

AMERICAN BANKER®

THE FINANCIAL SERVICES DAILY

Tuesday, September 22, 2009

COVER STORY

First Data's Second Layer of Security

■ BY DANIEL WOLFE

First Data Corp. is developing a security format that could assuage merchants' concerns about encrypting card data at the point of sale.

The Atlanta payment processor is expected to announce today that it is developing a system that uses tokenization, a technique that will make encrypted data more secure.

First Data's move is notable because "it puts this technology on the map," said Avivah Litan, a vice president and distinguished analyst at Gartner Inc. "It makes it more mainstream and accessible," and could sway some of First Data's merchant customers that were on the fence about using encryption.

Merchants "are just fed up on spending money on card security," Litan said.

By removing card data from merchants' systems, encryption and tokenization "reduces the compliance expenses," she said.

Indeed, a string of major data breaches have raised questions about how the Payment Card Industry data security standard is enforced, and both encryption and tokenization go beyond the PCI standard.

Under PCI, merchants send unencrypted card details to processors, but critics have said the data is vulnerable to hackers during this stage.

Michael Capellas, First Data's chairman and chief executive, said encryption and tokenization would address this issue by replacing the card details with gibberish that would be useless to criminals.

"More fundamentally, the data



Presto: Card data "doesn't exist" after this process, Capellas says.

doesn't exist" once it has been through this process, Capellas said in an interview Monday.

The processor is working with EMC Corp.'s RSA Security on what First Data is calling Secure Transaction Management.

Capellas said First Data plans to begin testing the new system in January and expects to have it ready for use by the end of the first quarter.

Under the format, merchants would encrypt the data from customers' cards as they are swiped at the payment terminal and pass it to First Data.

The tokenization system then creates a string of digits that resembles a credit card number, the last four of which match those of the card account used for the transaction.

This number, the token, functions as a

reference code for the encrypted account data. If merchants later need details of the transaction, for example to resolve a customer dispute, they no longer would need either the customer's account number or an encrypted version of it. Instead, they would use the token to identify the needed card data on file at First Data. In effect, tokenization adds a second layer of security, above encryption.

Litan said that if a merchant encrypts locally, that data is still vulnerable whenever the data must be accessed.

But if a merchant goes with a processor's encryption system, the merchant could lose some data-access flexibility and must accept the possibility of being locked in to a single provider's encryption scheme, she said.

Capellas said First Data is giving merchants a heads-up that the system is currently in development in the hopes of making them more willing to invest in encryption gear now.

The current PCI standard does not require encryption, though Visa Inc. and other companies involved in enforcing it have said that using the technology might help merchants meet many of the requirements.

And though some merchants have expressed interest in adopting encryption, analysts said that the lack of any formal guidance within the PCI standard has discouraged some who have feared they would invest in a system that might not comply with future changes to the security policy.

Merchants want to do everything they can to protect card data, but many of them

are wary about where they invest because “PCI compliance in itself is an extremely expensive, complex process,” Capellas said.

He said Secure Transaction Management would address this concern by supporting any payment terminals that already have encryption capabilities when it is introduced. “You don’t have to throw your entire investment away,” Capellas said.

First Data has not yet determined what it will charge for the system.

First Data is not the first processor to go this route — just the biggest. In August its smaller rival Electronic Payment Exchange in Wilmington, Del.,

unveiled BuyerWall, a system that adds tokenization to encrypted card data. The company has said combining the two methods is one of the most effective approaches to security available.

First Data Effort Seen as Boost for Card Encryption

Other processors are sticking with encryption systems.

Heartland Payment Systems Inc. has been one of the most vocal advocates of encryption, after announcing in

January that it had discovered a significant breach in its systems.

Heartland was already developing an encryption system, and subsequently fast-tracked the project.

The terminal-maker VeriFone Holdings Inc. already offers a system with encryption capabilities. Neither of these processors have announced plans to move to tokenization.

First Data, a unit of the private-equity firm Kohlberg Kravis Roberts & Co., is using RSA’s SafeProxy technology to handle the tokenization and other security management aspects of its system. ■

