INTELLECTUAL PROPERTY ARTICLE

ROBINSON BRADSHAW & HINSON

SEPTEMBER 2007

Merchants Face New Credit Card Security Standards

By John M. Conley and Robert M. Bryan

The rapidly growing problem of ID theft has created a dilemma for banks that issue credit cards. The typical credit card users have become accustomed to being protected from the risk that their cards will be improperly used by third parties. But absorbing the costs of improper use has become a burden for banks. One proposed solution to this problem is the adoption of broadly applicable security standards that may decrease the magnitude of the losses, together with the shift of a significant portion of the remaining cost of ID theft to those merchants that fail to implement the required security procedures.

Credit card security standards are not a new development for merchants. An earlier set of standards was promulgated several years ago by a consortium of financial institutions that were members of various credit card associations. But the standards were not rigorous and were not strictly enforced. That is changing.

As of the beginning of 2007, merchants are subject to new and stringent security standards. The new version of Payment Card Industry Data Security Standard (PCI DSS) was promulgated by a consortium that includes American Express, Discover, MasterCard, VISA, and JCB. Each of the card brands has modified its own security policies to conform to PCI DSS. The consortium is trying to assure consistency in enforcement by subjecting non-compliant member banks to fines. Merchants and service providers are subject to restrictions, up to and including denial of access, and some observers expect member banks to use contractual provisions to require merchants to reimburse them for fines they incur as a result of merchant non-compliance and, possibly, for the costs of holding card holders harmless from fraudulent use of their cards.

The PCI DSS consists of six overarching principles, or "control objectives," which are then implemented by a dozen more detailed "requirements." While the objectives seem to be matters of common sense, the requirements are highly onerous, especially for smaller retailers. The six objectives are: Build and Maintain a Secure Network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, and Maintain an Information Security Policy.

A sampling of the requirements shows just how difficult compliance may be. Under the heading of Build and Maintain a Secure Network, for example, is the requirement to establish a firewall configuration that meets 19 specific standards. To meet the Protect Cardholder Data objective, the merchant must meet 22 separate sub-requirements pertaining to stored cardholder data, and 3 more concerning the encryption of data transmitted across open networks (including the Internet and WiFi). In order to Maintain a Vulnerability Management Program, there is a requirement to "develop and maintain secure systems and applications." This sounds straightforward enough, until you start reading the 27 separate practices that are required. The merchant must not only "ensure that all system components and software have the latest vendor-supplied security patches installed," but is responsible for the "testing of all security patches and system and software configuration changes before deployment" -- in "separate development, test, and production environments."

The last objective -- Maintain an Information Security Policy -- sounds the simplest, but it may be the most onerous of all. Its first requirement is to "establish, publish, maintain, and disseminate a security policy that," among other things, "addresses *all requirements*" of the PCI DSS. Included in the 42 other specific duties under the policy heading are a "formal" annual risk assessment; a separate annual review of the whole policy and "updates when the environment changes;" a "security awareness program," directed at employees, together with written employee acknowledgement that they understand the policy and procedures; contracts with service providers committing them to PCI DSS; and an "incident response plan" that is tested annually. The import of this final objective is that a merchant must not only comply with every element of PCI DSS, but it must make compliance a part of a formal, enforced, and verified company policy.

PCI DSS does offer one alternative that may be useful for smaller merchants that would find compliance with the detailed requirements a costly burden. A merchant has the option of using "compensating controls" when it cannot meet a particular technical specification of a requirement but has sufficiently mitigated the associated risk. The example given deals with alternative controls when a merchant is unable to render cardholder data unreadable, as by encryption. While this alternative may seem attractive, there is a price to pay for using this approach. The concept of "compensating controls" is vague and there is no guarantee that any particular alternative will be viewed as adequate, so a merchant relying on "compensating controls" would lose the safe harbor protection of full compliance.

Guidelines promulgated by the various credit card brands reveal how they interpret the duties imposed by PCI DSS. VISA, for example, has folded the PCI DSS standards into the Cardholder Information Security (CISP) program that it mandates for its bank members, merchants, and service providers. But CISP imposes a level of "validation" above and beyond the PCI DSS requirements: "Separate and distinct from the mandate to comply with the PCI Data Security Standard is the validation of compliance whereby entities verify and demonstrate their compliance status." The specific validation requirements depend on the nature and size of the entity. Merchants, for example, are classified into levels 1 (6,000,000 VISA transactions per year or previous account data compromise), 2 (1,000,000-6,000,000 transactions), 3 (20,000-1,000,000 transactions), and 4 (fewer than 20,000 transactions). Level 1 merchants must have an "annual on-site PCI Data Security Assessment" by a "qualified security assessor" or an internal audit *if signed by an officer of the company*; lower-level merchants may combine annual self-assessment with quarterly network scans by an approved scanning vendor. In cases of non-compliance, VISA threatens fines against member banks and restrictions on merchants.

Although the new version of PCI DSS is barely half a year old, it is already possible to identify some significant practical issues and risks for merchants. First, the requirements are highly technical and compliance will not be easy. Some companies will have to use third-party vendors to comply. If a company does have internal IT specialists, they must be involved at every stage of compliance, from deciding what must be done to verifying that it has been done.

Second, the written policy requirement is not an afterthought and the adoption of an ambiguous and incomplete policy may have significant legal implications. Some commentators have speculated that the FTC may view these policies as being similar to privacy policies and treat the failure to comply with the policy as an unfair and deceptive trade practice.

Finally, because PCI DSS is a clear effort to define an industry-wide "best practices" standard, it is likely to be viewed by courts as the standard of reasonable care in a negligence suit brought by an identity theft victim. Many experts believe such claims will become more common in the future.
