

**Heartland Payment Systems® and OpenBook® Bring
State-of-the-Art Data Security to Lodging Industry**

Integrated Offerings to Improve Secure Payment Services for Hoteliers

PRINCETON, NJ, & REXBURG, ID — April 6, 2010 — Heartland Payment Systems® and OpenBook® — a division of Yellowstone Hotel Systems — plan on delivering secure payments to the hotel and lodging industry by integrating Heartland's E3™ end-to-end encryption solution with OpenBook's property management software. Heartland is one of the nation's largest payments processors and the American Hotel & Lodging Association's official preferred provider of card processing, check management, payroll and tip management services.

This integrated offering is expected to enable hotels using OpenBook software to protect sensitive cardholder and payment account information with E3, a technology that is designed to provide the highest degree of data security in the marketplace. Typically, cardholder data is unencrypted — visible in clear text — as it leaves a hotelier's system, putting it at risk of being compromised in transit.

With an E3 terminal or wedge, data is instantly encrypted the moment a card is swiped. E3 uses what is believed to be the strongest encryption methods available to safeguard cardholder data at rest and in motion throughout the lifecycle of payments transactions ... from the moment of card swipe ... to and through the OpenBook system and Heartland's processing network ... to participating card brands. E3 is designed to offer full lifecycle protection, not merely point-to-point like most competing solutions, and render payment data useless in the event of a compromise.

"Cardholder and payment data is particularly vulnerable in the lodging industry where point-of-sale systems, shared systems among chains, wireless networks and a high volume of card transactions are typical," said Zack Paul, president and chief executive officer of OpenBook. "By addressing these unique compliance and data security needs, Heartland and OpenBook enable hoteliers to protect their businesses — and their customers."

E3 is expected to be widely available in the second quarter of this year. This joint offering is scheduled to be available in advance of Visa's mandated security regulations that require merchants to use a Payment Card Industry (PCI)-compliant payment application by July 1, 2010. Every business that accepts credit/debit/prepaid card payments — and stores, processes or transmits payment card data — must meet

the PCI Data Security Standards (PCI DSS). This means merchants cannot use an application that stores prohibited data elements, such as magnetic strip or PIN data.

E3 is intended to satisfy Visa's mandate and reduce the costs of PCI compliance as well as the risks of being non-compliant. Non-compliant lodging establishments may face penalties and costly fines that can range in the hundreds of thousands of dollars. E3 is designed to have a tamper-resistant POS terminal, magnetic stripe reader/wedge and other devices and software tools that will never store cardholder data on a business' system, which is expected to relieve the business of PCI card data liability. In the unlikely case of a data breach for a merchant properly using E3, Heartland will reimburse breach-related fines.

"E3 provides hoteliers with unparalleled security and business-continuity protection," said Dan Keegan, Heartland's director of technology alliances. "And, it does this without costing more. Unlike other technologies on the market, Heartland's E3 solution is robust and cost-competitive. Many encryption offerings come with 'junk' fees — like security, additional transaction and monthly fees. Heartland does not believe hoteliers should have to pay more to be secure. As such, Heartland does not charge more for its encryption and security services. Hoteliers simply purchase E3 wedges and terminals — which are competitively priced with existing hardware in the marketplace that does not feature security protection. There are no extra fees or taxes for the security."

For more information on E3 — and to download a just-released white paper, "Card Payment Security for the Small Merchant," written by George Peabody of Mercator Advisory Group — visit E3secure.com. To learn more about the Heartland/OpenBook solution, email OpenBookReferrals@e-hps.com. To request photos of E3 hardware, contact LBrown@VaultCommunications.com.

###

About Heartland Payment Systems

Heartland Payment Systems (NYSE: HPY), the 5th largest payments processor in the United States, delivers credit/debit/prepaid card processing, payroll, check management and payments 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.

About OpenBook

OpenBook specializes in property management, channel management, website design, online marketing and reservation assistance for all types of hotels across North America. OpenBook provides consistent revenue enhancements through integrated business solutions for the hotel industry. The company's

business model offers a complete arrangement of products and resources to streamline every component of the hotel management and online marketing process. For more information, please visit OpenBookit.com.

Contacts

Leanne Scott Brown	Nancy Gross	Scott Bailey
Vault Communications	Heartland Payment Systems	OpenBook
610.455.2742	888.798.3131 x2202	208.624.0374
LBrown@VaultCommunications.com	Nancy.Gross@e-hps.com	scott.bailey@yellowstonehs.com

Forward-Looking Statements

This press release may contain 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 card brands may not agree to accept encrypted data, 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 these factors is contained in the Company's Securities and Exchange Commission filings, including but not limited to, the Company's annual report on Form 10-K, or 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.