

# BUSINESS credit

FEBRUARY 2009

THE PUBLICATION FOR CREDIT &amp; FINANCE PROFESSIONALS \$7.00

feature

## IT ONLY TAKES ONE DEALING WITH PCI-DSS

JACOB BARRON

With the advent of email and the Internet, the world of personal finance has taken a turn for the dramatic; whereas in prior eras, following the depression and the establishment of the Federal Deposit Insurance Corporation (FDIC), your money was yours, was kept in a bank and was safe from anything short of robbery coupled with governmental collapse. Now banks and their customers are beset on all sides by both active and passive security threats. Whether in the form of adolescent hackers, email scammers or merely a company's lax approach to IT security, the risks facing consumers and companies today are considerably greater than what they were even a decade ago, and a level of suspicion, as well as a judicious approach to spending, has become a necessity for sound financial management and planning.

But despite the increase in threats, the speed with which both consumer and B2B business is conducted shows no sign of slowing. Consumers continue to rely on credit cards and business vendors, despite the sometimes considerable, albeit manageable, interchange fees, continue to move toward accepting credit cards as a means of quick, assured payment. This being the case, the world of business and finance has had to come to terms with the seedy world of fraud, hacking and identity theft and find a way to better protect customer data and identifiable information.

The primary source of the data used and abused in breaches and hacks is from credit cards, which, as online transactions have increased, has become a bit easier to attain. Just a few years ago, as threats increased in frequency, notoriety and sophistication, regulations and measures were discussed and pored over in board rooms as much as living rooms, culminating in an agreement between all card brands to instate a set of standards to protect cardholder information. The result, established on September 7, 2006, was the Payment Card Industry Data Security Standard (PCI-DSS), a set of 12 standards that applies to all organizations, systems, networks and applications that process, store or transmit a cardholder number. This move, made with the blessing of Capitol Hill, requires companies that accept credit cards to never store any cardholder data beyond the name, number, expiration date and service code. Nothing has to be signed on the part of the merchant; if a company agrees to accept payment cards, it's implied that they will comply with these rules.

## Compliance

Twelve more standards atop the already considerable compliance requirements levied on businesses seems like an overwhelming prospect for companies merely looking to accept other payment cards as a means to reduce days sales outstanding (DSO) and increase payment cycles, but PCI-DSS compliance shouldn't deter merchants from making the switch to credit card acceptance. "Nothing here is so major that we can't overcome it," said Robert Day, vice president of commercial interchange at Fifth Third Processing Solutions. "It's a very serious matter and you do need to be alarmed, but at the end of the day, it's pretty simple stuff." In a recent NACM-sponsored teleconference, Day outlined what's expected of card-accepting merchants and iterated the seriousness of compliance, but still reassured his audience that all compliance requires is a carefully considered approach that's appropriate for the accepting company in question.

Credit professionals and companies should understand the 12 PCI-DSS standards and base a compliance plan around those basic tenets. They are:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Many of these standards are things that many companies already have in place and, depending on the sophistication of their business' operations, credit professionals may find only a small amount of work needs to be done in this matter. In addition to these 12 standards, PCI-DSS requires some merchants, depending on the size and number of transactions handled annually, to submit self-assessment questionnaires, conduct network vulnerability scans and, in rare instances, undergo on-site security audits. Day noted that these requirements were organized into four levels for merchants and three for service providers, with each level containing its own criteria pertaining to who falls into what category. "Unless you're doing a ton of transactions, you're going to fall in level four," he said. Level four companies are businesses that either do less than \$20,000 worth of e-commerce annually with one card brand, or businesses with less than one million transactions from any acceptance channel annually with one card brand. Luckily, these businesses aren't required to perform audits, nor is it mandated that they submit self-assessment questionnaires or network vulnerability scan results to card acquirers.

Still, Day noted that these things should be conducted as a best practice, and also noted that, should a company suffer a card data compromise, they could be bumped up to level one, which would then require them to undergo an audit and submit a report on compliance (ROC), as well as quarterly network vulnerability scans. For service providers, requirements are a bit more stringent, and even members of the lowest level, level three, that transmit fewer than one million transactions annually are required to conduct annual self-assessment questionnaires and quarterly vulnerability scans.

More information, including self-assessment questionnaires, can be found on the PCI-DSS headquarters website, at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI-DSS REQUIRES SOME MERCHANTS, DEPENDING ON THE SIZE AND NUMBER OF TRANSACTIONS HANDLED ANNUALLY, TO SUBMIT SELF-ASSESSMENT QUESTIONNAIRES, CONDUCT NETWORK VULNERABILITY SCANS AND, IN RARE INSTANCES, UNDERGO ON-SITE SECURITY AUDITS.**

### Common Errors

Despite the PCI Security Standards Council's (SSC) decision to use a more scalable, principles-based system, rather than an unforgiving, rigidly rules-based system, Day noted that many companies' security systems still fail to meet even the most generous definitions of adequacy. "You'd be surprised how many businesses don't even have a firewall," he said. "You'd be surprised how many people put routers and things like that in play and don't even change the default passwords. These are the things that they're telling you that you have to do." In several cases, Day noted that many companies put themselves in dangerous positions by thinking that the rules don't apply to them. "Some people say 'I'm not very big so this doesn't apply to me' or 'I'm so big and my network is so secure that no one's going to get into it,'" he said. "I do one transaction, 'I do a million transactions, 'I don't need to do this because our network is huge and it's so secure,' I don't need to do this because we only have one transaction per quarter;' the risk is not based on the dollar volume but on how many cards you touch. Even if you've touched only one card, you have to comply."

When actually working to comply with PCI-DSS, many businesses will make common-sense errors by overestimating one type of threat and leaving other vulnerabilities unchecked. "A lot of people will say 'we do business on a secure server, so bam, we're good,'" said Day. "You've spent a lot of time making sure that server was 100% by the book, but because you ran over budget on that, you decided to cut budget on some of your other computer stuff, so now a hacker gets into your other computers and once they get inside, they're inside. It's

like making a really strong backdoor, but if you don't put a \$5 lock on your front door, they're going to be inside in five seconds." Internal threats and a constant state of suspicion are also areas of PCI-DSS where companies open themselves up to potential violations. "You may spend a lot of money making sure that the server that handles your credit card data is secure, but it's not secure from your own network," he said, noting that personnel issues also come into play when trying to protect a company's customer card data. "You cannot just let anyone have access to these records. You need to make sure that you've done everything in your due diligence," Day added. "If you hire somebody with a criminal record that's had theft issues, or you didn't do a background check, if you think you're in compliance, Visa and MasterCard will not say the same."

**"THE RISK IS NOT BASED ON THE DOLLAR VOLUME BUT ON HOW MANY CARDS YOU TOUCH. EVEN IF YOU'VE TOUCHED ONLY ONE CARD, YOU HAVE TO COMPLY."**

One of the key spots where too many of a company's employees get a chance to traffic in customer data, increasing the risk of a breach, is in the acquisition and storage of customer information. As orders are received, processed and filed, depending on the vendor in question, employee access to that information broadens as does the risk that the customer's data will fall into the wrong hands. "It's about the card data. Some of it can be stored, the bulk of it cannot," said Day. "At the end of the day, you should be storing name, address and phone number. That's it."

Protecting a company from threats also comes down to what information is gathered on a tangible document, like a purchase order, and how it's organized. "You should never ever have a credit card number on your purchase order," said Day, who recommended that businesses looking to accept credit cards and prevent PCI-DSS violations consider an online payment environment, which can alleviate a great deal of a company's payment card security woes. "The web-based environment allows you to put the data in the system and stores the data off-site so you're never at risk," he said. "You should be running orders through a web gateway, one that will not store them on your PC but off-site, so that you're pushing the data away from you. Then you can recall the data as much as you want. Also, if you do recurring billing, it does it for you. You can have the web page set up and have the customer go there and enter it themselves. It takes you out of the equation." By shifting the burden of processing to another party, companies don't automatically come into total compliance, but they do take away the headache of protecting customer data from employees, whether they're disgruntled or merely absent-minded.

### So What If I Don't?

Since PCI-DSS doesn't mandate validation actions like questionnaires and vulnerability scans for all companies subject to

its standards, many company officials may easily write it off, rolling the dice and relying on the strength of their business' IT security setup. Some may store data in accessible places and violate other PCI-DSS precepts without any real repercussions for lengthy periods of time. The problem with this philosophy, however, is that it only takes one measly transaction to wreck a company's pristine record and wind up costing it thousands of dollars in fines. "You can store that data, it's just that if you get caught with it, they're going to come down heavy on you," said Day. "You want to keep that risk away."

While big-name breaches and multi-million, and sometimes billion, dollar violations are the ones that dominate the media, even minor, one-time breaches can wind up costing a company a great deal of potential profit. "Visa alone has fined businesses \$3.3 million for non-compliance," he noted. "One transaction, one credit card number, can result in hundreds of thousands of dollars in fines." Additionally, even if a company is technically compliant, breaches can get expensive even without penalties, including investigations and repayment, so while not all breaches may be preventable, PCI-DSS compliant companies will find their burden to be far smaller than those of non-compliant companies. "Even if you are breached and are innocent, keep in mind that when there is a breach, you do have to have an investigation and that is done and billed to you. If you *are* 100% good to go, you're not going to get the fees," said Day. "However, the data that was stolen from you — the breached data — you're still responsible for the lost money. One card could cost your company \$50,000 even if you're innocent. The good news is that the fines, fees and penalties will typically not amount to a whole lot more."

Some credit professionals might also ask themselves how this is anything other than an IT concern. The reality of the matter is that it should be *everyone's* concern. Day noted one instance in which a company was breached, found to be non-compliant and fined, resulting in ripple effects beyond the IT department. "Things came around, everybody got let go," he said, conceding that "I'm oversimplifying things, but somebody could say it's the IT guy's problem. If your company's breached, it could be your job." This makes it important for all company officials, from the highest rung to the lowest, to be aware of a company's security policy and remain obedient to it. "It comes down to how your individuals are being trained," said Day. "Ignorance is no excuse." ●

*Jacob Barron, NACM staff writer, can be reached at [jakeb@nacm.org](mailto:jakeb@nacm.org).*

Want to know more about credit card vendor liabilities? Read Robert Day's article on page 26, and be sure to check out his Credit Congress session. More information on this session can be found on page 53.

*This is reprinted from Business Credit magazine, a publication of the National Association of Credit Management. This article may not be forwarded electronically or reproduced in any way without written permission from the Editor of Business Credit magazine.*