

Beating the high-risk numbers game

WHENEVER A CONSUMER enters their credit card number on an online check-out form or slides the card in a point-of-purchase terminal, that number becomes not only a source of funds for the merchant but also a potential headache. Because of the Payment Card Industry Data Security Standard (PCI DSS, or PCI) rules, as well as privacy statutes enacted in 32 U.S. states to date, merchants must be able to protect that highly sensitive piece of data and store it securely – or face significant consequences.

Aside from the legal ramifications, payment card data is the leading target of fraud (accounting for \$22 billion in

2008, up from \$19 billion in 2007), so it is a major area of concern for businesses and consumers alike. Currently, there are a few approaches that merchants can take to protect this data. One is to encrypt the credit card numbers, which, while effective, has drawbacks. For one, it requires changes be made to all affected applications, since to ensure PCI compliance, every downstream application that touches such information would have to be modified to enable encryption. In addition, it requires that the encryption keys be securely managed so that the numbers can be decrypted for later, legitimate purposes.

Other methods typically used to protect credit card numbers include masking (e.g., xxxx-xxxx-xxxx-5608), which provides just enough information to confirm that the correct card was used without revealing the full number to an outsider's eyes, and hashing, which is a form of "one-way" encryption that is useful when storing numbers in a data warehouse. In both cases, however, the original card number cannot later be recreated when needed.

COMING TO THE RESCUE

An emerging solution known as tokenization (see box) solves these issues and more. Tokenization makes it impossible for hackers to ascertain and steal the original

credit card number and not only facilitates PCI compliance but also reduces the cost and scope of compliance efforts. Here's how it works.

When sensitive data such as a credit card number is input to an application or POS terminal, the tokenization server substitutes a randomly generated, cryptographically strong numeric value that preserves the format and look and feel of the original data structure but has no actual cryptographic or mathematical relationship to it. This means it cannot be "decoded" by a hacker. Furthermore, since there's no relation between the tokenized value and the actual number, downstream applications that receive and process it are not subject to PCI audit. Applications can simply allow the tokenized data to flow through, without the need for additional code or database schema changes.

The original, clear-text card number that corresponds to the tokenized value, meanwhile, is centrally stored and encrypted so it can be retrieved by authorized administrators and applications when needed. For maximum protection, the encryption keys are also stored and managed centrally, and the tokenized

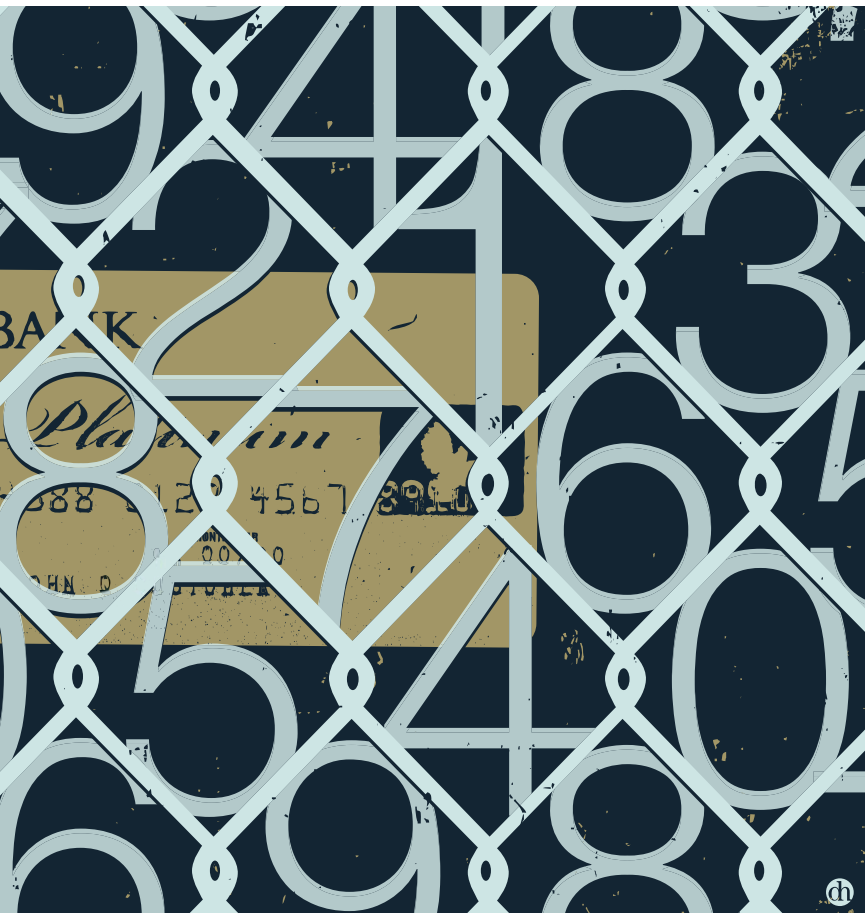
FIRST DATA AND RSA: PARTNERS IN PRIME

In September 2009, RSA and First Data, a global leader in electronic commerce and payment processing services, announced that they are partnering to develop First Data Secure Transaction Management, a tokenization-based service designed to reduce organizational risk and ease the process of complying with PCI DSS.

First Data Secure is powered by the RSA SafeProxy™ architecture, which employs a unique combination of tokenization, advanced encryption, and public-key technologies to provide merchants with the ability to eliminate credit card data from their environments without loss of business functionality or massive rewrites of applications.

According to Art Coviello, executive vice president of EMC Corporation and president of RSA, The Security Division of EMC, "This fruit of our partnership with First Data will provide organizations with a simplified and scalable solution for payment card protection that drastically reduces management complexity and costs. We look forward to a continuing and mutually rewarding collaboration."





value itself can be generated automatically at the moment the credit card number is transmitted.

A FIRST-CLASS SOLUTION

For credit card-processing company First Data, tokenization promises to protect its own interests as well as those of its merchant customers and their customers. With First Data® Secure Transaction ManagementSM, a service First Data will begin offering its customers thanks to a partnership with RSA (see sidebar), merchants will send their payment card numbers and other information to First Data for card authentication just as they do currently. But now, customers will receive back a tokenized value that can then be used in online applications instead of having to use actual card numbers. First Data will maintain the real payment card information in a highly secure data store from which it can be retrieved for payment processing once a

transaction is complete.

“Payment card data protection and PCI compliance are some of the most significant challenges that our merchant customers face today. Addressing these challenges is both complex and costly,” says Michael Capellas, chairman and chief executive officer of First Data. “The simplicity of integrating encryption with tokenization through the First Data Secure Transaction Management service dramatically redefines how merchants of all kinds manage and protect their customer payment data.” Merchants will benefit from First Data Secure Transaction Management because they will no longer have to process and store actual card numbers onsite, thereby greatly reducing their risk profile and the scope of PCI compliance efforts. They can also pass on assurances to their customers that their data is secure from hackers and identity thieves. The solution supports all types of payment card data.

Because tokenized data cannot be reverted to the original number without accessing a secure vault within First Data’s secure data center environment – and cannot be used to initiate a transaction at the point of sale – it is essentially worthless to criminals. Tokenized data can, however, be used safely and effectively by merchants in a range of important business capabilities, such as tracking customer loyalty, managing refunds and returns, and supporting customer analytics.

COMPLIANCE FOR BUSINESSES, CONFIDENCE FOR CONSUMERS

“No organization wants to be the lead in the next national news story about a company that had a data breach and allowed sensitive customer information to be accessed by hackers or insiders,” says Robert Griffin, director of solution design for the Data Security Group at RSA, The Security Division of EMC. “Tokenization is an ideal solution for these organizations because the cost, time, and impact of deployment are small relative to other solutions, yet it can also be more effective. Furthermore, it’s capable of supporting multiple data types and eliminates cross-platform complexities often introduced by encryption-based methods.”

In addition to PCI and the state privacy laws, tokenization can also help organizations comply with other regulations, such as those mandating security of Personally Identifiable Information (PII) and health information, where clear-text storage of sensitive information is prohibited.

Tokenization is a powerful new solution to achieve compliance, protect consumers, and thwart thieves. As such, it can be a valuable component of a comprehensive defense-in-depth system for data security. Supported by identity and access management, security information and event management, and enterprise key management, tokenization can ultimately make the numbers work in your favor. ■



TOKENIZATION VS. TOKENS Though the term “aliasing” is also sometimes used, “tokenization” has become the most common term for the substitution of sensitive data with a random numeric value. Though the terms are similar, tokenization in this sense is different from RSA SecurID tokens, which employ randomly generated numbers for strong authentication. RSA follows industry practice in using the term tokenization, while acknowledging the need to distinguish between tokenization and SecurID tokens, given the latter’s widespread success and deployment. The price of success!