Statement of Robert Carr,
Chairman and CEO Heartland Payment Systems,
Before the Senate Committee on Homeland Security and Government Affairs

September 14, 2009

Good morning Chairman Lieberman, Ranking Member Collins, and Members of the Committee. My name is Robert O. Carr, and I am the Chairman and Chief Executive Officer of Heartland Payment Systems, Inc.

Let me begin by thanking the Committee for this opportunity to appear today to share our lessons learned and the steps we have taken and what more can and should be done to better protect our customers and the public from criminal hackers.

Our primary business is to provide bank card payment processing services to merchants. This involves facilitating the exchange of information and funds between merchants and cardholders' issuing financial institutions, providing end-to-end electronic payment processing services to merchants, including clearing and settlement, merchant accounting, and support and risk management.

When a consumer's card is swiped at one of our merchants, we forward the authorization request through Visa or MasterCard to the issuing bank, and then send their approval back to the merchant, allowing the purchase to be

made. In the following days we will receive payment from the issuer and pass it on to the merchant, and provide statements and accounting to the merchant. It is important to note that in the course of our payment processing business we do not receive cardholder social security numbers, addresses or unencrypted PIN data.

We were founded in 1997, and have since grown to represent over 3,100 employees, with over 1,200 W-2 salespeople across the nation. As of December 31, 2008, we provided our bank card payment processing services to approximately 230,000 merchants. Our total bank card processing volume for 2008 was almost $67 billion.

On January 20, 2009, we announced the discovery of a criminal breach of our payment systems environment. This attack involved malicious software that appears to have allowed criminal access to in-transit payment card data while it was being processed by Heartland during the transaction authorization process. This data is not required to be encrypted while in transit under current payment card industry guidelines.

We were pleased to hear the recent news about law enforcement's efforts to investigate and prosecute the individuals who make up the criminal syndicate that law enforcement believes is responsible for the Heartland breach and others like it. Albert Gonzalez, the alleged mastermind of attacks on TJX and other retailers including Barnes Noble, Office Max, and Dave & Buster, has pled guilty to charges in a 19-count indictment that includes conspiracy,

wire fraud, and aggravated identity theft charges. Mr. Gonzalez is also accused of having hacked into our system, as well as that of Hannaford Brothers, ATMs stationed in 7-11s and two other national retailers. It is reported that he was part of a team with eastern European criminals who have attacked a variety of U.S. companies.

We appreciate the efforts federal law enforcement are making to help stop these attacks and to bring these criminals to justice.

This has been a difficult experience for me and the company. We have taken a financial charge of approximately $32 million just in the first six months of this year on forensics, legal work, and other related efforts. Unfortunately, the company is involved in inquiries, investigations and litigation, so I cannot address in more detail the specifics of the intrusion. But I now know that this industry needs to, and can, do more to be better protected against the ever more sophisticated methods used by these cyber criminals, and I want to provide this Committee with some additional information about what Heartland is working on to try and prevent such intrusions in the future.

Let me note two key areas where Heartland is hard at work to address industry deficiencies.

First, industry and government can be better coordinated. The Financial Services Information Sharing and Analysis Center or FS-ISAC has been a great resource to a broad range of financial services companies facing this

threat but I realized that we could benefit from greater focus on the payment processing industry. In order to address the needs of payment processors, we recently formed, within the FS-ISAC, the Payments Processing Information Sharing Council (PPISC), a forum for sharing information about fraud, threats, vulnerabilities and risk mitigation practices.

At the PPISC, I shared with the payment industry members the malware which we discovered had been used to victimize Heartland. I did this once I learned that criminals were using this malware to attack our industry. I believe that by sharing this with others, including our industry competitors, we can better respond to very organized attackers.

Second, as reflected in the indictments of Mr. Gonzalez, a modus operandi frequently used by these attackers is to attempt to steal payment card data while it is being transferred in the clear - meaning it was not encrypted at the time. It is clear to me that we can address this vulnerability, and our internal technology team is continuing the development of a possible solution we call E3 - end-to-end encryption. I believe it is critical we implement this new technology, not just at Heartland, but industry-wide. We at Heartland believe we are taking the necessary steps to do so.

Heartland is working to deploy E3 to render data unreadable to outsiders from the point of card swipe. We plan to use special point-of-sale terminals, with Tamper Resistant Security Modules, TRSMs, to protect cryptographic secrets. We also plan to use special tools in

our processing network, Hardware Security Modules, to protect the cryptography associated with the card data.

Our goal is to completely remove payment account numbers of credit and debit cards and magnetic stripe data such as expiration date, service codes, and other data, so that it is never accessible in a usable format in the merchant and processor systems.

We are taking the necessary steps to implement this E3 solution, and I want to let the Committee know where our efforts stand.

1. **We are working with various suppliers on the technology to make E3 a reality and more ubiquitous. We are hopeful that these efforts will minimize the costs to merchants while not inconveniencing cardholders and yield a payment processing system that is more secure. We are seeking partners who will not use encryption as an opportunity to profit at our expense or that of our merchant customers.**

2. **We believe this potential solution needs to be implemented on an industry-wide basis. We have been working with the Accredited Standards Committee X9 (ASC-X9), to seek adoption of a new standard to protect card holder data in the electronic payments industry so all users can benefit from it. Ultimately, the Payment Card**

Industry Security Council must approve this standard and we are hopeful that it will do so soon.

3. **Once the standards are established, we will need the card brands and other financial institutions to cooperate and to be willing to implement on their side the encryption system our merchants are willing to use. We have been meeting with the card brands and the issuers and we hope we will be able to make progress on adoption by the card brands. However, without the cooperation of all of the card brands, the encrypted data would have to be decrypted --and thereby rendered less secure, prior to transmission to the card brands and their issuing banks. I am hopeful that each of the card brands will ultimately accept encrypted transactions from Heartland and other processors.**

We are working on these solutions, both technological and cooperative, because I don't want any one else in our industry or our customers or their customers - the consumers - to fall victim to cyber criminals. The attacks we face in this country potentially can have substantial consequences but we can learn from our experience and, while we cannot eliminate the risk, we can make cyber theft more difficult. I look forward to continuing to work to beat these criminals and appreciate your help as we continue this battle.

I welcome any questions Members of the Committee may have about my testimony today.

***** As the CEO of a publicly traded company I note that several of the statements in this testimony and that may be made in response to questions relate to events that are expected to occur in the future. The actual outcome of the future events I discuss is subject to risks and therefore, it is possible that the actual outcome of these future events may turn out to be different than the projected outcomes described.**