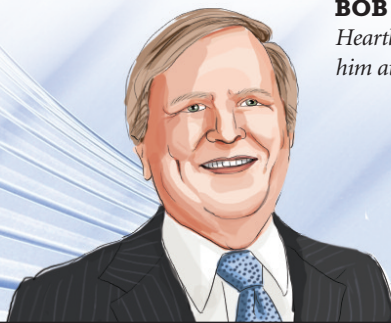


EDITOR'S NOTE: Earlier this year, Heartland Payment Systems and Visa Inc. reached a settlement in which issuers of Visa-branded credit and debit cards can obtain a recovery from Heartland with respect to losses incurred from the 2008 criminal breach of Heartland's payment system environment. CSP asked Heartland's Bob Carr to share lessons learned from the security violation.



BOB CARR is chairman and CEO of Heartland Payment Systems. You can reach him at bob.carr@e-hps.com.

Anatomy, Aftermath of a Criminal Breach

On Jan. 20 of last year, we at Heartland Payment Systems shared an awful discovery. We learned the previous week that criminals had breached our payments environment eight months earlier. We were stunned.

Last year turned out to be quite a year in many ways—some expected and some not. I would like to think that our breach and the manner in which we have handled it have resulted in many positive developments in the payments security arena already. I am confident that 2010 will be the year of major deployments of enhanced security processes in the United States, with more and more solid improvements coming in the following years.

In the meantime, I'd like to share with you some of the hard lessons we learned. It is my hope that by sharing the messages from the pain we incurred, we will help strengthen the security of the payments industry and advocate collaboration to improve the system, lower the costs and the risks—and better position ourselves to fight the bad guys.

Bringing Clarity

I have attended many conferences and conventions, including the NACS Show and NRF Tech sessions, over the past 20 months. I have addressed about 14 such

events either as a keynote speaker or panelist. I have listened carefully to what various industry experts and advocates have been saying, and I have watched what they are doing. I have testified before U.S. Sen. Joseph Lieberman's subcommittee on how best to protect industries against cyber attacks, and I've reached out to several U.S. representatives and senators about oppor-



tunities for improving our defenses against a faceless crime that is costing our nation billions of dollars.

On the whole, I must say I have never been more proud of the payments industry during this period. For the most part, I believe the security-focused authorities in the banking, card brand, government and payments

communities are responsible professionals using their best efforts to control the problem of cyber crime.

On the other hand, some of the vendors and some of the trade groups have been disappointingly shrill advocates for untenable positions.

The confusion about data security and PCI compliance is at an all-time high. Those we should rely on are either spot on or are working overtime to advocate their product or their organization's positions, making it difficult for those trying to understand what is real and what isn't. My goal in taking the time to write this and future articles is to bring clarity to the issues of data security and PCI compliance for the nonexpert who wants to reduce risk and cost for his/her organization.

In future articles, I will discuss my view of the merits of different methods of reducing risks and costs. But, in this inaugural article, I think it is worth saying "time out" and addressing issues I suspect may raise some eyebrows in the petroleum community.

Three Issues to Consider

The demonization of the card payment industry has reached hysterical levels in some corners of our industry. Much of the criticism is well deserved, but much of it is baloney and destroys

the valid arguments brought by petroleum retailers.

I have many concerns myself about the high cost of card acceptance these days and will discuss some of these in future articles. But first, I'd like to address three important matters that are worthy of the thoughtful attention of serious people in our industry. I think there is much misinformation for a variety of reasons in these important areas.

► **PCI compliance is a necessary and useful set of guidelines and best practices.** I have attended conferences where advocates have actually declared PCI was created for the sole purpose of taking money out of the petro dealers' pockets and putting it into the pockets of Visa and MasterCard. I have a secret for those who believe that: You're wrong!

Visa and MasterCard certainly don't need PCI compliance to transfer your money into their pockets. More important, the card brands have every reason in the world to end losses from data breaches, and to suggest that these companies are this evil is beyond the pale.

I have my complaints against the card brands, too, but let's put some sanity into this discussion. Petroleum professionals should know better than anyone what it is like to be on the receiving end of cheap shots. PCI compliance is not perfect, but it is certainly needed so that businesses, including the roughly 150,000 convenience-store operators, know how best to secure their systems from the hundreds of thousands of cyber criminals who are out to steal valuable card data.

► **Removing valuable card data from your systems is a very good answer for reducing risk/cost.** George Peabody, principal analyst at Mercator Advisory Group, has called it a "Reverse Rumpel-

stilskin." Rumpelstilskin took worthless straw and turned it into valuable gold. Turning valuable card data into worthless gibberish is the reverse, and that is exactly what techniques like encryption and tokenization can do to card data. Pretty much everyone agrees that encrypted or tokenized data is less valuable than card data "in the clear." But that is about where the agreement ends.

In the next article in this series, I am going to dig deeper into these two forms of protecting data—both good—but not equal in value to a business person wanting to reduce costs and risk. These kinds of technologies

Much of the criticism [of the card payment industry] is well deserved, but much of it is **baloney** and **destroys the valid arguments** brought by petroleum retailers.

are the future of reducing risk and cost in data security. Solutions are coming. This problem need not be an endless drain on operating costs!

► **It is false that business owners are the major victims of data breaches.** Banks are the major victims (with the notable exception of purchases with counterfeit cards at unattended fuel pumps and unattended vending stations).

How the Banks Suffer

More baloney is the contention that somehow the banks that issue cards pass all of their losses from fraud on to the merchants. Many of us have had

our credit or debit cards stolen, and the crooks have run up fraudulent charges. With the exception of PIN-based debit transactions (yet another story), most people I know who have had this happen have had their money returned by their bank. Yes, it is inconvenient for the cardholder to have to report these fraudulent transactions, and it is inconvenient to go back to the recurring payees to give them the new card number. But it is the banks that have to take the charge against their earnings and suffer the loss of cash flow, estimated at \$2 billion to \$3 billion. They are also the ones who have to make the right guess as to whether to cancel a card that has been reported as breached and incur that cost vs. taking the risk of future fraud. The cost of the fraud and the reissuance of the card are borne by the banks—except when it comes to the unattended fuel pump or vending machine.

The argument of the card brands is that, years ago, they did not want to allow cards to be used at unattended fuel pumps because of the problems of drive-offs and skimming. The story goes that the major petroleum companies agreed they would take the risk of drive-offs and counterfeit cards because the benefits of pay-at-the-pump were so significant compared to the risk of losses. Of course, that was back in the day, when fill-ups were a fraction of what they are today.

Whether this background is true or not, it is true that, today, petroleum outlets take the brunt of counterfeit card losses and drive-offs. I agree this is a valid criticism, but there is also a solution to this problem.

More on these topics in future articles. ■