



A Date with the DSS

How Are Level 4 Merchants Progressing With Compliance?

By Lisa Dowling

July 31, 2007. This was the deadline for acquirers of Level 4 retail merchants to submit summaries of their data security plans to Visa USA. Visa is working to bring merchants aboard the Payment Card Industry Data Security Standard (PCI DSS) platform. Acquirers were to e-mail Visa compliance plans containing a timeline of critical events, a risk-profiling strategy, a merchant education strategy, a compliance strategy and compliance reporting. Failure to do so would lead to the “imposition of risk controls.”

Visa USA issued a statement saying that 315 members met the deadline. That topped its estimate of 270 submissions for Level 4 merchants—those businesses processing less than 1 million retail transactions per year or less than 20,000 online.

Other Merchants Slower

However, the company’s figures on PCI compliance show slow progress in getting most other merchants to embrace the PCI DSS. According to its data, 40 percent of Level 1 merchants are presently compliant, up from 35 percent earlier this year. Level 2 merchant compliance increased from 26 percent to 33 percent in July. The data also revealed that 4 percent of the largest merchants, namely Levels 1 and 2, have not contacted Visa to confirm they’re not storing sensitive credit card security codes and PIN numbers. That’s quite alarming and makes one wonder about the effectiveness of guidelines and deadlines. Could it be that most organizations are trying to figure out what PCI DSS is and how it works...and more importantly, how it will impact their business?

According to Chris Mark, president/CEO of The Aegenis Group, the industry is heading in the right direction. Mark, one of the architects of the PCI DSS, helped the card associations define and label Level 4 merchants as high risk when it comes to compliance. His team also recommended that acquirers profile their merchants to assist in compliance issues.

“We’ve talked to a dozen leading acquirers, and they are all working towards developing effective plans,” says Mark. “We’re seeing a trend that is veering away from the more traditional idea of compliance and seeking

wising up and tackling the problem by taking the princess out of the castle, rather than building a big wall around the princess.”

PCI Council

Helping the industry tackle the compliance problem is the PCI Security Standards Council, an independent body providing management of the PCI DSS on a global basis. The PCI Council was formed last year by the major payment card brands—American Express, Visa, MasterCard, Discover and JCB. More than 275 companies involved in the electronic trans-

“Back in the day when you started a business, you needed electricity, insurance, permits. Now, you need security.”

—Bob Russo, general manager, PCI Security Standards Council

to get rid of critical data. While the larger companies are moving forward, smaller ones are still trying to figure out what it all means. For those organizations, as well as those who missed the deadline, there are directions on how to profile merchants in the VBR [Visa Business Review].”

Mark cites another option—an emerging niche market of companies that are offering data security solutions. One such company is Trust Commerce, a gateway that has built a program that can offload data for merchants.

“If there is no data storage, there’s no problem with PCI compliance,” says Mark. “Because of this budding business, our industry may look completely different in a few years. Companies are

action community have joined the PCI Council as participating organizations. General Manager Bob Russo sees great benefit in the PCI DSS standard as well as setting deadlines for compliance.

“Everyone, obviously, wants to be compliant as quickly as possible,” says Russo. “With bad guys getting smarter, the best defense is the standard, and setting deadlines makes sense. Anything that creates forward motion is good for the industry. At the PCI Council, we’re doing lots of educating. We’re constantly being asked what companies need to do and how to get it done. We point them in the right direction. The first step is not to store Track 2 data. That cuts down on the amount you need to worry about.

While it doesn't make you compliant, it will manage your biggest risk, and that lessens the chance of you getting hit by hackers or fines."

Russo's advice for ISOs and acquirers that missed the Visa deadline is to get compliant as soon as possible.

"Take care of your biggest risk now," says Russo. "Back in the day when you started a business, you needed electricity, insurance, permits. Now, you need security. It has to be your No. 1 priority. It is something that can literally put you out of business. The paradigm has changed. A year ago, guys were asking why did they have to do it. Now, they're asking how fast can they get it done."

Heartland Payment Systems boasts 150,000 Level 4 merchants, and all are part of the plan Heartland submitted to Visa—a three-step plan that involves a questionnaire, a vulnerability scan and software that can detect when merchant databases are erroneously storing card numbers. Heartland makes its security plan questionnaire mandatory for all Level 4 merchants. The scan is implemented only when necessary.

"The vulnerability lies in the process, and I don't see a lot of value to Visa's approach," says Bob Carr, president/CEO of Heartland. "The problem isn't with the acquirers. The problem is with the software vendors. They've been manufacturing software for a long time that is not compliant. Instead of having a ridiculous policy of off-loading responsibility to every one of their member banks, why don't the card associations require software writers not to violate their security policy?"

Carr believes some organizations in compliance with the PCI DSS may suffer from the cost of that compliance.

"Companies are evaluating their risk of losing customers to somebody not compliant," says Carr. "We're seeing merchants jump to other acquirers that don't enforce the stricter compliance rules. It's happening in the industry. It has happened to us. It hasn't impacted us significantly, but for small ISOs, it's a different story. And we know who the violators are because Visa publishes a list on their Web site

of which systems are not compliant. What's the disconnect on that?"

Carr predicts the card associations will continue down a path of cosmetic applications.

"I see them working on the cosmetics of the security problem so that people will feel good, but I don't see any serious attempt to solve the problem," he says. "Why not? Because the system is flawed. Having responsibility imposed on acquiring banks doesn't work in the real world. The alternative is to have the card associations hold the software writers accountable for what they do. The methodology in the system is flawed because the software writers are responsible to hundreds of acquirers as opposed to one authority."

Carr says the July 31 deadline would have had more of an impact on the industry if it had been enforced.

"As for the deadline, the trigger hasn't been pulled," says Carr. "There are no realistic sanctions for violators. There's an outline of goals rather than a requirement."

Perhaps the answer lies in new regulations for software. Perhaps the answer lies in a few specialized companies whose focus is solely on data security rather than with thousands of organizations that don't have that focus.

As Mark says, "We would rather have the data with one trusted company than 20,000 who don't have that core business." **TT**

Visa's Guidelines for Level 4 Merchant Compliance

Level 4 Merchant Compliance Plans must include a timeline of critical events, a risk-profiling strategy, a merchant education strategy, a compliance strategy and compliance reporting.

Timeline of Critical Events

Outline target completion dates for the overall strategy. Summarize plans to monitor progress of program execution and provide updates to acquirer Audit and Risk or other appropriate executive management committee.

Risk-Profiling Strategy

Define a process that prioritizes Level 4 merchants into appropriate risk categories or subgroups to focus security efforts on merchants that pose the greatest potential risk.

Merchant Education

Describe plans to educate Level 4 merchants about cardholder data security, storage of prohibited planned communication channels and approximate frequency. Describe the methodology for distributing pertinent Visa communications to merchants.

Compliance Strategy

Apply targeted compliance measures to merchant subgroups based on the following risk-prioritized steps: 1) Eliminate prohibited data; 2) Protect stored data; 3) Secure the environment in accordance with the PCI DSS.

Verify that prohibited cardholder data is not retained after transaction authorization. Identify payment applications used by Level 4 merchants and ensure they are on Visa's List of PABP-Validated Payment Applications. Ensure that merchants don't use a payment application that stores prohibited data. Establish a strategy to ensure that third-party agents used by Level 4 merchants have validated PCI DSS compliance. Ensure merchants with a business need to retain cardholder account numbers protect the data in accordance with PCI DSS.

Compliance Reporting

Monitor progress of program execution monthly. This should include regular reporting to executive management and the board as appropriate.