A HOLISTIC APPROACH TO MERCHANT PAYMENT SECURITY
WHY DEALERS AND ACQUIRERS ARE PIVOTAL TO SECURING THE MERCHANT PAYMENT ENVIRONMENT.

For the past fifteen years, navigating the payment security landscape has been a constant struggle for merchants. It’s kept small business owners up at night and tested the mettle of information security professionals at even the largest retail chains. Those sleepless nights have only been exacerbated by the recent transition to EMV.

Payment security used to be relatively easy for merchants. In the early days, before the PCI DSS (Payment Card Industry Data Security Standard), card brands took the brunt of payment risk. That left merchants free to explore new commerce channels and payment acceptance vehicles without fear of repercussion in the event of a compromise.

A string of high-profile breaches and the simultaneous introduction of new, often mobile payment applications fueled a flurry of activity at PCI Security Standards Council, including the fast evolution of the PCI DSS to its current v3.1, the advent and maturation of the PA-DSS (Payment Application Data Security Standard), P2PE (point-to-point encryption) standards, wireless security protocols, and PIN security standards.

Meanwhile, a myriad of mobile payment apps hit the market and Windows XP hit the end of its road. Just when it looked like things couldn’t get any more tumultuous, we were introduced to EMV. It’s enough to make any merchant’s head spin.
The reality, however, is that the payment security measures being enacted in the retail industry are necessary to thwart the threats we face. In 2014, 43 percent of respondents to a Ponemon survey said their company experienced a data breach. That’s up ten percent over the prior year. Sixty percent said their company experienced more than one data breach in the past two years, up from 52 percent of respondents in 2013.¹ And according to the National Cyber Security Alliance, one in five small businesses are victimized by cybercrime each year. A full 60 percent of those victims go out of business within six months of an attack.²

Today, merchants are no longer immune to the risks associated with a payment security data breach. In fact, the recent Cost of a Data Breach study from Ponemon Institute pegged the average cost of a data breach at $5.5 million, and the average cost per compromised record at more than $194.³ While these figures are somewhat inflated by the million+ compromised records in recent high-profile tier-1 breaches, even 500 compromised payment records approaches a $100,000 liability for a breached merchant.

Those statistics make it clear that merchants and their vendors who handle consumer card data are both at risk and a responsible party in mitigating that risk. It’s also clear that making sense of the payment security landscape is a daunting challenge, and that few retailers can do it alone. The first step on the merchant’s journey toward a secure payments environment is understanding that it’s not a plug-and-play endeavor; not PCI compliance, nor EMV, nor an anti-fraud service can stand alone to protect card data.

³http://www.databreachcalculator.com/GetStarted.aspx

In 2014, 43 percent of respondents to a Ponemon survey said their company experienced a data breach.

A full 60 percent of victims go out of business within six months of an attack.
Merchants of all sizes are bombarded with marketing from a burgeoning cottage industry of so-called payment data security solution providers. Much of this information is laced with misinformation that results in market confusion. To cut through the clutter, merchants must understand the role of the individual technology and service “fingers” that create a holistic approach to payment security:

- **EMV AUTHENTICATES THE CARD**
- **END-TO-END ENCRYPTION PROTECTS THE TRANSMISSION OF DATA**
- **TOKENIZATION PROTECTS THE STORAGE OF DATA**
- **PCI PROTECTS THE CONSUMER DATA**
- **ANTI-FRAUD SERVICES PROACTIVELY ADDRESS PAYMENT ANOMALIES**

It’s important for merchants to understanding the necessity of this comprehensive approach not just because it offers the best path to self-protection, but also because consumers are keenly interested in knowing they’re protected. When your consumers recognize that you accept EMV chip and PIN, or that secure mobile transactions can be conducted with ApplePay, for instance, their confidence in your brand grows. But peace of mind isn’t the only benefit of creating a secure payment acceptance environment based on the five elements noted here. Vendors that are proven enablers of these five fingers of payment security, and they should turn to their merchant acquirers for breach and PCI assistance programs. If your partners aren’t up to the task, it’s time to find new partners.
A fully integrated, feature-rich, well supported, and secure payments environment is foundational to a host of revenue-driving opportunities. Let’s explore just a few of them.

- **INCREASED FOOT TRAFFIC.** Today’s secure, integrated payment systems accommodate myriad payment types, including gift and stored value cards. Gift and stored value cards afford merchants the opportunity to gather consumer information, get to know their customers on a deeper level, and offer targeted promotions. Payments data—when it’s secure yet accessible—offers a trove of consumer information, which drives smart promotions that increase traffic.

- **HIGHER AVERAGE TICKET SALES.** Mobile and e-commerce enable consumers to order ahead, buy online, and in restaurant environments, order and pay from the table. Some restaurants are even including QR code-driven smartphone and tablet apps on wine, beer, and food menus to enable order entry from the table. When customers are afforded an opportunity to browse a menu before engaging an order electronically from their table, we’ve measured average ticket price increases between ten percent and fifteen percent. But, giving the consumer this power requires a responsible, secure payments environment.
• **INCREASED VELOCITY.** Mobile POS improves staff productivity and increases customer throughput. When lines form at the register, sales are lost to consumers who avoid the inconvenience of waiting. Mobile POS can shave critical time off the checkout process, especially during particularly busy periods, resulting in real money. In restaurants, the efficiencies gained by mobile POS allow servers to cover more tables and make more money for both the business and themselves. When orders are sent electronically to the kitchen, restaurants can offer higher levels of customer service with fewer servers. When consumers are given the opportunity to pay at the table on a secure device without handing over or losing sight of their payment card, they’re more confident to patronize the establishment again.

Your POS dealer, developer, and acquirer should be working congruously to help you understand how a secure, integrated payment acceptance environment dovetails with these benefits. They should also be working congruously to lift the burden of creating, deploying, and maintaining that environment from your shoulders. That’s especially important in the context of mobile POS.
It’s important to discuss mobile POS distinctly in the context of payment security, given the incredible rate of mobile device adoption in retail. The 2015 Mobile POS Software Market Share report from IHL pegged industry-wide mobile software installation growth at 41 percent from 2014 to 2015, and the consultancy anticipates there will be 3.6 million tablets in service at retail establishments by 2017.4 This proliferation of mobile devices introduces new security risks to the enterprise. The device itself must be secured, as well as its peripheral card reader. It must be EMV enabled. Its operating system must be maintained and updated.

On the other hand, enabling consumers to pay with their smart phones, or “mobile wallets,” is an equally compelling opportunity—consider that PayPal’s annualized mobile payment acceptance volume grew from less than $1 billion in 2010 to $46 billion in 20145—and considerably less daunting than mobile POS in an EMV-ready environment. Modern EMV readers are secure contactless payment enablers by design, and their dual authentication (password and biometric) security protocol is inherently secure. Still, merchants considering mobile POS and contactless payments should subject their plans to the aforementioned five fingers of security, ensuring they’re encrypting card data down to the device level and using tokenization in both cases.

*IHL pegged industry-wide mobile software installation growth at 41 percent from 2014 to 2015.*

5 https://www.paypal.com/webapps/mpp/about
There’s no question that the pace of change in payment security renders attaining a secure payments environment a moving target. That’s why it’s so critical that merchants turn to their retail systems provider ecosystems—their suppliers, QSA (qualified security assessor) accredited dealers, and acquirers—for help. Your support community should be your go-to resource for ensuring you’re not merely EMV ready or PCI compliant, but that the cardholder data you handle is tokenized and encrypted, and that your systems are actively looking for signals of fraud. Collectively, your retail solution providers have the capacity to create an integrated and secure payment acceptance environment that opens your business to the myriad of new payment vehicles consumers demand.

For more information on how a tight relationship with a merchant services provider of integrated payments can help, contact Vantiv Integrated Payments at 800.846.4472, or visit www.mercurypay.com. To get started on the path to a secure payments offering, contact Vantiv Integrated Payments at 800.846.4472, or visit www.mercurypay.com.
Vantiv, Inc. (NYSE: VNTV) is a leading payment processor differentiated by an integrated technology platform. Vantiv offers a comprehensive suite of traditional and innovative payment processing and technology solutions to merchants and financial institutions of all sizes, enabling them to address their payment processing needs through a single provider. We build strong relationships with our customers, helping them become more efficient, more secure and more successful. Vantiv is the second largest merchant acquirer and the largest PIN debit acquirer based on number of transactions in the U.S. The company’s growth strategy includes expanding further into high-growth channels and verticals, including integrated payments, ecommerce, and merchant bank.

Vantiv
4610 South Ulster St.
Suite #600
Denver, CO 80237

800.846.4472

SalesSupport@MercuryPay.com
ICS@MercuryPay.com