DISCUSSION PAPER
PAYMENT CARDS CENTER

Heartland Payment Systems: Lessons Learned from a Data Breach

Julia S. Cheney*

January 2010

Summary: *On August 13, 2009, the Payment Cards Center hosted a workshop examining the changing nature of data security in consumer electronic payments. The center invited the chairman and CEO of Heartland Payment Systems (HPS or Heartland), Robert (Bob) Carr, to lead this discussion and to share his experiences stemming from the data breach at his company in late 2008 and, as important, to discuss lessons learned as a result of this event. The former director of the Payment Cards Center, Peter Burns, who is acting as a senior payments advisor to HPS, also joined the discussion to outline Heartland's post-breach efforts aimed at improving information sharing and data security within the consumer payments industry. In conclusion, Carr introduced several technology solutions that are under discussion in payment security circles as ways to better secure payment card data as they move among the different parties in the card payment systems: end-to-end encryption, tokenization, and chip technology. While HPS has been very supportive of end-to-end encryption, each of these alternatives offers its own set of advantages and disadvantages.*

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: julia.cheney@phil.frb.org. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.philadelphiafed.org/payment-cards-center/

I. Introduction

On August 13, 2009, the Payment Cards Center hosted a workshop examining the changing nature of data security in consumer electronic payments. The center invited the chairman and CEO of Heartland Payment Systems (Heartland), Robert (Bob) Carr, to lead this discussion and to share his experiences stemming from the data breach at his company in late 2008 and, as important, to discuss lessons learned as a result of this event. The former director of the Payment Cards Center, Peter Burns, who is acting as a senior payments advisor to Heartland, also joined the discussion to outline Heartland's post-breach efforts aimed at improving information sharing and data security within the consumer payments industry. In conclusion, Carr introduced several technology solutions that are under discussion in payment security circles as ways to better secure payment card data as they move among the different parties in the card payment systems: end-to-end encryption, tokenization, and chip technology. While Heartland has been very supportive of end-to-end encryption, each of these alternatives offers its own set of advantages and disadvantages.

Heartland Payment Systems has built its business on the acquiring side of consumer payment systems. In a four-party system,[1] on one side are bankcard issuers and their customers who hold consumer payment cards. These cardholders use their credit, debit, and prepaid cards to make purchases at merchants. The term "merchants" is broadly defined to include not only retail merchants but also any entity, such as a doctor's office, that accepts card-based payments in exchange for goods or services. On the other side, merchant banks or, as is many times the case, their merchant acquiring or processing partners[2] process consumer card payments into payment

[1] For more detail, see James M. Lyon, "The Interchange Fee Debate: Issues and Economics," *The Region*, June 2006, Federal Reserve Bank of Minneapolis. (www.minneapolisfed.org/publications_papers/pub_display.cfm?id=3235)

[2] The roles played by merchant banks, merchant acquirers, and merchant processors are not always distinct. Merchant banks may act solely as a partner to merchant acquirers or merchant transaction processors for the purposes of sponsoring access to payment card networks. On the other hand, a merchant bank may also act as an acquirer or a processor. Merchant acquirers that are not also merchant banks may only acquire

card networks on behalf of merchants.[3] For example, in its role as a merchant acquirer and processor, Heartland acts as the intermediary between the merchant point of sale (POS) and the banks' card networks (Visa Inc., MasterCard Worldwide, American Express, and Discover Financial Services). Heartland receives and stores the payment information, including card details and purchase amount, from the merchant and sends it to the appropriate network in order to obtain payment authorizations, facilitate account reconciliation between merchants and bank card issuers, and manage the chargeback process.[4]

Heartland Payment Systems has been in the merchant acquiring and transaction processing business since 1997. It has built its merchant base from 2,500 clients, processing $0.4 billion in transactions, to over 250,000 clients, processing over $80 billion and 4.2 billion transactions annually. According to *The Nilson Report*, Heartland is currently the fifth largest merchant acquirer in the United States ranked by number of general-purpose-card purchase transactions.[5] Heartland has also expanded its processing services to include more than credit, debit, and prepaid card payments. Today, Heartland also processes payments related to payroll, Check 21, online payments, micropayments, and gift and loyalty programs.

merchant processing contracts on behalf of merchant banks or merchant processors. Merchant acquirers may also be merchant processors and, therefore, acquire merchant processing contracts to expand their own processing business. Similarly, merchant processors may also be merchant acquirers, or, alternatively, they may perform only those duties associated with the processing of merchant transactions.

[3] In order to access the payment card authorization networks managed by Visa and MasterCard, a merchant processor either must be a bank and a member of the payment card network or must have a partnership with a bank sponsor to enable access to the card network. In Heartland's case, it has partnered with bank sponsors to allow it direct access to the payment card networks.

[4] Merchant transaction processors perform a number of other account management functions for merchants, but this discussion focuses on the role these firms play in the movement of data among the four parties in the consumer card payment systems. For more information on the various activities performed by merchant acquirers and processors, see Ann Kjos, "The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges," Payment Cards Center, October 2007. (www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf)

[5] *The Nilson Report,* Issue 922, March 2009, p. 1.

II. Heartland's Data Breach: What Happened?

The method used to compromise Heartland's network was ultimately determined to be SQL injection. Code written eight years ago for a web form allowed access to Heartland's corporate network. This code had a vulnerability that (1) was not identified through annual internal and external audits of Heartland's systems or through continuous internal system-monitoring procedures, and (2) provided a means to extend the compromise from the corporate network to the separate payment processing network. Although the vulnerability existed for several years, SQL injection didn't occur until late 2007.

After compromising Heartland's corporate network, the intruders spent almost six months and many hours hiding their activities while attempting to access the processing network, bypassing different anti-virus packages used by Heartland. After accessing the corporate network, the fraudsters installed sniffer software[6] that was able to capture payment card data, including card numbers, card expiration dates, and, in some cases, cardholder names[7] as the data moved within Heartland's processing system.[8]

The fraudsters' focus on compromising data as they moved within Heartland's network – data in transit – rather than when they were stored in consumer databases — or, in other words, when data were at rest — was a relatively new phenomenon as described by Carr. One example, if not the first, of this expansion in focus toward data-in-transit compromises was the data breach at

[6] Sniffer software is defined as "a hardware or software mechanism that monitors, and possibly records, data traffic on a network." See the *Encyclopedia of Information Science and Technology*, 2005 edition.

[7] Thomas Claborn, "Heartland Payment Systems Hit by Data Security Breach," *Information Week*, January 20, 2009. (www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212901505)

[8] According to a Heartland press release, "No merchant data or cardholder Social Security numbers, unencrypted personal identification numbers (PIN), addresses or telephone numbers were involved in the breach. Nor were any of Heartland's check management systems; Canadian, payroll, campus solutions or micropayments operations; Give Something Back Network; or the recently acquired Network Services and Chockstone processing platforms." For more information see the press release, "Heartland Payment Systems Uncovers Malicious Software in its Processing System," Heartland Payment Systems, January 20, 2009. (www.2008breach.com/Information20090120.asp)

Hannaford Brothers announced in early 2008[9]. In Carr's opinion, the technique used in the Hannaford case is something that should have been well understood by the industry in a few weeks' time. Instead, after the Hannaford breach, Carr emphasized that the same method of attack focused on stealing data in transit had been applied many times prior to Heartland's breach.

For Carr, this precedent raised a clear signal that quicker and more efficient methods of information sharing related to breach techniques were needed in order to limit fraud risks. He underscored the fact that knowledge of breach techniques should not be viewed as a competitive advantage among merchants or their processors. Rather, sharing this information is an important contribution to securing increasingly important consumer payments systems and increases the network value for all participants.

In addition, Carr noted that Heartland was certified by network-approved quality security assessors (QSAs) as being PCI compliant at the time of the breach[10] and, in fact, had received this certification several times during the period in which the vulnerability had been present. He used this point not to diminish PCI but rather to emphasize that PCI compliance is a minimum standard and that most companies regularly do much more than required by PCI. Heartland Payment Systems was one of those companies that had met its PCI requirements and had made data security one of its top, if not its top, business priorities. Carr said that Heartland manages data security 24/7 and has about 7 percent of its information technology staff focused on security efforts, including a recently hired senior executive who focuses solely on data security and

[9] Clarke Canfield and Brian Bergstein, "Hannaford Data Breach Offers Twists from Prior Attacks," Associated Press, March 20, 2008.

[10] The Payments Cards Industry (PCI) Security Standards Council was founded in 2006 by five card networks — Visa, Inc., MasterCard Worldwide, Discover Financial Services, American Express, and JCB International. Together these card brands equally share in the governance of the organization that is responsible for the development and management of PCI Data Security Standards (PCI DSS). PCI DSS is a set of security standards that all payment system participants, including merchants and processors, are required to meet in order to participate in card payment systems. To help validate that card payment system participants meet PCI DSS standards, the card brands have approved about 100 companies to be qualified security assessors (QSAs). QSAs perform security audits on firms that meet certain criteria to determine their compliance with PCI DSS. A list of these standards, the PCI DSS audit requirements, and more information about the PCI Security Standards Council and the QSA assessment process is available at www.pcisecuritystandards.org/.

strategy.[11] That a data breach occurred despite Heartland's strong focus on data security and its status as being PCI compliant has led Carr to the opinion that more must be done to increase the security of data transfers (data in transit) among participants in the payments system, including merchants.[12]

To address his concerns regarding data sharing and payment network data security, Carr initiated two strategic objectives at Heartland in the wake of the breach: provide leadership (1) in creating a collaborative information-sharing capability and (2) in advancing technical solutions to secure data, in particular as they move among participants on the acquiring side of the payments system. Senior payments advisor Peter Burns led a discussion of these efforts described in the next section.

III. Heartland's Response

As noted, Heartland's response to its data breach rested on two pillars aimed at the merchant acquiring and processing side of the payment system: improve data sharing and better secure data, particularly data in transit.

a. Improve Information Sharing

Burns observed that the merchant acquiring side of the payments network has always faced greater coordination challenges than the issuing side of the business. Unlike bank card issuers, the acquiring side does not enjoy the range of information-sharing outlets sponsored by such bank-oriented organizations such as the American Bankers Association or BITs. Coordination problems have arisen on the merchant acquiring side for a variety of reasons, including a much more fragmented marketplace than on the card-issuing side. For example, in the

[11] For employee information, see also Heartland's 2008 10-K filing.

[12] For more information on data at rest and data in transit, see James C. McGrath and Ann Kjos, "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges," Payment Cards Center, September13-14, 2006, p. 7. (www.philadelphiafed.org/payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pdf)

U.S., there are over 7 million card-accepting merchants, while there are only about 6,000 credit card-issuing depository institutions.[13] Moreover, the merchant processing supply chain is more extended and complex than on the card-issuing side, with roles played by merchants, merchant banks, merchant acquirers, third-party processors, independent sales organizations (ISOs), and a variety of additional third-party service providers.[14]

To overcome the coordination problems, Heartland, Burns noted, identified an already existing infrastructure that could be leveraged in support of its data-sharing initiative. This infrastructure, managed by the Financial Services Information Sharing and Analysis Center (FS-ISAC),[15] allows for the dissemination of information about security threats to a broad membership that includes not only banks but a wide range of financial services providers. FS-ISAC relies on a foundation of public-private partnerships to facilitate the gathering of information about a range of security threats and disseminating that information among law enforcement, government agencies, and FS-ISAC's private-sector member companies.

In partnership with the FS-ISAC, Heartland helped to establish the Payments Processing Information Sharing Council (PPISC) as a subgroup under the FS-ISAC umbrella. Burns noted that, at this time, membership in PPISC is limited to bank-owned and third-party card payment

[13] U.S. Government Accountability Office, "Credit Cards: Rising Interchange Fees Have Increased Costs for Merchants, but Options for Reducing Fees Pose Challenges," Report to Congressional Addressees, November 2009, p. 6.

[14] For more information on the types of service providers that may participate in the merchant processing supply chain, including ISOs, see Ann Kjos, "The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges," Payment Cards Center, October 2007, p. 7-8. (www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf)

[15] FS-ISAC was established as the result of a 1998 Clinton Presidential Directive (63) that was later updated by President Bush in 2003 under Homeland Security Presidential Directive 7. This directive mandated identification of infrastructures, which included the banking and finance industry, critical to the operation of the U.S. economy and the U.S. government. As these sectors became more reliant on information technology, more overlap existed with regard to system risks due to physical and cyber security threats. In recognition of this commonality, the directive aimed to better coordinate information-sharing efforts such that threats could be identified earlier and then shared not only across the critical infrastructures but also between the public and private sectors. The FS-ISAC is the organization established to support information sharing among members of the banking and financial services industries and between the private-sector industry and the public sector. For more information on FS-ISAC, visit its website at www.fsisac.com.

processors serving the merchant community. In order to provide a venue and structure for quickly and confidentially sharing information about new and emerging types of security threats and risk mitigation techniques, each member must sign a nondisclosure agreement[16] Following an organizational meeting held in conjunction with the FS-ISAC annual conference in May, response from the industry has been supportive; companies representing some 85 percent of the industry's processed merchant transactions have joined. Since the date of this workshop, the PPISC has formed a Steering Committee and elected Bob Carr as its chair. It has also formed two working groups among its members, developed a member-only portal on the FS-ISAC website, and helped structure a computer-based exercise involving data threats to be held in February 2010.Ultimately, Burns emphasized that the objective of this information-sharing initiative is to enable member firms to more quickly identity data security threats and to more efficiently respond to these threats.

Carr raised another facet of information sharing that is challenging merchants and their processors and one that he feels needs further attention: the PCI auditing process. In Heartland's experience, qualified security assessors (QSAs) had repeatedly rated Heartland as being PCI compliant[17] without detecting the existing SQL injection vulnerability. In addition, after the breach, Heartland was required to contract with a qualified incident response assessor (QIRA) to perform an independent forensic investigation of the breach to determine its source. Even though the method of attack had been used many times in the months preceding Heartland's breach, Carr emphasized that it went unidentified during QSA audits. It also took the QIRA six weeks to identify the cause of Heartland's compromise.

[16] According to the *Modern Dictionary for the Legal Profession, Third Edition,* a nondisclosure agreement is an "agreement restricting the use of information by prohibiting a contracting party from divulging data." In essence, a nondisclosure agreement is a legal contract between two or more parties that defines information that will be shared among the parties and that may not be shared with any entity not a party to the contract.

[17] The PCI Security Standards Council has approved over 100 companies and 1500 employee assessors to validate firms as being PCI compliant. For more information, see www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

In both cases, Carr suggested that better data sharing — among the 100 or so companies approved by the networks to perform PCI compliance audits and the handful of companies approved by Visa[18] as response investigators — might have helped to identify the vulnerability before it happened and, once it did, to identify the cause of the breach more quickly, thereby limiting the amount of card data that the thieves were able to steal. Carr suggested that clients' privacy concerns and competitive positioning by QSAs and QIRAs may be hindering information sharing among these firms. At the same time, he believed that these obstacles could be overcome by structuring information-sharing efforts in a way that ensures client anonymity and focuses information sharing narrowly on the attack methodologies.

In his concluding remarks on information sharing, Carr noted several additional observations taken from Heartland's data breach experience that are instructive: (1) do not underestimate the insider threat, (2) ensure the appropriate audit scope, and (3) maintain in-house security expertise at the senior executive level. Carr emphasized that insider threats may not stem from intentional fraud but rather from misplaced employee goodwill. For example, an employee may retain cached files, including account information, on their computer in order to more quickly process customer service requests. In addition, security protocols must be universally applied and enforced among all employees, at all levels of hierarchy and across all departments. Ensuring that auditors have a wide scope to review systems for security vulnerabilities is also important to identify situations, such as happened at Heartland, in which fraudsters were able to penetrate the processing systems by first compromising another, separate network, in this case the corporate network. Finally, security expertise and strategic planning are critical skills that should be emphasized at the highest levels of the corporate structure.

[18] Visa has published more information on its data breach response process at www.usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf as well as a list of companies approved as QIRAs. See www.usa.visa.com/download/merchants/cisp_qualified_cisp_incident_response_assessors_list.pdf.

b. Better Secure Data, Particularly Data in Transit

The second pillar of Heartland's response to its data breach rested on providing leadership in advancing technical solutions that would better secure data in transit. Carr described three technologies that his company considered: end-to-end encryption, tokenization, and chip technology. After reviewing these solutions, Heartland's data security team and executive management identified end-to-end encryption as the technology best able to address security risks as data move through the merchant processing chain in the authorization and capture process. Also, end-to-end encryption was the option that gave Heartland, as a merchant processor, the most direct influence.[19]

Before discussing Heartland's view of end-to-end encryption and the steps the company has taken to date to move it toward a reality, a simple overview of each of these technology solutions follows:

- **End-to-end encryption**

  The concept behind end-to-end encryption[20] is to encrypt payment card data[21] when it must be shared among payment network participants (data in transit) and when it must be stored in proprietary systems (data at rest) as part of the process to authorize, authenticate, and settle card transactions. Some commentators believe that encryption should begin with the plastic card itself (e.g., chip or smart cards). Others, including Heartland, establish the starting point for encryption as the card swipe at the point of sale as the magnetically stored digits (analog data) are converted to digital data by the magnetic stripe reader. In either case, end-to-end

[19] Other payment processors are also offering or testing end-to-end encryption platforms, including RBS WorldPay and Electronic Payment Exchange. See Avivah Litan, "Where to Begin for End-to-End Encryption Systems," *American Banker*, September 15, 2009.

[20] End-to-end encryption is defined as "the continuous protection of the confidentiality and integrity of transmitted information by encrypting it at the origin and decrypting it at its destination." See Smart Card Alliance, "End-to-End Encryption and Chip Cards in the U.S. Payment System," September 2009, p. 5.

[21] Payment card data are related to information associated with the card account and the individual transaction. Such information may include cardholder name and address, card number and expiration date, and transaction details such as the dollar amount and a unique identifier.

encryption requires that once encryption occurs, from that point forward in the processing chain card data should never be transmitted in clear text among the participating parties in the payment system.

- **Tokenization**

  Tokenization is the use of randomly generated numbers or "tokens" as replacements for card data. Generally, tokens are assigned after authorization and matches between the tokens and card data are maintained by third-party service providers. This process allows merchants to delete card data in their systems and use the assigned tokens to reference transactions. Moreover, after authorization and capture, the tokens may also be used to reference the transaction and the card data as the transaction travels through the payment system and during the potential dispute period that remains for several months after settlement has occurred. Therefore, if a merchant or its processor is hacked, thieves are unable to steal actual card data because they aren't held in these systems. On the other hand, card data are still at risk if the third-party service provider's systems are compromised.[22] Many times tokenization is combined with a form of encryption.

- **Chip technology**

  Chip technology embeds a computer microchip within the traditional plastic payment card or in alternatives such as a contactless payment card or key fob to enable encrypted storage of data on the payment card, encrypted exchange of card data between the card and the merchant terminal, and encrypted transmission of card data among payment system participants.[23] To date, U.S. payment system participants have been reluctant to pursue chip

[22] In some ways, PayPal may be seen as a provider of a form of tokenization technology because it facilitates transactions between merchants and consumers without requiring merchants to obtain, store, or process payment information.

[23] Chip or smart card solutions may take many formats, depending on the technology applied. For more information on these variations, see the Smart Card Alliance website at www.smartcardalliance.org. See also Richard Sullivan, "Can Smart Cards Reduce Payments Fraud and Identity Theft?" Federal Reserve Bank of Kansas City, *Economic Review*, Third Quarter 2008.

technology because estimates of implementation costs, including upgrading infrastructure and acceptance and processing systems, are significant.[24]

In fact, each of these technologies may be applied to the market in a variety of ways and formats, including systems that offer a combination of these and other solutions.[25] These variations are also continually evolving. As a result, it is difficult to adequately estimate implementation costs that may fall on individual payment system participants or on the payment system as a whole.

IV. Heartland's End-to-End Encryption Solution

Among these three technology solutions, Heartland chose to support end-to-end encryption for a number of reasons. Heartland executives believed they could exert the most direct influence over the development and implementation of this technology without requiring the cooperation of other payment system participants.[26] It was important to Carr that Heartland be able to control much of the rollout of end-to-end encryption because, in this way, Heartland could avoid potentially significant coordination problems. Carr also emphasized that Heartland leveraged third-party technology providers in order to fulfill its vision of end-to-end encryption. These partnerships helped Heartland quickly develop and execute its plan for better data security as well as minimize costs for its merchant community. As important, Heartland executives saw end-to-end encryption as the technology best able to immediately address data-in-transit risks as data moved among Heartlands' merchants, its proprietary systems, and its network partners. At the

[24] Speer & Associates, Inc. estimated this cost to be over $10 billion in its March 29, 2008 issue of *Strategic Commentary*. See Susan Herbst-Murphy, "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud," Payment Cards Center, conference summary, April 2008, footnote 7, p. 15. (www.philadelphiafed.org/payment-cards-center/events/conferences/2008/PCCAprEvolvingThreatsFraud.pdf)

[25] For example, Heartland's CIO, Steve Elefant, recently discussed combining end-to-end encryption with tokenization and a solution he described as dynamic data authentication. For more details, see Tom Field, "Heartland CIO on Improving Payments Security: Steven Elefant Discusses the Breach, End-to-End Encryption," *Bank Info Security*, November 17, 2009.

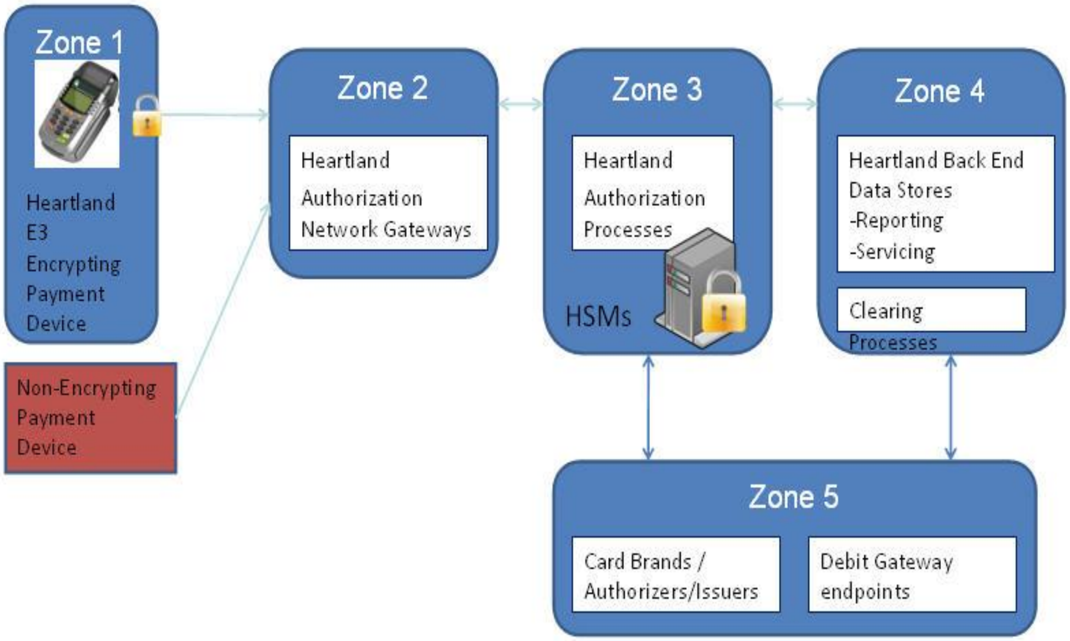
[26] For more details, see the discussion of Heartland's encryption zones (1-5) in the next paragraph.

same time, Carr believed that end-to-end encryption also facilitated encryption of data at rest when held in private networks, either in merchant or processor systems.

To further define the end-to-end encryption process envisioned by Heartland, Carr described five encryption zones making up the merchant processing chain. Each zone represents a point in payment processing at which, traditionally, data must be decrypted and re-encrypted. Again, Carr emphasized that Heartland's end-to-end encryption model positioned Heartland to secure much of this process (zones 1-4) using its own resources; only zone 5 encryption required cooperation from the card brand networks.

- Zone 1: The payment processing system at the merchant, including the payment terminal located at the merchant point of sale.
- Zone 2: The transmission of card data from a merchant's systems to its processor's systems.
- Zone 3: The internal processing that takes place within the computer systems and hardware security modules (HSMs) of the payment processor.
- Zone 4: A data-at-rest function encompassing the payment processor's internal data storage system.
- Zone 5: The transfer of data from the payment processor to the card networks. (authorization and settlement)

The graph below illustrates these five zones as described above by Carr.


Zone 1
Heartland E3 Encrypting Payment Device
Non-Encrypting Payment Device
Zone 2
Heartland Authorization Network Gateways
Zone 3
Heartland Authorization Processes
HSMs
Zone 4
Heartland Back End Data Stores
-Reporting
-Servicing
Clearing Processes
Zone 5
Card Brands / Authorizers/Issuers
Debit Gateway endpoints

**Source: Heartland Payment Systems*

As Heartland's team discussed how best to develop end-to-end encryption, they identified three potentially significant barriers to merchants' investment in this technology: cost and design of terminal hardware, operational burden imposed by key injection and public key management, and compatibility with legacy systems. Carr described each of these challenges and how Heartland addressed them by leveraging innovative solutions and the participation of a variety of technology providers.

Heartland faced two potential obstacles when addressing initial encryption procedures at its merchants' sites. The first was to design an encryption system that could be cost effectively incorporated into terminal hardware and the second was to support and develop merchants' incentives to invest in the upgraded terminal hardware. Heartland and its terminal design partner leveraged security technology used at the point of sale for the entry of personal identification numbers (PINs). Simply, this process encrypts PINs using cryptography housed in tamper-resistant security modules (TRMs) housed within a merchant's POS terminal (. Then the encrypted PINs are transmitted to payment processors who use hardware security modules (HSMs) to manage the keys necessary to decrypt the PINs as part of the authorization process. In

Heartland's model, a similar process is employed for magnetic stripe, non-PIN cards as well as PIN cards. In the case of non-PIN magnetic stripe cards, the primary account number (PAN) and other track data[27] are encrypted when the card is swiped at the merchant terminal and remain encrypted as they are transmitted to the merchant's third-party processor (zones 1 and 2). The data also remain encrypted while processed and stored at the third-party processor (zones 3 and 4). Data are decrypted only after they have been received into Heartland's HSM and when required by the card brands in order to enter their authorization networks. Carr emphasized that he has received positive feedback from the card brands regarding efforts to accept encrypted data. He noted that this work is continuing and, if successful, will complete the final step in the end-to-end encryption process envisioned by Carr and his team.

Carr acknowledged that the terminal designed by Heartland and its partner is not free for merchants. It costs between $300 and $500. He discussed incentives for merchants to invest in the upgraded terminal, ones that will influence participation levels in Heartland's end-to-end encryption scheme. Foremost, Carr noted that merchants are weighing the costs of compliance with PCI DSS plus the investments they would have to make to institute end-to-end encryption against the potential relaxation of their compliance responsibilities.

Obviously, part of this analysis will examine PCI-DSS compliance costs for merchants. According to a report by Mercator Advisory Group, Inc., these costs are significant and increasing. Average PCI compliance costs for tier 1 merchants (over 6 million transactions a year) in 2008 were forecast to be almost $3 million, a 127 percent increase over PCI compliance spending in 2006. Costs for tier 2 merchants (between 150,000 and 6 million transactions a year) in 2008 were estimated to be almost $1.5 million, a 97 percent increase over 2006 costs. Finally, 2008 costs for tier 3 merchants (fewer than 150,000 transactions) were projected to be about $.17

[27] Track data include the card number, the card's expiration data, the cardholder's name and address, and a service code, along with discretionary information that may represent the PIN verification value or card verification value (a three- or four-digit code printed on the back of the payment card).

million, a 16 percent increase over 2006 levels.[28] While PCI compliance requirements for smaller merchants (tier 3) are less burdensome, the average cost per transaction in 2008 was likely more than four times greater than those costs for tier 2 merchants.[29]

To the extent that end-to-end encryption is able to reduce the scope of PCI audits and the associated compliance burdens on merchants, Carr stated that the resulting cost savings can justify investing in the terminal hardware that enables this technology.[30] Any compliance savings would require that card brands and the PCI Security Standards Council support end-to-end encryption as a mechanism to reduce risk at participating merchants and third-party processors. There is some evidence that both constituencies[31] are studying the protections afforded not only by end-to-end encryption but also by other emerging technologies, including tokenization and chip technology. For example, the PCI Security Standards Council contracted with PricewaterhouseCoopers to "evaluate which technologies have the potential to facilitate compliance and reduce risk associated with payment card data."[32]

In Carr's experience, merchants are also very conscious of the potential reputational risk and cost exposure that may arise because of a data breach. Merchants do not want their customers

[28] George Peabody, "End to End Encryption: The Acquiring Side Responds to Data Loss and PCI Compliance," Mercator Advisory Group, June 2009, p. 9.

[29] This estimate was derived by dividing the average 2008 PCI compliance cost by the ceiling number of transactions, for both the tier 2 and tier 3 merchant categories. For example, the average 2008 PCI compliance cost for tier 2 merchants was $1,450,000 and the tier is bounded by merchants with 6 million transactions. The PCI compliance cost per transaction was calculated by dividing $1,450,000 by 6,000,000, equaling $0.24 per transaction. The same method was used to calculate the per transaction cost for tier 3 merchants: dividing $168,600 by 150,000 transactions, which equals $1.12 per transaction.

[30] The PCI Security Standards Council announced that it has begun the process to review stakeholder feedback as part of developing the next iteration of the PCI DSS. One area being considered as part of the update to PCI DSS is "examining the impact of technologies like tokenization, end-to-end encryption, chip technology, and virtual terminals on PCI standards." See PCI Security Standards Council, "PCI Security Standards Council Enters Next Phase of Data Security Standards Development," press release, November 16, 2009.

[31] Ellen Richey of Visa, Inc. stated that "we are working on an approach that would allow merchants to satisfy some of our compliance requirements through the application of chip or encryption tools." See Avivah Litan, "Where to Begin for End-to-End Encryption Systems," *American Banker*, September 15, 2009.

[32] PricewaterhouseCoopers, "PCI Standard Evolves to Address Continued Security Threats," *Quickbrief*, August 31, 2009.

to choose to do business with a competitor because of perceptions about data security, nor do merchants want to be subject to card brand fines or issuer recovery costs associated with, for example, card reissuance. To the extent that merchants can reduce or eliminate their exposure by storing less card data or better encrypting card data, Carr believes that there are real incentives for merchants to do so.

The next potential barrier identified by Carr dealt with the operational and cost burden placed on merchants due to the key injection and management process. In the past, each PIN point-of-sale terminal required a unique key to identify the terminal. Keys have a limited shelf life due to fraud controls, changes in processors, or potential compromises, requiring new keys to be "injected" into terminals. In most cases, key injection requires that terminals be swapped out while their keys are changed. Depending on the number of terminals a merchant maintains, this can be a costly and cumbersome proposition.[33] When expanding the PIN security infrastructure to all magnetic stripe cards, Heartland recognized that broadening key management responsibilities for merchants may act as a barrier to adoption of end-to-end encryption.

To address this problem, Heartland partnered with Voltage Security, a company that offers identity-based encryption (IBE). Among other things, identity-based encryption does not require key injection after the public key is injected during the manufacturing process. As a result, merchants participating in Heartland's end-to-end encryption need not swap out terminals in order for key injection to occur because IBE provides an alternative solution.

Finally, the Voltage Security product also preserves format, which means that legacy systems designed to store primary account numbers do not need to be modified to accommodate a larger number of bytes, as has been traditionally required when encrypting card data. Therefore, the format-preserving platform limits system modifications and associated costs that might have been necessary if merchants were required to modify platforms to accommodate a larger field.

[33] Stuart Taylor, "Go Remote: Boost Security and Profits," *The Green Sheet* 2.0, Issue 09:04:02, April 27, 2009. (www.greensheet.com/emagazine.php?issue_number=090402&story_id=1313)

By designing its end-to-end encryption platform in this way, Heartland was able to address many merchant concerns about hardware replacement costs and increased operational costs. A remaining concern for Carr and others centers on the development of standards for end-to-end encryption technology and its process. [34] Carr noted that his company is working with the American National Standards Institute (ANSI) to begin development on standards but acknowledged that this is typically a long process. In the meantime, Heartland is making its end-to-end encryption process public, including sharing details of its solution with competitors and its terminal specifications with other terminal vendors. Carr hopes that by doing so, Heartland will be able to (1) build adoption and support for standards consistent with its end-to-end encryption model and (2) address one last merchant concern – increased switching costs – by making the Heartland end-to-end encryption process a common offering in the merchant processing community.

V. Conclusion

Carr acknowledged that Heartland is working within the confines of the merchant acquiring and processing environment to address data security both through improved information sharing and security of data in transit. He recognized that end-to-end encryption is not a solution that makes sense in mitigating some types of fraud faced primarily on the card-issuing side of payment networks, such as application fraud and new account identity theft.[35] At the same time, he believes that it is important to contribute to better data security measures in meaningful ways and in areas where his company can have a direct influence on the development of enhancements to the payment system.

[34] Visa released a best practices document addressing data field encryption, otherwise known as end-to-end encryption, to "assist merchants in evaluating the new encryption solutions emerging in the marketplace." See Visa Best Practices, "Data Field Encryption Version 1.0," October 5, 2009. (www.corporate.visa.com/_media/best-practices.pdf)

[35] Carr also stated that end-to-end encryption doesn't address counterfeit card fraud.

In addition, Burns suggested that because data security and fraud mitigation priorities may differ depending on the role a participant plays in the consumer payment card networks, the prospect of larger coordination and incentive problems are raised. And while Heartland chose to address data security on a specific side of payment networks – the acquiring side – and has aimed to do so in such a way that it can exert some control over the process, this choice does not mean that Heartland undervalues the contribution made when all payment system participants engage in discussions of how to better secure payment and consumer data.

For example, Burns and Carr observed that card brands are uniquely positioned to influence merchant incentives to adopt technology solutions and to address competitive issues arising in efforts to improve data sharing. Among the levers card brands may use to encourage technology adoption among merchants include facilitating the development of standards, reducing interchange costs or data security fines for participating merchants, or subsidizing hardware purchases for those merchants interested in pursuing an end-to-end encryption or similar risk-reduction strategy. Card brands may also be best situated to encourage information sharing, especially among QSAs and QIRAs, as a way to leverage merchant and processor fraud experiences to limit future exposure and, potentially, subsequent losses. Each of these efforts alone or in conjunction may help boost merchants' confidence that their investment in emerging data protection technologies will garner returns in the form of cost savings.

In the end, the data breach at Heartland was very costly for the company: Immediately following the breach, it lost 50 percent of its market capitalization and, as of August 2009, had spent more than $32 million on legal fees, forensic costs, reserves for potential card brand fines, and other related settlement costs. Carr emphasized that others in the payments chain also face losses when data breaches occur. Most important, if the breach is significant enough or if there are a number of breaches over a short period of time, consumer confidence in card-based electronic payments may suffer, causing consumers to switch to less efficient forms of payments. If this were to happen and card transaction volumes declined, card brands and issuing banks will also face contractions in their business. In responding to breaches, issuing banks might face costs due to card reissuance, fraud losses, or customer attrition as a result of the event. For these reasons, Carr emphasized that all participants in card payment networks have many incentives to reduce risks associated with data breaches and, indeed, these firms are finding more ways to coordinate their efforts in doing so.