

Data Security Top Concern for Merchants

Yet First Data Survey Finds Many Merchants Unaware of Consequences, Solutions

First Data recently conducted a survey asking merchants about data security. Not surprisingly, it is a universally important issue: More than 80% of small and mid-size merchants described themselves “very concerned” about payment card security. But these merchants’ experiences with data violations differ vastly, as does their understanding of the consequences of a breach.

Concern and Experience with Breaches

Of the small merchants, 42% of respondents said they have never been exposed to a security breach. In contrast, 17% of mid-size merchants relayed that they have never been exposed to a breach.

Cost of a Breach

The First Data survey also revealed that larger merchants tend to have a better understanding of the consequences of a breach than many small and mid-size retailers have. The latter group is less aware of the tangible and intangible costs, including their own liability for data breaches. Almost one-third (31%) of small and mid-size businesses indicated they did not know their liability in case of a data breach prior to the survey. And almost one in five respondents in that same group didn’t believe that they are liable for a data breach.

This shaky foundation of knowledge could be disastrous to merchants. The Ponemon Institute cites the potential costs of a breach to be around \$200 per compromised record or card. Using that number and 5,000 compromised records as an example, the cost of even a small breach could be astronomical: \$1 million. And that doesn’t include the infinitely unquantifiable costs of reputation damage and loss of customer loyalty.

PCI Compliance Doesn’t Equal Security

Compliance with the Payment Card Industry Data Security Standards, PCI DSS, is the single most recognized component of a data security program and often (incorrectly) considered the only necessary step to keeping data secure. Yet, even PCI compliance is frequently misunderstood and only haphazardly carried out.

More than 60% of mid-size merchants surveyed by First Data had completed the annual PCI self-assessment, and 72% described themselves as “highly familiar with PCI standards”. Only 23% of small retailers had completed the self-assessment, while 40% disclosed that they had not. More than one-third of this group was not sure if their businesses had completed the yearly PCI self-assessment.

The PCI DSS standards are considered to be a worldwide set of best practices for securing sensitive data—but they are not without their limitations. Even those mid-size and small merchants who *did* complete the annual PCI self assessment audit were not adequately educated about data security issues. There is much more to data security than just PCI compliance, as evidenced by the continued growth of breaches among PCI-compliant merchants.

Data Security in the News

- First Data announced the expansion of a merchant pilot of the First Data® TransArmorSM solution. More than 400 U.S. merchants of all sizes will assess the comprehensive data security solution over the next four months.
- Fifth Third Bank, PNC Financial Services and national retailer Hancock Fabrics each confirmed security breaches that put a number of their respective customers at risk.
- The 19th annual RSA® Conference, the world’s leading information security conference and exposition, was held in San Francisco. Major information security themes were addressed by respected experts including Secretary Janet Napolitano of the U.S. Department of Homeland Security and Federal Bureau of Investigation (FBI) Director Robert S. Mueller.

Taking Steps to Data Security

While many merchants are perilously unaware of essential elements of the problem, such as the breadth of the consequences and choice of potential solutions, most realize the overall criticality of keeping payment card data safe. Two-thirds of mid-size merchants and slightly more than half (53%) of small merchants indicated they would be “very likely” to implement a transaction security tool in the next 12 months—a solution that includes a blend of data tokenization and encryption.

What do the businesses find appealing about such a solution? Mid-size merchants value the reduced risk that the combination of tokenization and encryption offers their business while small merchants compare the cost of a breach with the cost of the product.

The Integrated Solution

Until now, a realistic and holistic solution hasn’t been much more than a pipe dream. But First Data® TransArmorSM, our secure transaction management solution, has changed that. First Data will help merchants of all sizes proactively address the vulnerabilities they face when capturing, processing and potentially storing consumer payment card data. TransArmor is an easy-to-implement service-based solution that protects merchants and consumers by encrypting sensitive customer payment card data in transit and—through tokenization—ultimately removing the need to store that data at the merchant level.

For more information about the new solution provided by the partnership between First Data and RSA, please contact your sales representative or visit firstdata.com.

Still More News

→ Albert Gonzalez was sentenced to two concurrent 20 year sentences for his role in the 2008 Heartland Payment Systems and the 2006 TJX breach. (TJX asserts that the breach has cost them \$171.5 million so far, and the Heartland breach impacted an estimated 130 million credit/debit cards—the largest such incident ever reported.) (http://www.bankinfosecurity.com/articles.php?art_id=2344)

→ Dave & Buster’s, Inc. settled Federal Trade Commission charges that they didn’t appropriately secure consumers’ credit and debit card information. The breach resulted in unauthorized access to about 130,000 credit/debit cards and several hundred thousand dollars in fraudulent charges. (<http://www.databreaches.net/?p=10847>)

And, while D&B’s didn’t publicly announce their legal expenses, the Ponemon Institute reports that all businesses are spending more on legal defense costs due to a growing fear of successful legal retribution resulting from loss of sensitive data.

→ March 7-13 was National Consumer Protection Week, with a focus on kids and financial education. As President Obama put it in his March 5 Presidential Proclamation, this education is needed to “help our children grow into financially responsible adults and avoid frauds and scams” (<http://www.whitehouse.gov/the-press-office/presidential-proclamation-national-consumer-protection-week>). More than 15 partner organizations (from the AARP to the USPS) provided free resources to help people of all ages learn to protect their privacy, avoid identity theft, and steer clear of frauds and scams among other topics.