

AMERICAN BANKER[®]

THE FINANCIAL SERVICES DAILY

Monday, March 23, 2009

COVER STORY

Iron-Particle 'Fingerprint' Could Thwart Data Thefts

■ BY DANIEL WOLFE

WASHINGTON — Tiny iron particles may be the next item in the banking industry's antifraud toolkit.

Visa Inc. and Fifth Third Bancorp are testing a system that evaluates the physical properties of the iron in the magnetic stripes on payment cards. The companies say these characteristics are different for every card and can function as a financial "fingerprint" that could prevent stolen account data from being used to produce fake cards.

"The right long-term goal is to make data unusable to criminals and therefore reduce the incentive to steal it," Ellen Richey, Visa's chief enterprise risk officer, said at Visa's Security Summit here last week.

Don Roeber, the vice president of merchant compliance at Fifth Third Processing Solutions, said his company has installed about 1,000 card readers that have the components needed to evaluate the iron particles in magnetic stripes. He described the technology as invisible to the merchant and said the readers are delivered during merchants' normal upgrade cycles.

Though criminals have devised many ways to steal the account data stored on cards, the physical properties of the original card's stripe would not be duplicated if a criminal tried to copy stolen data onto a new card, Visa said.

During transactions, terminals verify that the stripes are affiliated with the account number and then generate a one-time code to authenticate the transaction.

Because so much stolen card data is



Richey: Visa's goal is "to make data unusable to criminals."

available, Roeber said it is important that banks "figure out a way to make that data of no value to the criminal."

The test is being done at several merchants, which Fifth Third would not specify. It began in February 2008 and is expected to run through June.

The technology was developed by MagTek Inc., and uses terminals from VeriFone Holdings Inc.

Andy Deignan, MagTek's vice president of global marketing and strategy, said in an interview Friday that the technology can work with any mag-stripe card.

"The stripe itself is made up of tiny particles of ferrous oxide — iron — and those particles are randomly sized and distributed throughout" it, he said.

"Because each stripe is unique and

because they are magnetic in nature, each stripe gives off a low-level noise that is unique to the card, it is repeatable within the card, and it is verifiable within the card," he said. "We use those properties to authenticate the card."

Once the reader authenticates the card, it generates a 54-byte string of data to authorize the transaction. This code changes with every transaction, and can be correlated to the fingerprint associated with the card. The system also considers the age and degradation of the stripe when comparing them to reference fingerprints that are generally kept by issuers.

Avivah Litan, a vice president and research director at the market research company Gartner Inc., said the system "sounds like a very robust method for card authentication, which is what the challenge is all about; it's all about making sure the criminals are not able to use stolen data."

She cautioned that no security method is perfect and, since the technology is not widely used, it is hard to properly gauge its effectiveness. "If it works as advertised, I think it's a great idea."

Financial companies are also considering other ways to make stolen data less useful. Heartland Payment Systems Inc., for example, in January, shortly after announcing that its systems had been compromised, called for encrypting card data as soon as a card is swiped. It said that end-to-end encryption would have rendered useless the data stolen during the security breach.

Roeber said that this encryption strategy is impractical. “If you have a larger merchant that has a thousand stores,” he said, “that can be a significant challenge for them to manage all those keys.”

With the mag-stripe fingerprinting system, “there’s no key management to work with here,” Roeber said. “There’s not a whole lot of implementation issues.”

Visa also announced at the conference that as of last week 90% of the U.S. merchants it classifies as Level 1 and Level 2 have validated their compliance with the Payment Card Industry Data Security Standard and 99% have stopped storing prohibited card data.

Gerry Sweeney, Visa’s global head of e-commerce and authentication product

innovation and development, said that while compliance is up, “we must move from static data to dynamic data for authenticating consumers and cards.”

Though dynamic data is used today in contactless and other chip cards, it can be used without any change to the card. “We’re doing a lot more at the terminal level,” he said. ■

MAGTEK®

MagTek® Inc., 1710 Apollo Court, Seal Beach, CA 90740 | p 562-546-6400 | f 562-546-6301 | 800-788-6835 |
www.magtek.com Registered to ISO 9001:2000 PN99800083 Rev 1.0 4/09