



## Solving the Level 4 Challenge

*Acquirers can reduce risk by offering merchants education, outreach, and support*

By Joan E. Herbig

**A**lthough PCI compliance among Level 1 and Level 2 merchants has garnered much industry attention, savvy acquirers instead are focusing their attention on Level 4 merchants. Keeping these customers compliant—and secure—is the key to mitigating risk.

The 6 million Level 4 merchants in North America alone pose a significant risk for their acquirers. Defined by Visa as those with less than one million total transactions (or less than 20,000 e-commerce transactions) each year, these merchants represent 85 percent of reported data compromises, and their PCI compliance rates are in the single digits.

Engaging small merchants on security issues, however, is challenging because most are focused on daily business, and few have adequate resources to make compliance a priority. Therefore, it's up to acquirers (banks and ISOs) to educate them and drive the compliance initiative.

### Initial Steps

Even in the best circumstances, few small merchants understand what to do to achieve compliance or who they can trust to help them. Acquirers can help eliminate much of this confusion by implementing a PCI program that includes merchant education, outreach, and support.

All Level 4 merchants are required to complete the PCI DSS self-assessment questionnaire (SAQ) on an annual basis. Some, primarily those that store card data, also must have quarterly vulnerability scans that must be certified by a PCI approved scanning vendor (ASV). Unlike Level 1 merchants, Level 4 merchants are not required to undergo an external audit to confirm their compliance with the PCI DSS; but they must attest to the accuracy of their answers themselves.

To ensure small merchants meet PCI DSS, acquirers must devise a compliance plan that includes a timeline of critical events, strategies for risk profiling, merchant education, and compliance, as well

as some kind of reporting mechanism. For best results, acquirers should consider:

- the merchants most at risk
- the number of merchants that require scanning compared with those that simply need to complete the SAQ
- their relationship to their merchants
- their current merchant attrition rate and how it will be affected by a PCI program
- their communication vehicles, frequency, and response level from merchants
- their response to a breach
- portfolio value and how a 70 percent or more compliance level will affect it.

Although acquirers pass on any fines associated with data compromises to the merchants, they are ultimately responsible for payment. To maximize compliance rates, they should segment their small-merchant portfolios based on risk level and then create specific plans accordingly.

A consistent education program that effectively conveys the risks of non-compliance also will encourage Level 4 merchants to engage in the process. Acquirers should take advantage of the improved information currently offered by the PCI Council and some of the card brands and consider using Webinars and podcasts to deliver their message. These programs should provide merchants with tips to secure their businesses, such as not storing credit card data, which simplifies compliance requirements and reduces risk. They also should encourage merchants to upgrade to PA DSS compliant applications as well as offer them tools for determining their PCI merchant type and requirements for quarterly scans.

### Support and Monitoring

Because small merchants tend to be hard to reach, acquirers should use the same agents or other channels they normally use to reach their end merchants to get their compliance messages across. If acquirers work directly with their merchants, but don't frequently communicate with them, they should increase their contact.

The merchant type also can affect how the compliance message is conveyed. Many retail brick-and-mortar merchants don't have computers, let alone e-mail addresses, so acquirers may need to use regular mailings and phone calls to reach them. Most acquirers will need to test multiple vehicles to reach their merchants, including Webcasts, statement inserts, e-mails, and call and mail campaigns.

They also need to educate sales people and give them the proper tools to support merchants and guide them through the process. This is a great opportunity to help develop and solidify their roles as trusted advisors to their merchants.

Once plans are in place, a consolidated compliance reporting plan helps acquirers ensure their efforts are working and monitors their ongoing risk. Statistics generated in the reviewing process must be reviewed at least quarterly so that adjustments can be made.

Deciding whether the process takes place in-house or is outsourced should be dictated by the amount of resources available, especially for outreach and support. If, after the recommended due diligence, an acquirer decides it cannot sustain an ongoing PCI compliance program and still manage its day-to-day business, it should consider outsourcing the process to a reputable PCI compliance solutions provider. Acquirers should pick a provider that not only is experienced in all aspects of the compliance process but also demonstrates success in working specifically with Level 4 merchants.

Acquirers need to be realistic about the efforts required and go through the necessary due diligence process to determine the best method to achieve higher PCI compliance rates for their Level 4 portfolios. Not only will they reduce their risk, they will build a more valuable portfolio for the long term. **TT**

*Joan E. Herbig is CEO of ControlScan in Atlanta.*