring for installation of systems that aren't up to industry standards. In the Louisiana litigation, one restaurant paid only $20,000 for the POS system – but now has spent many times that amount in damages as a result of a security breach that could have been avoided.

New State Regulations

For years, data privacy and security laws that require a business to protect consumer personal and financial information have been implemented on the state and federal level. But a new regulation that will take effect in March 2010 may change the playing field.

A new regulation issued by the Massachusetts Office of Consumer Affairs and Business Regulation (201 Code Massachusetts Regulations 17.00) requires that every affected business take reasonable steps in the selection and retention of technology vendors the business uses in collecting and storing personal information (a due diligence requirement before you contract for any technology). Further, effective March 1, 2010, *all businesses covered under the regulation must include a section* ***in every relevant vendor contract*** *requiring the vendor to comply with appropriate security measures* (as set out in the regulation).

While the regulation only covers businesses that collect/house personal information of Massachusetts' residents, it is consistent with the current Federal Trade Commission Safeguard Rule that applies to financial institutions and is probably just the first in a series of new state laws and regulations that will attempt to mandate, by statute, the type of best practices in technology contracts that many software vendors have resisted (and practices that many small software vendors have failed to, or cannot, comply with).

What does this mean for the typical business? If you take and store the information from one personal check that has printed checking account numbers from a Massachusetts resident or employ even one person who claims Massachusetts residency for whom you are required to keep W-4/I-9 forms (including social security numbers), 201 CMR 17.00 is waiting for you.

The good news is the new Massachusetts regulation doesn't require much beyond what should be standard business practice for any company capturing and storing personal financial data. It just makes these best practices a regulatory mandate (and requires that you pass this mandate down to your technology vendors by contract).

As computer criminals become more sophisticated, the hospitality and retail industry can expect more attacks against their most vulnerable spot: the POS system. Audit your current systems. Review your POS vendor contracts and contact your current vendors about security concerns. And be alert to this overlooked threat to the finances and goodwill of your business.

If you would like to discuss the impact of the new state requirements or the type of provisions you should include in any of your technology contracts with vendors that relate to the personal financial information you collect, please contact your Baker Donelson attorney.

---

[1] The PCI rules stipulate certain procedures, processes, and technology elements in POS systems designed to enhance security of payment cardholder information captured in typical merchant transactions. See generally, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

[2] 2009 Data Breach Investigative Report, Verizon.

[3] The plaintiffs include Crawfish Town USA, Don's Seafood & Steak House, Picante's Mexican Restaurant, Mel's Diner, and two locations of Sammy's Grill. Crawfish Town USA, Inc. et al. v Computer World, Inc. and Radiant Systems, Inc., filed 15th Judicial District, Lafayette Parish, State of Louisiana, March, 2009.

[4] One diner processing about 60 to 70 card transactions a day indicated that 669 card numbers were stolen during one three-week period during which the hacker was in his system. See the report online at: http://www.wired.com/threatlevel/2009/12/breaches-more-sophisticated/

[5] Cost for one user totaled $19,000 for forensic audit, $5,000 fine from Visa for not being PCI compliant, a $100,000 fine for not being PCI compliant (that was eventually waived) and $20,000 in customer chargebacks. Id.

[6] Id.

[7] According to Verizon, less than 20% of such systems confirmed to be PCI compliant were implicated in a breach. Verizon, supra.

[8] The Verizon study found that over half of the reported incidents related to unauthorized access via the default or shared usernames and passwords. Supra.