



Fighting the Fallout

Heartland Payment Systems addresses breach with encryption development and information sharing

By Julie Ritzer Ross

A few short months after what is being called the largest-ever data breach of its kind, Princeton, New Jersey-based Heartland Payment Systems appears to be well on the way to addressing the fallout from the incident and implementing measures aimed at preventing history from repeating itself.

The company is investing significant resources in enhancing data encryption, according to Robert O. Carr, chairman and CEO. On several occasions after the breach, Carr has publicly stated that issuers must consider using such technologies as chip and PIN, tokenization, and end-to-end encryption (E3) to expand baseline PCI security. Heartland considers encryption the best route because it currently provides the quickest, safest way to secure card data in a manner that goes beyond any prescribed by PCI, the executive says. But while the payment processor intends to fully support efforts by the American National Standards Institute (ANSI) ASC X9 Committee to develop an industry-wide E3 standard, and will utilize it when it becomes available, it is already beyond the initial stages of implementing its own E3 encryption scheme.

Transaction Zones

In late June, Heartland announced that it had successfully completed the kickoff phase of its E3 pilot project, which entailed the transmission of live AES (Advanced Encryption Standard)-encrypted card transactions from a merchant to Heartland's processing platform. AES is the highest level of encryption and is currently on track to replace DES (Data Encryption Standard) and Triple DES as the desired standard for the transmission of sensitive data.

Aimed at testing each of the major card brands, the trial involved a Texas-based merchant and multiple credit card, prepaid, and signature debit card transactions. All cards were read by Heartland's newly developed tamper-resistant security module (TRSM) terminal. The data was encrypted as the



electronic digits left the magnetic stripe and entered the TRSM hardware device. It was then transmitted to and through Heartland's processing platform for authorization and settlement. Carr says this trial represents the first time encrypted transactions have been sent from a merchant's card reader to and through a major processor's payments network.

In working to develop E3, Heartland has been looking at five distinct transaction zones. Zone 1 extends from data entry/card read at the merchant to the authorization network of the processor, and Zone 2 stretches from the entry into the authorization network of the processor and through all points in which data is in motion within the network(s) of the processor and its subcontractors. Zone 3 is the point at which data resides in a central processing unit (CPU) or a host security module (HSM), and Zone 4 marks data containment in a direct access storage device (DASD) or archival storage. Zone 5 represents the movement of data from the processor to the authorization and settlement centers of the card brand or issuer.

"The pilot test involved Zones 1, 2, 3, and 4," states Steven M. Elefant, Heartland's

executive director of end-to-end encryption. "We believe that protecting data in these zones alone will significantly impact the protection of cardholder data."

Heartland intends to enhance data protection in Zone 3 and conduct a pilot test on a set of security-protected chips to further safeguard data throughout the entire transaction later this year. Active discussions with several card brands, some of which Carr says have expressed a willingness to pursue accepting transactions from these encrypted processors, are underway in an effort to enhance data protection in Zone 5.

"We plan to continue to expedite the development of E3 and launch it commercially late this year, as well as to continue working with the ANSIASC X9 Committee in crafting an end-to-end encryption standard and to follow that standard as much as practical," Carr asserts.

Partnership Payoffs

In mid-June, Heartland teamed up with Voltage Security, an enterprise security company in Palo Alto, California, to develop E3 software specifically suited to payments processing. It also is working with

established U.S. equipment and software manufacturers to integrate their TRSM devices into E3 as it evolves. The Voltage SecureData product line will power the software component of Heartland's E3 solution.

"Typically, cardholder data is unencrypted as it leaves a merchant's terminal and is not encrypted until it is either tokenized in a gateway or at rest in the processing platform's data warehouse," explains Mark Bower, director of information protection solutions at Voltage. "This puts it at risk of being compromised should cyber-criminals or hackers get at it with network or memory sniffer malware and the like."

By contrast, the Voltage technology reportedly will enhance card data security throughout the processing cycle by maintaining encryption from the card-swiping stage through receipt by the payments network. "Even if a database is indeed hacked, the (perpetrators) will be unable to map credit card numbers, preventing them from committing fraud and identity theft," asserts

Wasim Ahmad, Voltage's vice president.

Heartland also has been sharing breach details in recent months. Carr spearheaded the founding of the Payment Processor Information Sharing Council (PPISC), whose mission is to give organizations in the payments industry a forum for sharing information about security threats, vulnerabilities, and fraud. At the group's first meeting in May, Heartland distributed USB drives containing 14 pieces of malware found on its systems following the breach. Attendees also received software needed to detect the malware from Mandiant, a forensics investigation company with offices in Washington, D.C., New York, and Los Angeles. Heartland promoted its sharing of the malicious code with the 19 companies attending the PPISC meeting as a sign of its willingness to divulge details of the attack with others in the industry.

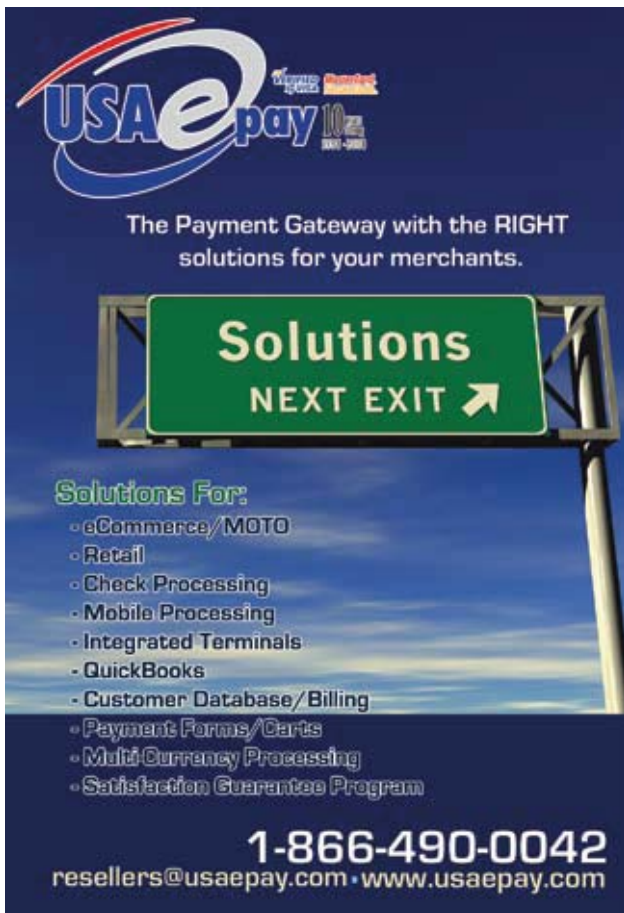
In the future, data about incidents affecting PPISC members will be shared anonymously via listserv, and conference calls will be held to update members of breaking

news. PPISC also plans to conduct mock post-breach exercises in which members react as if the incident were real. The objective is to test participants' ability to get on a call quickly and respond to the circumstances.

PPISC works with the Financial Services Information Sharing and Analysis Center (FS-ISAC). This nonprofit organization distributes breach-related and security-compliance information to its members, the government, and telecommunication and utility companies.

"We believe the marketplace will accept this higher level of payments security and are willing to share our knowledge and learning with all industry stakeholders via the PPISC, FS-ISAC, and Secure POS Vendor Alliance organizations," Carr concludes. "We are making great strides and will continue to do so." **TT**

Julie Ritzer Ross is a contributing writer for Transaction Trends. Reach her at jritzerross@gmail.com.



USAePay
The Payment Gateway with the RIGHT solutions for your merchants.

Solutions
NEXT EXIT →

Solutions For:

- eCommerce/MOTO
- Retail
- Check Processing
- Mobile Processing
- Integrated Terminals
- QuickBooks
- Customer Database/Billing
- Payment Forms/Carts
- Multi-Currency Processing
- Satisfaction Guarantee Program

1-866-490-0042
resellers@usaepay.com • www.usaepay.com



Wanted: ISO Startups
Is someone you know starting up a new ISO?

Transaction Trends wants to know.

A new series will follow several ISOs as they navigate a new startup. Please contact editor Angela Brady at abrady@strattonpublishing.com for more information.