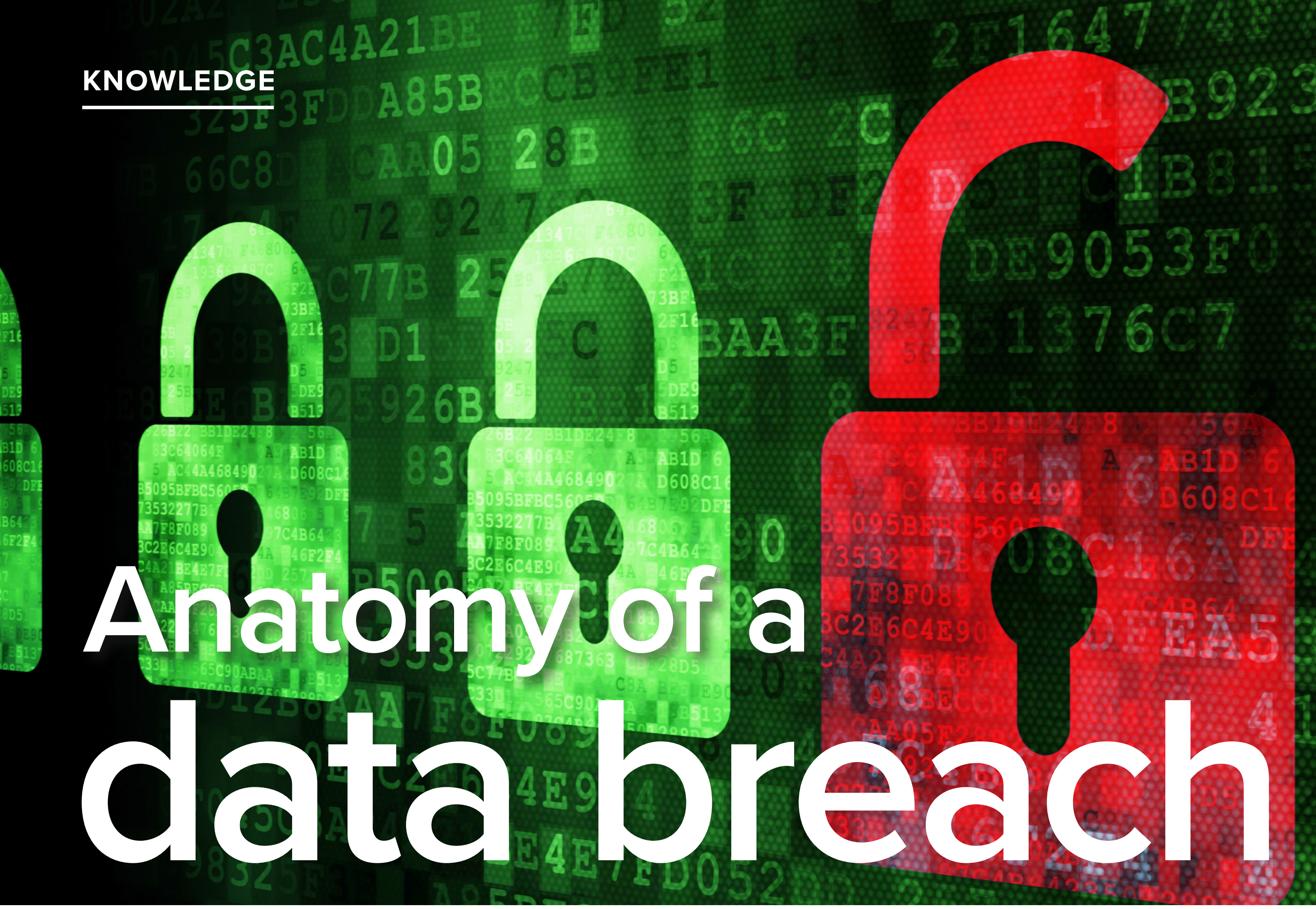

Anatomy of a data breach

By Justin Zeigler,
RSPA Data Security/
PCI Committee Chair

There you are, on what seems like a pretty unremarkable Tuesday morning. Coffee in hand, you open the door to your office and take a seat at your desk, ready to settle in to your routine — checking email and scores from last night's games — when the phone rings. It's one of your long-time customers. They're panicked. A rep from their bank called to notify them of a suspected data breach at their store. They were given a gaggle of instructions that they can't remember. Instead, they've been online researching the potentially business-ending fines that Visa may have in store for them. "You have a plan for this, right?" your customer asks you frantically. Well, do you?

According to the Identity Theft Resource Center (ITRC), in 2016, the number of U.S. data breaches rose 40 percent from 2015. Nearly half of the 1,093 reported data breaches last year affected the business sector; clearly, our industry has a growing problem. As a point-of-sale pro, your customers rely heavily on you not only to secure their systems within the guidelines of the most current version of PCI DSS (Payment Card Industry Data Security Standard) but also to stand at their side in the event of a data breach that may or may not have had anything to do with your installation. For that reason and others that we'll go over, it's essential that you understand the basic anatomy of a data breach and have a plan in place to mitigate liability for your customer and yourself should you ever find yourself in this position.

WHAT IS A DATA BREACH AND HOW DO THEY MOST COMMONLY OCCUR?

Simply put, a data breach consists of any unauthorized access to a merchant's network that leads to the theft of cardholder data. Breaches generally can be segmented into one of four categories:

- Network-related (remote hacking)
- Malware and spyware
- Attacks based on physical access (skimming devices, swapped hardware)
- Dishonest/criminal employees

By far, the most common type of breach is related to improperly secured remote monitoring and management (RMM) software. An easy-to-guess password (who could have known that "Password1" wasn't the way to go?), repeated use of the same password, accounts shared across multiple locations and/or an online-accessible list of remote management passwords have led to many of the recent high-profile breaches.

If you're reading this and thinking, "I use secure payments software, follow PA-DSS implementation guides to the letter and install the latest RMM solutions to monitor each site, so breaches won't be a concern for my customers," think again. Regardless of how secure the merchant's site, there's little a point-of-sale pro can do to prevent the installation of skimmers by a third party or protect against the actions of a dishonest employee. Until the forensic investigation (we're getting there) is completed, and you're absolved of any responsibility, it's in your best interest and that of your customers to have a breach plan in place and follow the necessary steps to mitigate losses for all parties.

WHAT CAN A MERCHANT AND POS PRO EXPECT WHEN A BREACH OCCURS? WHAT ARE THE STEPS?

Visa lays this out in more detail in their What To Do If Compromised supplement that's available on their website, but here are the basics:

- **Notification.** This is going to be determined by how the breach was discovered, but if the merchant's processor isn't yet involved, the merchant should contact their processor immediately and report the breach. The merchant will be asked to provide status of PCI DSS compliance and proof of PA-DSS validation from their payments provider.
- **Initial investigation.** Within three business days, provide the Visa Initial Investigation Report (available on their website), including actions taken to contain the breach. Do not alter the compromised system, change passwords or delete logs as this will interfere with the forensic audit. Limit further exposure by disconnecting the compromised system from the internet.
- **Independent forensic investigation.** Visa has the option to use a PFI (Payment Card Industry Forensic Investigator) to perform an independent forensic audit of the merchant's system. If Visa requires this, the merchant is responsible for the associated costs.
- **Provide exposed accounts.** All known or suspected exposed accounts must be uploaded to Visa's Compromised Account Management System (CAMS) within five business days.
- **PCI-DSS.** Compromised merchants must achieve full PCI compliance and be independently validated by a QSA before resuming integrated payments. Because this process is often time-consuming many merchants are forced to use non-integrated stand-beside terminals in the interim.

Beyond the steps to reduce losses and fines, merchants should also consider proactive outreach to their customer base to inform them of the breach. This is of course up to the merchant and their relative size and the scope of the breach, but a proactive approach to customer notification allows the merchant to control the narrative — instead of a third party.

WHO IS LIABLE?

Fees associated with data breaches quickly can reach exorbitant levels. Some of the fines to expect in a standard card data breach include merchant-processor and card-brand compromise fees, forensic investigation fees, on-site QSA assessments post breach, card reissuance penalties and, of course, the costs associated with legal counsel, technology and security updates to bring the solution back in spec of PCI-DSS. Depending on the scale of the breach, federal and municipal fines and an increase in processing fees should be expected as well. These fines often total hundreds of thousands of dollars and for large-scale breaches can climb into the millions. In many cases, a data breach is a fatal blow for a

continued from page 27

small merchant.

So, who is liable? In almost all cases, the merchant is responsible for a data breach as they're generally considered the "data owner," so a POS pro is unlikely to be directly fined unless you're responsible for managing, processing or storing consumer card data. That said, remember the forensic audit that we mentioned earlier? If the merchant (or more likely, the merchant's legal counsel) determines through that forensic audit that the breach was somehow the fault of the installer, the POS pro can expect to be sued in civil court. When a merchant is facing hundreds of thousands of dollars in data breach fines, their legal representation will search for any opportunity to transfer liability to you.

BEST PRACTICES FOR POS PROS TO PREVENT BREACHES AND MITIGATE LIABILITY

Establishing and maintaining diligent installation and maintenance procedures in conjunction with the use of secure and proven payments solutions are key to prevent data breaches and lessen associated liability should a breach occur for reasons beyond your control. Here are some best practices for POS pros:

- **QIR (Qualified Integrators and Resellers) Certification.** The card brands are messaging to merchants that they should only deal with POS pros that are QIR certified. If you're not on the list, you're missing out on installations (whether you know it or not) and potentially opening yourself up to litigation in the event of a breach. Beware of marketing gimmicks from payments providers that claim to help you skirt QIR. This requirement isn't going anywhere.
- **Clearly documented installation procedures.** Follow the PA-DSS Implementation guides (required for all PA-DSS validated payments apps), and create your own checklists to ensure that your merchants are able to achieve and maintain PCI compliance.
- **Diligent remote access methods.** This one is key. Most data breaches are caused by remote access intrusion; be sure to use proper password management procedures that comply with the latest PCI-DSS requirements, including multiple factors of authentication and encrypted connections.
- **Use of secured networking solutions.** RMM solutions can be a helpful tool to ensure that your merchants' networks are operating efficiently and securely.
- **Use of PA-DSS validated payments applications with a data security focus.** The use of a PA-DSS validated payment application is a prerequisite for a merchant's PCI compliance, so that should be a bare minimum requirement. Beyond that, look for proven payments solutions from established providers that offer security-centric features like EMV, point-to-point encryption (P2PE) and tokenization. Protecting data in transit should be a priority.

As payment security options like EMV, P2PE and tokenization become readily available to merchants, fraudsters are targeting merchants with outdated systems more aggressively. Secure payment implementation that adheres to a regimented installation procedure will go a long way toward protecting your merchant customers from a data breach and mitigating your overall liability. Of course, you can't completely eliminate the chance of a data breach no matter how careful you are, but with a little bit of preparation, employee training and the right mix of security-centric products, you can have confidence and peace of mind, secure in the knowledge that you have a plan in place should you ever find yourself on the receiving end of that panicked merchant call. c

RSPA's Data Security/PCI Committee, newly re-formed, can help the retail technology industry better understand the realities and risks of PCI compliance and be the voice of our community to strategic partners, such as the PCI-SSC. For more information on the committee, email Education@GoRSPA.org.

HELPFUL LINKS:

- https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
- http://my.gorspa.org/files/public/c201405_LegallySpeaking.pdf
- https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
- https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
- https://www.pcisecuritystandards.org/program_training_and_qualification/qualified_integrator_and_reseller_certification