CYBERSECURITY

THE NEW PROFESSIONAL RISK

PART 2 OF 4: KEEPING CUSTOMERS' DATA CLOSE TO THE VEST – CYBERSECURITY CHALLENGES IN THE RETAIL, RESTAURANT AND HOSPITALITY INDUSTRY

Karen Painter Randall and Steven A. Kroll Connell Foley LLP

The recent cyberattacks on large corporations such as Neiman Marcus, Target, eBay and Home Depot have brought cybersecurity to the forefront of mainstream pop culture, as the data stolen from these retailers exposed the personal identifiable information of millions of customers. Stolen credit card data typically is posted online and sold on the black market at prices ranging from $3 per Social Security number to as much as $1,000 per bank account login. While these figures seem modest, when multiplied by the millions affected, the financial and reputational damage inflicted can easily ruin any business. In fact, once a retailer suffers a major breach, consumer confidence drops, resulting in a significant drop in profit. As the total average cost of a data breach is now $3.8 million, up from $3.5 million the previous year, the question facing companies is not only how to prevent a cyberattack, but how to position themselves to sufficiently and quickly respond to same. In the second of a four-part series touching on various professional, business and insurance sectors, this article discusses cybersecurity and compliance issues facing the retail, restaurant and hospitality (RRH) industry in today's rapidly evolving technological climate.

TYPES OF DATA BREACHES AFFECTING THE RETAIL, RESTAURANT AND HOSPITALITY INDUSTRY

The number of reported data security breaches continues to increase while the types of breaches are becoming more diverse and sophisticated. Retail companies are often targeted by cyber criminals because they possess voluminous financial data across their chain of stores throughout the country and overseas. Often these companies are victims of Point-of-Sale malware. In general, there are three basic types of data security breaches that affect the RRH industry and lead to the compromise of a business' data: physical breach, electronic breach and skimming. The following is a brief overview of each type of breach.

PHYSICAL BREACH

The first type of data breach affecting businesses in the RRH industry relates to a physical breach. This involves the physical theft of documents or equipment containing cardholder account data, such as cardholder receipts, files, PCs and Point-of-Sale terminals. A physical breach can also involve terminal scams wherein an individual attempts to tamper with merchant Point-of-Sale terminals in order to gain access to card data contained in the device or to perpetrate fraud using the device. For example, a terminal scam may include phone calls received by merchants in which the caller attempts to reprogram client terminals.

Some best practices for a business in the RRH industry to employ to help prevent a physical data breach include: having a detailed security strategy that involves monitoring employees who use Point-of-Sale terminals and conveying clearly defined restrictions to them; installing cameras at computer room entrances and exits as well as check-out lanes where Point-of-Sale terminals are positioned; defining procedures to monitor the cameras and corporate networks and keep recorded footage for a reasonable period of time; requiring ID badges for access to sensitive data centers; and maintaining a log of visitors to sensitive facility areas.

ELECTRONIC BREACH

A second type of breach affecting the RRH industry is an electronic breach. This involves the unauthorized access or deliberate attack on a system or network environment (at a business or its third-party processor) where cardholder data is processed, stored or transmitted. This can be the result of acquiring access, via Web servers or Web sites, to a system's vulnerabilities through application-level attacks. Some examples of system vulnerabilities include unsecured remote access, lack of proper password management, and lack of proper access restrictions to cardholder data systems.

There are a number of methods used by hackers in the case of an electronic data breach. For example, a "packet sniffer" is an application that intercepts and logs traffic passing over a digital network or part of a network. This is a standard tool that has been used in network troubleshooting and analysis for many years. Unfortunately, this

tool is increasingly being used by hackers to collect card data in transit inside merchants' networks. Another example among the most dangerous of so-called "spyware" is keylogging. This interjects programs into a merchant's network systems using malware, which is then used to count and record data entry key strokes. Some more sophisticated programs can also capture screenshots containing data even though no data is typed. This allows hackers to obtain direct access to card data or to the system passwords that lead to it.

Once again, some best practices for businesses in the RRH industry include: never storing prohibited cardholder data, such as track data or card security codes on payment applications or in credit card processing environments; using only secure Web and database servers; and utilizing strong, up-to-date anti-virus, anti-spyware and anti-malware software. A business can also validate its payment applications' compliance with the Payment Application Data Security Standard (PA-DSS) or undergo a Payment Card Industry Data Security Standard (PCI DSS) code review to ensure that its system is in compliance.

SKIMMING

The third type of breach affecting businesses in the RRH industry involves skimming. Skimming is the capture and recording of card magnetic stripe data using an external device, which is sometimes installed on a merchant's Point-of-Sale system. Skimming can also involve a dishonest employee utilizing an external device to collect the card magnetic stripe data. The data is then used to create counterfeit credit and debit cards. Restaurants and bars are common victims for skimming because the perpetrator actually has physical possession of the victim's credit card. In this situation, the perpetrator often uses a device so small it can fit in the palm of their hand to read and store data encoded in the magnetic stripe on the back of the victim's credit card. The perpetrator may also use a small keypad device to record the three or four-digit security code printed in the signature box. Skimming may also involve tampering with vulnerable Point-of-Sale terminals and PIN-pad equipment. Typically, a perpetrator inserts a device into the terminal or PIN-pad at the merchant location, then uses it to collect credit card and PIN data.

Some ways to minimize skimming include closely monitoring the handling of cards when employees have frequent physical possession of credit cards out of view of the cardholder, closely monitoring activity on Point-of-Sale terminals and PIN-pad devices, and regularly checking equipment for attached skimming devices or evidence of tampering.

WHAT BUSINESSES IN THE RRH INDUSTRY NEED TO UNDERSTAND ABOUT COMPLIANCE

A regulatory body very active in regulating the RRH industry is the Payment Card Industry Security Standards Council (PCI SSC). Founded by American Express, Discover, JCB, MasterCard and Visa, the PCI SSC has promulgated a 12-part guide, the Payment Card Industry Data Security Standard (PCI DSS), for securing cardholders' information that RRH businesses store, process and transmit. PCI DSS v3.1 is the current enforcement of a new payment card security standard, which calls for immediately ending the use of the outdated Secure Sockets Layer encryption protocol that can put payment data at risk. The council demands that stronger encryption be used, although may still believe it is not sufficient and should require full-disk encryption on terminals that process card payments.

The penalties for failing to comply with the PCI DDS can be severe to businesses in the RRH industry. Namely, because the banks and card processors have separate agreements with members of the RRH industry for indemnification of the fines, based on the size of the business, these are often paid by the businesses themselves. As a result, businesses in the RRH industry must review their own internal policies and procedures to include PCI DDS fundamental security practices. Additionally, RRH industry businesses should also review and amend vendor contracts to address compliance with PCI DSS, as well as only use third-party providers that understand and operate in compliance with said standard.

Furthermore, in late 2014, President Obama signed a BuySecure Executive Order to accelerate the transition to stronger technologies and the development of next-generation payment security tools. This new technology will apply to both new and existing credit cards issued by the General Services Administration to government employees, as well as debit cards issued as part of benefit programs like Direct Express. It will also upgrade retail payment card terminals at federal agency facilities to accept Chip and PIN-enabled cards. With Chip and PIN technologies, credit, debit and other payment cards will contain embedded microchips instead of magnetic strips, and face-to-face transactions will require consumers to type their personal identification number (PIN), similar to ATM cards. Once fully in place, these measures will hopefully drastically reduce the number and scope of Point-of-Sale malware attacks.

CHANGES IN TECHNOLOGY

A company doing business in the RRH industry must also be cognizant of the technological changes occurring. For example, a deadline has been imposed for U.S. retailers and card issuers to adopt EMV chip-and-PIN technology by October 2015. Due to what is being called the Payment Networks' Liability Shift, financial institutions will no longer assume financial responsibility for fraudulent transactions if a merchant is using non-EMV compliant technology, including Point-of-Sale systems. While this may not prevent a future cyberattack, merchants in the RRH industry must take steps toward a more secure payment future.

Cybersecurity and compliance issues cannot be addressed across the board due to the limits placed based upon the size of a business and its budget. While larger companies within the RRH industry are the most lucrative targets of cyberattacks, it is the small to midsize company that will be forced to close its doors if a breach occurs for failure to have proper security safeguards and compliance best practices in place.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, NJ, and Co-Chair of the Firm's Cyber Security and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, a former Chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability, general insurance litigation and employment law handling matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, and received the distinguished award of Order of the Coif.