Participation Will Be Key to Heartland's Encryption Effort

Published: 13 May 2009

Analyst(s): Avivah Litan

Heartland Payment Systems will offer end-to-end encryption to re-establish its credibility as a secure processor and strengthen its security practices. To work, its plan must be adopted by merchants and card brands.

News Analysis

Event

On 7 May 2009, during its 1Q09 earnings call, the U.S.-based credit and debit card and check payment processor Heartland Payment Systems announced that it plans to offer end-to-end encryption for merchants and other users, extending from the point of sale (POS) to the processor. Details of the plan's rollout were not available.

Analysis

As a top 10 payment processor, Heartland could have a substantial influence over the future of payment card processing. If it can develop a demonstrably secure end-to-end encryption service and persuade the main payment card networks (such as Visa and MasterCard) to participate, other payment processors could follow its lead.

Heartland’s proposal for end-to-end encryption occurs in the wake of the company’s reinstatement in Visa’s list of Payment Card Industry (PCI) certified service providers. It is part of Heartland’s strategy to strengthen its security practices and restore its image as it recovers from its January 2009 discovery of a major data security breach, which occurred even after Heartland was audited six times by a PCI-qualified security assessor that consistently determined the processor was PCI-compliant.

Spanish card processors already have a large-scale end-to-end encryption effort under way in Spain, and some large U.S. retailers also encrypt data in transit (and at rest) within their organization. But the top full-service U.S. payment processors don’t currently support this practice; thus, retailers that encrypt card data in transit typically must decrypt it before they send it to their processor.
End-to-end encryption would be most effective if data was encrypted from the time a card was swiped at a POS until it reached the card issuer, similar to the way personal identification numbers (PINs) currently are encrypted according to card brand standards. However, Heartland is limited by the scope of systems it manages and from which it accepts data; it can only seek to influence the card industry to carry end-to-end encryption beyond the processor stage, through the card networks and onto the card issuers. The proposal’s success also depends on merchants’ willingness to invest in terminal upgrades that support card data encryption.

If Heartland implements its proposed project more securely than it has managed in the past with its network, it will make payment card processing more secure for merchants, especially if they don’t manage the encryption keys and leave key management to their processor. Nevertheless, the process will always include vulnerabilities at the point where data is encrypted and decrypted. These vulnerabilities can be limited by using sound key management practices and enforcing extra security measures, such as requiring two separately managed sets of keys for cryptographic operations.

**Recommendations**

- **Merchants and other card-accepting enterprises**: Consider using processors that support end-to-end encryption of data in transit to minimize data exposure if they have had their infrastructures certified as secure by independent qualified security assessors.

- **Visa and other card brands**: Encourage merchants that participate in end-to-end encryption by offering a reduced set of PCI compliance requirements.

- **Heartland Payment Systems**: Subsidize merchant POS system upgrades in return for multiyear service contracts.

**Recommended Reading**

- “Visa Heartland/RBS WorldPay Statement Brings Needed Clarity” — In March 2009, Visa issued a statement to Gartner indicating that merchants and other card-payment-accepting enterprises could continue to do business with Heartland and RBS WorldPay without the threat of a fine from Visa. By Avivah Litan

- “Heartland Case Shows Stronger Security Is Still Needed” — A highly damaging data breach highlights the ongoing need for upgraded PCI security requirements and processes to protect against the most significant current threats. By Avivah Litan

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)