

TRANSACTION

trends

M & A

Break Down

**Recession leaves investors
and sellers searching for
ways to connect**

ALSO INSIDE:

**Strategies for Picking
a Processor**

**ETA Annual Meeting
& Expo Coverage**



Transaction Security, Evolved

Authentication makes transactions as easy as they once were and safer than they are now

By Mimi Hart

For a payment system to be effective, merchants and consumers must find it convenient and easy to use. But as fraud becomes more sophisticated, inspiring confidence without overly complex processes becomes a greater challenge. Authentication may provide the answer.

Industry professionals who worked with POS transactions in the early 1980s can remember the paper “Warning Bulletins” bankcard associations mailed bi-weekly to merchants. When a customer presented a bankcard, the merchant would look through the bulletins to ensure the card wasn’t listed as lost or stolen. If it was, the merchant was supposed to take the card, cut it in half, and send it to their bank for a reward.

As POS transaction processing evolved in the 1980s, it became faster, easier, and more cost-effective to install online authorization and settlement systems. Inexpensive POS devices were used to authorize and electronically deposit receipts for merchants who received lower discount fees as interchange fraud decreased.

Now in 2009, we continue to find significant challenges with the current POS infrastructure, which presents a major burden for retailers, processors, gateways, ISOs, and others involved in the industry. Large retailers and processors seem to be getting compromised on a regular basis, even though they follow the rules and regulations put into place by PCI.

Multiple points of compromise

Today’s criminals have skills, tools, bravado, and a level of innovation that is maddeningly daunting. Just a few years ago, massive breaches were unheard of. Although thieves could rewrite the magnetic stripe to alter account numbers and expiration dates, then melt down and re-emboss the cardholder information, the introduction of CVV and CVC soon prevented this swindle.



Unfortunately, the industry has added few other security measures since then to thwart the use of tampered, cloned, or counterfeit cards. Recently, the PCI DSS mandated cardholder data be protected, but only in a few places, namely when the data is “at rest.” This was a logical first step since thieves are attracted to large repositories of data “at rest” because the effort provides the likelihood of greater reward and a lesser chance of apprehension.

With the recent data breaches of organizations audited by PCI QSAs, it is likely that PCI will soon require the protection of cardholder data in other areas as well, namely data “in transit.” As a result, merchants will invest in POS devices that encrypt cardholder data at the point of swipe. This will add expense to merchants’ POS systems, but offer savings in the compliance process and add an effective layer of security that consumers may value. It will definitely make theft of cardholder data from within the payment processing network more difficult, but encryption at the POS will not stop fraud.

While encryption will be a valuable tool for the industry, it won’t deter the more enterprising fraudsters because cardholder data can still be obtained in other places. The most well-known techniques

for doing so are via pocket skimmers, tampered rogue POS terminals, fake ATMs, Internet phishing sites, front-end skimmers on legitimate kiosks and ATMs, altered gas pumps, and “card cleaning” swipe stations. Even data encrypted at point of swipe is still vulnerable if it is decrypted at any point before reaching the authorizing party. But the problem is larger still.

Considering 10 billion payment cards are in use, it is safe to say that at least 10 billion possible points of compromise exist. Many industry professionals mistakenly believed that cardholder data on the magnetic stripe is encrypted, and hence secure. The cardholder data is encoded, but it is not encrypted. Perhaps because the word “encode” is often used as a synonym for “encrypt,” it is often presumed the magnetic encoding is secure. The truth, however, is that cardholder data recorded on the mag-stripe contains only zeros and ones, which can be read by anyone familiar with binary code.

Multiple authentication methods

Access to cardholder databases allows criminals to create counterfeit cards that can be used for fraudulent transactions at ATMs or the point of sale. These cards

are virtually undetectable because the current payment infrastructure does not require authentication of the device cardholders use to identify their accounts. If issuers or stand-in processors were in a position to authenticate the physical card itself, not just the data carried thereon, data breaches would all but disappear.

Card authentication allows the issuer, acquirer, or another authorized party to affirm the physical card is genuine and has not been cloned or altered. A strong authentication method also introduces an element of disorder because the authentication data itself changes with each swipe, yet can be reliably verified during each use. When this dynamic authentication value generated at the point of swipe is used, the actual cardholder data, by itself, becomes useless.

The use of physical card authentication renders stored cardholder data worthless to criminals. To perpetrate fraud, they must reproduce an identical copy of the physical token on which to place the stolen data. A strong card authentication method would make this task practically impossible. A substitute card could not be used at ATMs or POS

devices without raising a giant red flag.

In addition, security techniques, such as challenge-response “mutual authentication” of the card reader/terminal and the host, can further prevent data theft. When implemented properly, the reader will not turn on until it has been authenticated with a legitimate host. Therefore, the cardholder data from the swipe is never captured or broadcast anonymously “into the cloud.” Moreover, a password or PIN combined with a nonclonable unique card can further verify the cardholder via strong, two-factor authentication, while a MAC or digital signature can be used to confirm the transaction details have not been altered en route to authorization or later. Combined, these additional security measures can ensure authenticity of the card, the card data, the cardholder, the host, the card reader terminal, and the data message itself.

Getting the industry on board

The real challenge for the payment card industry is getting merchants and consumers to recognize transaction authentication as the true “end-game” in payment security. If the public is to have the same level of confidence in plastic cash

as it has in paper currency, then similar machine-readable, anti-counterfeit measures are required for the card and the other system components.

The payment system must be able to validate the card itself, the encoded data, the reader, the cardholder, the data recipient, and the details of the transaction. (These same security elements are necessary whether the payment mechanism is a card, a fob, a wristwatch, cell phone, a sticker, or a yet-to-be-invented device.) When we know with a high degree of certainty that each of these elements is genuine and hasn't been altered, the system can be considered trustworthy and will inspire confidence. More importantly, this level of transaction security will alleviate the need for industry police, fines, lawsuits, and acrimony among the parties. Compliance will not be considered burdensome and PCI can restore the payment card's best feature—convenience—which was the hallmark of card programs introduced decades ago. **TT**

Mimi Hart, president and chairman of MagTek in Seal Beach, California, is a member of ETA's Technology Committee. Reach her at mimi.hart@magtek.com.

© 2009

Reprinted with permission from the
June, 2009, issue of *Transactions Trends*,
the official publication of the
Electronic Transactions Association.
www.electran.org



Published by the Electronic Transactions Association
1101 16th Street NW, Suite 402
Washington, DC 20036
202/828-2635