Card Data Security & Compliance

A Commerce Bank White Paper
About Commerce Bank

Commerce Bancshares, Inc. operates as a super-community bank offering an array of sophisticated financial products delivered with high-quality, personal customer service. The Company’s customer promise - We ask, listen and solve - is not just its brand, but also its corporate focus. With this platform, Commerce is continually building its long-term franchise while paying strict attention to asset quality and expense management. Commerce provides a full range of financial products to consumer and commercial customers including: lending, payment processing, and trust, brokerage and capital markets services. Serving its customers from 204 full-service branches and 406 ATMs in Missouri, Kansas, Illinois, Oklahoma and Colorado and commercial offices throughout the nation’s midsection, Commerce uses a variety of delivery platforms including an expansive ATM network, full-featured Online Banking and a central contact center.

Executive Summary

With the advent of the digital age, protecting customer data has become increasingly important. The liability of protecting sensitive data is continually increasing and has become more significant to entities handling this private information. The great majority of businesses want to eliminate their liability when processing sensitive data and seek further protective measures.
As a result, merchants who implement a layered security network with the following solutions will address virtually all known security vulnerabilities:

- P2PE (point-to-point encryption) and Tokenization
- EMV (Europay, MasterCard, Visa), also known as chip card
- PCI DSS compliance (Payment Card Industry Data Security Standard)

The objectives of Commerce Bank’s White Paper are to:

- Explain why EMV protects cardholder security, not a merchant’s
- Describe why encryption and tokenization are effective tools in preventing a data breach
- Clarify why merchants should implement additional precautions to minimize an e-commerce fraud shift
- Summarize the security benefits of merchant compliance with the PCI DSS standards

Commerce Bank’s White Paper will portray how the implementation of a layered security approach offers premier protection against hackers seeking sensitive payment information. The combination of encryption and tokenization, EMV and PCI DSS compliance implemented in a merchant’s payments processing network may ultimately protect a merchant’s payment data from being compromised.

A Layered Security Approach: It’s Your Business

As a result of increasing competition, ever-growing payment system regulations and new opportunities for fraud and loss, many banks have implemented stronger payment security standards for merchants. After the Target breach in 2013 left an estimated 70 million customer records compromised, a greater emphasis by merchants to implement stronger data security technologies has exploded. As a result, retailers of all sizes are focusing more resources and emphasis on security technologies found in P2PE and tokenization. While many merchants may already comply with the PCI DSS and/or have deployed an EMV solution, security alternatives address other weaknesses in point-of-sale (POS) networks that can be exposed by black hat hackers. Businesses are now more interested than ever in eliminating the liability of possessing sensitive data, whether at rest or in transit. As such, more business owners are seeking further protective measures, leading to a layered security approach in their POS networks and cardholder data environments.

With the liability shift behind us now, EMV acceptance technology is certainly a popular subject matter in the U.S. payments industry, however, it is not top of mind for merchants who are more interested in deploying a P2PE solution first. EMV strengthens a card’s authenticity and virtually eliminates counterfeit fraud losses but a well-informed merchant also knows that EMV alone will not improve their own security position. Those retailers understand the real security benefits come in protecting card data during and after the transaction, and encryption is the answer. Encryption is a method of scrambling data so it becomes useless if compromised. To make it useful again, it must be decrypted, which occurs by a technology service provider managing a unique encryption key to “unlock” the scrambled or encrypted data. Furthermore, some retailers will choose to retain
payment data for various business reasons and to do this while eliminating PCI scope and liability, tokenization is necessary. A “token” is generated by a token service provider who replaces the actual card number for future use in instances like recurring payments, chargeback management and returns processing. Only the token service provider can generate a uniquely created token record, usually a one-for-one match to a cardholder account number and merchant number. This token cannot be paired any other way, which also makes it useless if compromised. For card-present merchants, the implementation of both encryption and tokenization can substantially reduce exposure risks to the black hat hackers, contrary to many of the merchant names we’ve seen in headlines who had not invested in these extra security measures prior to their breach event. For card-not-present merchants (e.g., catalog, direct marketing, phone order and e-commerce), card data should be traversing through a secure or encrypted channel already. When using these channels, tokenization becomes the added security layer option.

EMV technology introduces a new means to protect the payments industry from proliferating counterfeit fraud at the POS and the U.S. region is migrating at the pace of the market’s demand. Increased levels of EMV card penetration, along with the liability shift, are naturally stimulating an increase in merchant adoption. In preparation for the migration, numerous communication campaigns on the subject have been delivered through various forms. To comply with the EMV liability shift (October 1, 2015), a merchant’s POS device must be capable and enabled of accepting these card products. When a merchant is presented an EMV card and they do not have chip reading capability, the merchant bears responsibility for counterfeit fraud disputes. To reiterate, while EMV transactions protect the card and cardholder from fraud, it does not protect the card data for the merchant. From a merchant’s data security standpoint, EMV transactions are no different than a magnetic stripe read card. Unless this clear text card data is protected through encryption at the point of interaction, it can be compromised through illegal hacking. Being EMV ready ultimately protects the merchant from chargeback liability, not from an intrusion of their network.

At this point, we’ve navigated through the security benefits of P2PE and tokenization and have a clearer understanding in the value of an EMV implementation. Now, let’s shift the focus to PCI compliance. The PCI DSS evolved from the major card brands’ security programs, creating the first version of the standard in December 2004. Since then, each card company has mandated merchant compliance to this minimum level of security. Validating PCI compliance applies to any entity that stores, processes, transmits and/or controls or could impact the security of cardholder data. As a merchant, you are likely very familiar with the requirement to comply with these standards and provide evidence through annual validation. Annual compliance validation is only a periodic screening of your security health; however, PCI compliance and effective risk management is accomplished through continual policy and controls implementation, not a once-a-year validation. While other security compliance standards apply specifically to hardware, security technologies and payment applications, it is the PCI DSS requirement that provides a minimum security structure for these entities to protect card data during and after a transaction. Without this framework and the card companies’ data security programs mandating the compliance, the card payments system would surely not be as secure. As a business, not securing payment card information can result in an unnecessary compromise or data breach, leading to forensic investigation fees and card company fines passed on by your acquiring provider. Most importantly, the damage to your brand, reputation and integrity with your customers is at stake. Is any of this worth the risk?
As we evolve further into a digital age, securing customer data has become more critical. The liability of possessing unprotected sensitive data has become more meaningful and targeted directly towards the entities handling the data, resulting in proactive measures to mitigate the exposures. Furthermore, we know EMV will greatly reduce the effectiveness of fraud in card-present networks, consequently leading to a fraud shift to other payment channels. As a result, a greater emphasis in fraud monitoring will become more important to card-not-present merchants. For card-present businesses, the ultimate protection from a data compromise points squarely at a layered security approach by combining the benefits of implementing PCI compliance, P2PE, tokenization and EMV. The ultimate objective is to plan, develop and implement a secure acceptance network through the use of security technologies and compliance together, not singularly. The evolution of these security and compliance options is evident, leading merchants to rely heavily on vendor solutions and their merchant provider.

Businesses today are investing more research, time and resources into protecting their environments where sensitive data may reside. Securing a POS environment occurs through effective design and implementation of multiple security technologies and compliance. The deployment of one solution is certainly not enough and merchants are seeing the substantial benefits in a layered security implementation instead. At Commerce Bank, we believe the layered security approach is a highly effective method to minimize unnecessary harm to the brand, reputation and integrity of any business. All businesses can benefit from the value these solutions provide. Many merchants have already taken the necessary steps to secure their POS environment by leveraging the Commerce Bank relationship. We fully welcome and appreciate the effort to add security in the payments industry by offering solutions and consulting services to all of our merchants. After all, it is your business.

To learn more about this topic, contact our Merchant Support Center at 1-800-828-1629. Commerce Bank has the experience and resources to help you through it all.