

**HEARTLAND PAYMENT SYSTEMS® COMMERCIALY LAUNCHES
STATE-OF-THE-ART PAYMENT CARD SECURITY TECHNOLOGY**

Designed to protect businesses and consumers nationwide, Heartland's end-to-end encryption safeguards credit and debit card account information from the moment of card swipe and through the Heartland network. With no additional transaction fees charged to merchants, E3 also reduces the cost of Payment Card Industry (PCI) compliance and the risk of being non-compliant.

2010 National Restaurant Association, Hotel-Motel Show — Chicago, IL — May 24, 2010 —

Heartland Payment Systems® (NYSE: [HPY](#)), the nation's fifth largest payments processor, has commercially launched its new, state-of-the-art payment card security technology — making it available to merchants and business owners nationwide. Heartland has spent more than two years developing and ten months beta testing and iteratively improving this end-to-end encryption technology — called E3™ — that is designed to protect cardholder credit and debit card data, rendering scrambled data useless to cybercriminals.

“Heartland leveraged its unique experience and knowledge to develop E3 — and made the financial investment needed to protect this sensitive information. Data is protected from the point of swipe and through Heartland's processing network — not just at certain points during the transaction flow,” noted Bob Carr, Heartland's chairman and chief executive officer. “We are making the highest degree of security available to every merchant regardless of size — without charging extra monthly or transaction fees and taxes. Additionally, because E3 does not allow card numbers to exist on or through a merchant's system or network — when combined with our Self-Assessment Questionnaire (SAQ) assistance services — E3 reduces the cost of PCI compliance and the risk of non-compliance for business owners.”

In today's world, protecting cardholder data is critical — for merchants and consumers alike. In the past two years, there were more than 650 reported breaches — a significant number considering many believe the majority of breaches are never reported. That number continues to increase daily because — in just a few brief seconds — from the time a customer swipes a credit or debit card to pay for a purchase until the transaction is complete, sensitive cardholder data can be vulnerable. If a business' system is breached without encrypted card data, the owner may be forced to pay steep fines and deal with the stress and cost of legal issues, business recovery and rebuilding customer confidence — and potentially the possibility of going out of business.

Heartland launches E3™ technology/2

To protect against this, E3 features layers of security using both software and tamper-resistant hardware — employing the Advanced Encryption Standard of encryption — AES — the most secure encryption algorithms available. E3 encrypts all Track 1 and 2 data from the card's magnetic stripe the moment it is converted from analog to digital data and enters a merchant's system as scrambled data ... never storing card numbers or passing them through the merchant's system or network.

Carr explains, "Centuries ago, cities across the world gave up on trying to protect themselves by making walls higher and thicker and more distant with moats. The enemy was always finding new ways to destroy the walls or circumvent the security efforts with Trojan horse attacks. We believe it is important to make card data indiscernible as it enters the payment cycle so if the firewalls are too weak, the enemy gains nothing of commercial value. We believe this is the enhanced security method the payment industry requires in today's world."

E3 is easy and cost-effective to implement. There are no changes to a merchant's daily routine or the speed of transactions — and no large equipment investment. Merchants purchase an E3 terminal or PC-based magnetic stripe reader/wedge* at — or below — the prices of standard, less-secure processing equipment on the market today. E3 devices include EMV/chip card technology capabilities — which may be coming to the United States — and the ability to update encryption technology.

Once the hardware is installed, merchants continue normal business operations — saving time and money because E3 automates the process of continually changing the encryption keys that convert sensitive account information to encrypted data. These necessary encryption updates are performed at no extra cost to business owners. In line with Heartland's goal of making adoption of state-of-the-art data security easy for business owners nationwide, Heartland also does not impose extra — unnecessary — monthly or transaction fees and "taxes" for E3 technology.

Additionally, Heartland helps the vast majority of merchants who use E3 complete the appropriate forms required for PCI compliance so they don't have to decipher the complexities by themselves. All business owners who accept credit and debit cards are subject to the standards of the PCI Council. The PCI Data Security Standards (DSS) define how sensitive data is stored, processed and transmitted. Most owners of small and mid-sized businesses are on their own to ensure they meet the more than 230 PCI standards.

Lastly, in the unlikely event of a data breach using E3, Heartland — with its "E3 End-to-End Encryption Warranty" — will reimburse a merchant's breach-related fines. If, during the warranty period on any particular Heartland E3 device, the device fails to prevent the unauthorized decryption of cardholder data on that particular device, and that failure is a result of a defect or error in Heartland's software or hardware, Heartland will pay the merchant the amount of compliance fines, fees and/or assessments the

Heartland launches E3™ technology/3

merchant pays to the card brands, issuing bank or acquiring bank. Heartland will also pay the merchant any costs he/she pays for a directly related forensic audit conducted by a PCI-certified Qualified Incident Response Assessor.

“Data security is mission critical in today’s world,” Carr concluded. “That’s why Heartland is taking a leadership role in making end-to-end encryption available and easy to implement for merchants large and small. While not a silver bullet, we feel this technology is a significant leap forward in helping the payments industry — as well as merchants and consumers — mitigate much of the risk of cybercrime. We have been working on this solution for two years now and are proud to be able to offer it to the stakeholders of the electronic payments world.”

For more information on this warranty and E3, access to a new payments security blog — “The E3 Blog” — and “*Card Payment Security for the Small Merchant*,” a white paper written by Mercator Advisory Group’s George Peabody — visit E3secure.com. To request photos of E3 hardware, contact LBrown@VaultCommunications.com.

###

** PC-based point-of-sale (POS) systems may require some integration by the POS provider.*

About Heartland Payment Systems

Heartland Payment Systems, Inc. (NYSE: HPY), the fifth largest payments processor in the United States, delivers [credit/debit/prepaid card processing](#), [gift marketing](#), [payroll](#), [check management](#) and related business solutions to more than 250,000 business locations nationwide. Heartland is the founding supporter of The Merchant Bill of Rights, a public advocacy initiative that educates merchants about fair credit and debit card processing practices. For more information, please visit HeartlandPaymentSystems.com, MerchantBillOfRights.org, CostOfABurger.com and E3secure.com.

Contacts

Leanne Scott Brown
Vault Communications
610.455.2742

LBrown@VaultCommunications.com

Nancy Gross
Heartland Payment Systems
888.798.3131 x2202

Nancy.Gross@e-hps.com

-more-

Forward-looking Statements

This press release contains statements of a forward-looking nature, which represent our management's beliefs and assumptions concerning future events. Forward-looking statements involve risks, uncertainties and assumptions and are based on information currently available to us. Actual results may differ materially from those expressed in the forward-looking statements due to many factors, including, without limitation, the risks that we may be unable to successfully develop and implement end-to-end encryption technology, the market may not accept the change from current encryption technology to end-to-end encryption technology and our end-to-end encryption may not work as intended. Information concerning other factors that could cause actual results to differ from the forward-looking statements set forth herein is contained in our Securities and Exchange Commission filings, including but not limited to, our annual report on Form 10-K, or our quarterly reports on Form 10-Q, as applicable. We undertake no obligation to update any forward-looking statements to reflect events or circumstances that may arise after the date of this release.