

AMERICAN BANKER®

THE FINANCIAL SERVICES DAILY

Friday, June 26, 2009

VIEWPOINTS

PCI Standard Still the Best Answer to Fraud

■ BY ELLEN RICHEY

With high-profile breaches in the news, some have questioned the Payment Card Industry's data security standard, or PCI, and publicly wondered whether it remains effective.

From Visa's perspective, the answer is an emphatic "yes."

What keeps us believers? Simply this: Despite all the talk about compliant entities being breached, the truth is that no compromised entity to date has been found to have been compliant with the standard at the time of the breach. In all cases, forensic investigations have concluded that significant compliance deficiencies were major contributors to the breach.

Put another way, in every case specific elements of the security standard would have addressed the vulnerabilities attacked.

A great deal of confusion has emerged on this point, so it is fundamentally important to understand what the security standard is and is not. It is a program of basic security safeguards that — if fully adopted and maintained — protect a company from hackers and let it detect intrusions quickly with minimal harm done. But the standard is not a "silver bullet." In complex processing environments, it is only the starting point for a comprehensive security defense.

Most importantly, PCI validation is not the same as PCI compliance. Annual validation is important, but ongoing vigilance is essential. Real compliance means a commitment to following the standard and keeping consumer data safe — 24 hours a day, 365 days a year.

It is natural to focus on data compromises that make headlines, but we should also

remember that these events are the exception, not the rule. More than 90% of the largest card accepting merchants and about 97% of processors in the United States have validated compliance with PCI. The companies that fully embrace it are protecting themselves every day by maintaining their defenses, scanning systems, detecting anomalies and addressing threats.

Our financial institutions, merchants and processors deserve praise for dedicating resources to install robust data security programs, starting with PCI. We do not hear about their everyday successes in the news, but we can see them in our results. Thanks to massive investments and innovative solutions by the payments industry, fraud rates remain near their all-time lows — and cardholders are protected from the fraud that does occur under our highly successful "zero liability" policies.

The naysayers who question the standard, the assessment process and the PCI Security Standards Council are missing this larger picture. Despite what the critics say, PCI remains an effective and necessary tool to protect cardholder data and should remain a key part of our industry's collective efforts.

As the headlines show, criminals have become adept at exploiting security gaps and lapses in risk controls. They seek to intrude into systems, install malicious software, gain access to sensitive data and remove it undetected so that they can commit fraud. However, companies that follow good security practices, including the PCI standard, have the opportunity to thwart the criminals every step of the way. We can minimize our storage of sensitive cardholder information. We can secure our

systems with firewalls and access controls. We can run programs to detect intruders and root out malware. And we can likewise scan the system to catch the criminals on their way out.

But we must always keep in mind that the standard was never intended to be the sole means of safeguarding data within the payment system. The standard is just one part of a multilayered approach that operates on many levels.

Even in today's economic downturn, the payments industry continues to invest in security technology solutions. Additional layers are evolving in encryption, authentication, monitoring tools and information sharing — all of which can be used in conjunction with the PCI standard. For its part, Visa is investing in innovative solutions within all these layers.

On the encryption front, for example, we get encrypted data today from the business community and stand ready to support those companies willing to implement the robust key management that this requires.

The reality is that the fight against data thieves is a complex and multidimensional task. No single solution will make fraud go away. As criminals get better at what they do, our efforts to stop them must keep pace. Payment system participants should — and we will — continue to explore additional tools to safeguard data and prevent fraud. While these additional solutions are being evaluated, we must not abandon the tools we have available today. And foremost among these is PCI. Simply stated, PCI is the strongest industry standard in existence, and it is still the best defense against criminal attacks.

Ellen Richey is the chief risk officer of Visa Inc.