

**HEARTLAND PAYMENT SYSTEMS® INSTALLS E3™ TERMINALS AT 1,020 MERCHANTS
SINCE MAY 24 LAUNCH OF ITS END-TO-END ENCRYPTION SOLUTION**

Business owners take action to protect cardholder data, embrace ease of use of Heartland's end-to-end-encryption terminals, no-processing-fee approach to security and warranty

PRINCETON, NJ — June 24, 2010 — Heartland Payment Systems (NYSE: [HPY](#)), the nation's fifth largest payments processor, has installed its E3 terminals at 1,020 merchants since commercially launching the industry-leading end-to-end encryption technology on May 24 at the 2010 National Restaurant Association Hotel-Motel Show in Chicago. E3 technology is designed to protect cardholder credit and debit card data, rendering it useless to cyber criminals.

"There has been much talk in the payments industry about security solutions, and many have questioned how actively owners of small and mid-sized businesses would be willing to participate in the movement to secure cardholder data," said Bob Carr, Heartland's chairman and chief executive officer. "The fact that 1,020 merchants — most of whom own and/or operate these kinds of businesses and represent 118 different merchant category codes — have purchased E3 terminals in such a short timeframe demonstrates their commitment to protecting their establishments and their consumers. This is also a good indication of the widespread adoption of E3 by a diverse marketplace of merchants — and the engagement of our sales organization as 585 Heartlanders were responsible for these sales over the past month."

Heartland is committed to making the highest degree of security available to all merchants — regardless of their size. As such, the company doesn't charge additional processing fees or "taxes" for its state-of-the-art encryption equipment and software.

E3 terminals feature layers of security, employing both tamper-resistant hardware and AES (Advanced Encryption Standard) encryption, the most secure encryption algorithm available. E3 encrypts all Track 1 and 2 data read from the card's magnetic stripe or manually entered so merchants never have access to sensitive card data and never risk storing card numbers or transmitting them through their systems or networks. E3 also securely automates the process of changing the encryption keys that convert sensitive account information to encrypted data.

Heartland achieves 1,020 sales of E3 terminals / 2

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 magnetic stripe reader/wedge (for PC-based payment applications) at — or below — the prices of standard, less-secure processing equipment on the market today. E3 terminals include EMV/chip card technology capabilities — which may be coming to the United States.

“EMV will likely be coming to the US as a result of demand from young people wanting to use embedded NFC chips in their cell phones to make contactless payments,” Carr predicts. “An unintended consequence of smartphones is that they will serve as the most secure payment form factor: contactless EMV payments authenticated with a PIN. The risk of accepting electronic payments will come off the backs of the merchant community and be placed firmly with the consumer — just like with cash and PIN debit. Heartland is investigating contactless EMV as we strive to continually raise the bar on payment security. As such, we recommend business owners not upgrade to any new equipment that does not contemplate contactless EMV in the future.”

Keith Primeau, store owner of Bain's Deli and several other food establishments in the Philadelphia region, upgraded to E3 and was one of its first users.

“As the owner of several businesses, I recognize the importance of protecting my customers' data,” he commented. “E3 does that without hampering our operations — or charging extra fees. E3 also helps me address PCI (Payment Card Industry) compliance regulations. It has a lot of benefits for both me and my customers, yet is extremely simple to implement with no changes to our daily routine or speed of transactions.”

Steve Elefant, chief information officer at Heartland, concluded, “Additionally, merchants are protected by Heartland's “E3 End-to-End Encryption Warranty” which — in the unlikely event of a data breach using E3 — will reimburse a merchant's breach-related fines. All of these benefits offer significant relief to card-accepting businesses.”

For more information on E3 technology, 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 or HeartlandPaymentSystems.com.

###

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 and loyalty programs](#), [payroll](#), [check](#)

Heartland achieves 1,020 sales of E3 terminals / 3

[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

Nancy Gross
Heartland Payment Systems
888.798.3131 x2202

LBrown@VaultCommunications.com

Nancy.Gross@e-hps.com

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 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.