# PUBLICATION

## The New Wave of Cyber-Crime Facing Retailers

**September 13, 2010**

*Originally published in Shopping Center Legal Update*

Retailers are under attack from a new wave of low-tech, high-tech criminals. These second-generation cyber-criminals are not necessarily the genius-hacker-types popularized by Hollywood in tag lines such as "Log on. Hack in. Go anywhere. Steal everything."[1] This new generation of cyber-criminal merely combines a rudimentary knowledge of the digital data collection/ storage processes used by retailers with a basic understanding of human psychology. Nevertheless, the result of the new low-tech criminal activity is that retailers are losing millions of dollars in revenue every year, and losing hard-won brand credibility when such activity adversely affects customers.

### Point of Sale (POS) as Point of Attack

A recent case in Louisiana, *Crawfish Town, et al. v. Computer World and Radiant Systems*,[2] illustrates the very real threats faced by retailers from the new breed of cyber-criminals, even when such retailers rely upon sophisticated Information Technology (IT) vendors to support their business processes. The *Crawfish* complaint alleged that:

1. The plaintiffs purchased a POS system and support from a local IT supplier, under the assumption that the POS system complied with industry security standards. However, the POS devices at the retail locations allegedly stored (locally) all of the information from a customer's bankcard magnetic stripe in an unencrypted format (including card verification and PIN data) after a customer transaction.
2. The remote access software on the POS system (designed to allow their POS vendor to correct local retail locations' problems from off-site) used the default settings that came with the system.[3]
3. These default login credentials were used for all of the POS vendor's customers, making all of the POS customers vulnerable to a security breach once a cyber-criminal discovered the default settings.

As a result, a relatively low-tech hacker allegedly accessed the POS systems of the retailers and installed malicious software in an effort to capture all of the POS customer payment card information.[4]

Charles Huff, general counsel of the Georgia Restaurant Association, indicated in late 2009 that the *Crawfish* case was "just the tip of the iceberg for POS security breaches," since most IT vendors settle security complaints rather than risk public exposure through court cases,[5] which is exactly what happened in the *Crawfish* case after some initial pre-trial activities—the settlement included new educational materials provided by the vendor on the threats faced by retailers. (The material indicates that three times as many restaurants were victims of credit card theft in 2009 as in 2008).[6]

### Data Privacy and Security—It's Not Just About the Retailer Anymore

Retailers are subject to a patchwork of federal and state regulation with respect to securing their data systems and protecting the digital information that is input into and stored on these systems.[7] However, new state laws have begun to acknowledge the growing dependence of retailers upon their IT vendors with respect to data privacy and security, and have set new standards for retailers in contracting with these vendors.

Specifically, a new Massachusetts data protection law provides insights into industry standards to which retailers will be subjected and requirements with respect to using vendors in administration of those standards.[8] The new law adopts a "risk-based" approach to data security, requiring a written security program by the business owner that takes into account the business's size, scope of business, resources, nature/quantity of data collected and stored, and the need for security.[9] However, the new law also sets minimum standards that require encryption of data on laptops and other portable devices, up-to-date firewall and operating system patches, and practical login credential provisions. The new law also explicitly provides that simply hiring an IT vendor for these functions does not absolve the retailer from liability; each retailer must complete minimal due diligence on potential IT vendors to make sure that they are compliant and include within the vendor contract (as of March 2010) provisions requiring the IT vendor to implement and maintain the same type of security measures for personal information as set out in the statute.[10] While this new law only relates to Massachusetts resident information, it is clearly consistent with current trends in the marketplace to force compliance through the chain of control of digital information, even down to the vendor level, to those points most vulnerable to attack.

With respect to POS and other personal financial information, retailers are also subject to the vagaries of evolving credit card company standards and merchant processing systems. Standards such as PCI-DSS and PA-DSS[11] provide the general requirements for both systems and processes that must be in place within retailers. The ultimate enforceability of these standards lies with the ability of the credit and debit card processing entities upon which retailers are reliant to access penalties and fines—or even cease the processing of financial transactions.

### Getting Past the Acronyms to the Real Problem

What do all of these statutes and acronyms mean to a retailer that is faced with the new cyber-criminals? Basically, data security and protection of customer financial information for retailers is about much more than technology buzz-words or verbal reassurances from your IT professional (or your IT vendor) that your company is "compliant" with whatever data privacy or security standard is being tossed about. The real problem is human nature—and the business process steps that retailers can take to interject themselves between the habits of employees/subcontractors and the low-tech cyber-criminals that prey on very real human weaknesses in the digital domain.

### The Weakest Link in Data Security—People!

People are creatures of habit. With respect to data security for retailers (and low-tech cyber-criminals), that means that the weakest link in any retail data system is probably going to be a result of human nature.

Start with logging on: This simple human task associates a "username" with a "password" to gain authorized access to retail data processing systems (locally at your retail location or globally across your retail support systems). In 2009, in one security breach, over 30 million passwords were pirated and posted to the Internet.[12] Given the volume of the breach, we now have a remarkable snapshot of how psychology interacts with technology to create risks:

The passwords in the 2009 security breach were stored on the hacked system in native, unencrypted formats. Once the hacker gained access to the database, all of the password information within the database was available for criminal use without any further effort. The practical lesson for retailers—when customer, financial or other valuable personal information is stored (whether in a large centralized database, on a lowly laptop PC or even on a $20 thumb drive)—is always to store that information in encrypted format.

If left to our own discretion, humans are very careless about creating username and password combinations. The analysis of the 30 million stolen passwords revealed that the top five passwords selected by users included (in order): 123456, 12345, 123456789, Password and iloveyou (probably because the breach was of

a social networking site). Almost all of the top 5,000 passwords (that were used by 20 percent of the users) were names, slang words, dictionary words or trivial combinations of consecutive characters (such as 12345). Using a relatively low-tech "brute force" attack and the list of 5,000 passwords as a guide, a hacker with relatively meager skills could gain access to one account every second and could access up to 20 percent of all accounts within a reasonable time period.[13] (Remember: All of this hacked information was uploaded to the Internet, so every criminal in the world had access to it.) The practical lessons for retailers:

- Do not let your employees (or your customers) choose the passwords they use for your retail systems without some very persistent guidance. For example, use applications that advise employees and customers of the strength of their password or that force more complex passwords (using requirements for special characters, letter/number combinations, punctuation, a mixture of lower and upper case characters, etc.).
- Educate employees and customers about using mnemonics or simple sentence structure abstractions in constructing passwords (in order to avoid passwords that have popular significance, such as a word in the dictionary or a slang term). For example, as suggested by iMPERVA, swap out letter combinations with numbers (e.g., substitute "2" for "to") or take a sentence such as "This little piggy went to market" and abstract it into "tlpWENT2m."[14] Forcing complex passwords without providing education about why they are required and how they can be easily created and used by others is a bit like trying to swim upstream—you can encounter a lot of resistance.
- Implement mechanisms to detect and limit the type of low-tech brute force attacks that allow low-tech hackers to capture large numbers of login credentials. For example, for systems exposed to the Internet, use CAPTCHAs or other challenges to slow down the speed at which cyber-criminals can access your systems and monitor your systems for unusual activity (especially from international servers under-represented in your typical customer profile).[15]

Frequently, people find a username and password combination and use it repetitively. A recent report by *Reuters* indicates that the vast majority of banking customers use their bank login credentials to access other Web sites.[16] The report estimates that over 70 percent of Internet bank customers use their online banking passwords with non-financial sites, and almost 50 percent use both their online banking username and banking password at other Internet sites.

The practical lesson for retailers:

- Create a business rule/process that forces employees (and customers/vendors accessing retail systems) to create unique passwords for access and then educate them about the risks involved in using the same login credentials across multiple systems and sites. For example, implement rules as set out above with respect to special characters, letter/number combinations, punctuation, or a mixture of lower and upper case characters and explain why this is important.
- When capturing financial information at a retail location (such as PIN data), remember that the PIN may be used by the consumer for other purposes (such that exposing the PIN in unencrypted formats, locally or in a centralized database, may jeopardize not only the customer relationship with the retailer, but also with other merchants with whom the consumer uses the same login credentials).

Also, remember that people create almost all of the software and systems a retailer contracts for, so the issues with respect to login apply equally to all vendors and subcontractors of the retailer. This includes those vendors supplying financial capture and other POS devices, providing IT consulting services, and other vendors who we may consider to be "sophisticated" in the ways of security and privacy. A few tips:

4. Conduct due diligence on vendors that are providing the services, software applications or hardware that touches your data and the data of your customers.

5. Have each vendor provide a representation and warranty in their contracts with respect to critical compliance issues (such as Payment Card Industry compliance for financial information),[17] and
6. 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/used for your retail business fails or is subject to a security incident. You may also want to include a provision for security audit rights or have specific attachments to vendor contracts that spell out how the vendor handles security (from resetting default passwords18 to background checks on vendor employees who will have access to login information).

## Summary

Data-rich retailers are clearly being targeted by cyber-criminals. These attacks start at the POS (with devices that are easy targets for low-tech hackers) and extend to enterprise-level exposures that are inadvertently created by ignoring both industry standards and the habits of retail employees and customers. While technology is key in reducing digital risks in retailing (and evolving laws and regulations clearly link digital risk assessment/reduction with implementation of the appropriate levels of technology), education of customers and employees and adoption of simple business process steps (such as effective login credentialing and use of login challenges) can have a huge impact in reducing overall retail exposure to the vast majority of low-tech digital attacks. Adequate due diligence of IT vendors, and recurrent audit and supervision for compliance by these vendors, also play a part in reducing the digital risks in the retail market space.

Audit your current systems. Review your vendor contracts and contact your current vendors about security concerns. And be alert to the growing number of low-tech, high-tech criminals that represent one of the greatest threats to the finances and goodwill of your retail business.

7. Tagline from the movie *Swordfish*. See http://www.imdb.com/title/tt0244244/

- 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.
  - In this case, the default login, as set out in the published documentation for the system, was “administrator” and the default password was “computer.”

- 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/
- *Id.*
- Personal communication, March 31, 2010.
- See, generally, the regularly updated listing of resources maintained by the National Conference of State Legislatures at http://www.ncsl.org/Default.aspx?TabID=756&tabs=951,71,539#539.
- 201 CMR 17.00, implementing M.G.L. Chapter 93H.
- 201 CMR 17.03.
- 201 CMR 17.03(2)(f)2.

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

  The PA-DSS deals with secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure that their payment applications support compliance with the PCI-DSS. See, generally, https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
  - The breach involved a security problem published by iMPERVA and reported at http://techcrunch.com/2009/12/14/rockyou- hacked/. iMPERVA subsequently posted a report analyzing the compromised passwords. See: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf.

- *Id.*, at page 4.
- *Id.*, at page 5.

- CAPTCHA is an acronym for a specific type of challenge and response process, called Completely Automated Public Turing test to tell Computers and Humans Apart. Note that even CAPTCHA systems are under attack and have been breached, however.
- See http://www.reuters.com/article/idUSLDE61122W20100202.
- According to Verizon, less than 20 percent of such systems confirmed to be PCI-compliant were implicated in a breach. 2009 Data Breach Investigative Report, Verizon. See, generally, http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html
- The Verizon study found that over half of the reported incidents related to unauthorized access to data systems were via the default or shared usernames and passwords. *Id*.