Editorial

The Future of PCI

PCI London, January 2018

Adam M. Sommer, Vice President, Security Standards & Compliance

Payment Gateway Services

How it all began...

It is hard to believe that it has now been 12 years since the launch of the PCI Security Standards Council (PCI SSC). In just over a decade, the PCI SSC, Mastercard and our fellow Payment Brand Members, as well as the wider community of Participating Organizations, Affiliate Members, Strategic Members, Assessors and our Board of Advisors have accomplished more than anyone could have imagined for securing payment card data. I am even more excited about our collective future, focused on technologies that will successfully devalue and desensitize payment card data and ultimately ensure our industry is the hardest target possible for hackers.

Just a few short years ago, the PCI SSC had less than a handful of security standards. Today, there are 12 PCI Security Standards. As an industry the focus has traditionally been on the PCI Data Security Standard (PCI DSS), which is the original and first PCI Security Standard and an excellent source of good, basic security requirements. In its brief lifetime, the PCI DSS has transformed security for payment card data, formalizing a set of foundational security requirements, providing for a professional population of Qualified Security Assessors, and driving compliance programs such as Mastercard's Site Data Protection Program.

Countless compromises have been prevented, detected, or responded to because of the PCI DSS – the security impact on our industry has been priceless. That said, the PCI DSS is about protecting cardholder data, whereas our future for payment security will be focused on devaluing and desensitizing that data in the first place.

The simple fact is that criminals want payment card data.

The data we use as a payments industry is valuable to organized crime, and as long as we continue to store, process, and transmit this valuable data we as an industry will be a popular target for hackers. Ultimately, we win against this crime by devaluing and desensitizing our data in the first place. This objective can be achieved through technology solutions designed to remove the Primary Account Number (PAN) from storage, processing and transmitting, especially in the merchant environment. Working together, technologies such as EMV, Point-to-Point Encryption (P2PE), and tokenization, offer an excellent solution.

What's new?

The newest PCI Security Standards are critical in achieving our objective of devaluing and desensitizing payment data. The PCI Token Service Provider Standard (PCI TSP) provides security requirements to properly secure EMVCo Payment Token vaults and their environments. The PCI Point-to-Point Encryption (P2PE) Standard provides a set of security requirements for P2PE solutions, and in its newest version, also provides requirements for individual components of solutions. The P2PE Standard is also supported by a PCI SSC program, including a public listing of validated

P2PE Solutions. Published in late 2017, the newest standards, PCI 3DS Core and PCI 3DS Software Development Kit (SDK), provide security requirements for the latest EMVCo 3DS specifications which help prevent unauthorized card-not-present (CNP) transactions in a secure way. These are just a few examples of how the latest PCI Security Standards are focused not solely on protecting payment data, but also achieving our collective objective of devaluing and desensitizing the payment data in the first place.

The benefits of these security solutions are not limited to devaluing and desensitizing data; because these solutions reduce risk to the payments ecosystem, they also provide a lower compliance requirement. Tokenization is an excellent example of this benefit. The PCI SSC, through publically available FAQs on its website, has stated that both EMVCo Payment Tokens as well as Payment Account Reference numbers (PAR) are not in-scope for the PCI DSS as neither meets the definition of Account Data. In simple terms, this means entities that only store, process, or transmit EMVCo Payment Tokens and/or PAR are exempt from PCI DSS validation.

Mastercard's compliance program, the Site Data Protection (SDP) Program, is also encouraging the use of these security technologies through lower compliance requirements, in complete alignment with the strategy of devaluing and desensitizing payment data. Less than a year ago, the SDP Program was updated to add incentives for both EMV and PCI Council listed P2PE solutions, including allowing merchants to participate in the Validation Exemption Program (VEP), effectively exempting merchants that use either of these technologies from validating their PCI DSS compliance to Mastercard.

Our future is focused on devaluing and desensitizing the data.

Payment security and PCI compliance have always been a top priority for Mastercard Payment Gateway Services. Its feature rich and high capacity global gateway delivers secure, reliable and costs effective solutions for merchants of all sizes, across all industry sectors. Our platform has been designed to significantly reduce merchants' PCI compliance scope by combining a range of unique solutions like omni-channel tokenization (facilitating secure 'click & collect' functionality), fully accredited Point-To-Point Encryption and a selection of flexible integration options such as Hosted Payment Pages.

Working together as an industry we can, and will, defeat the criminals who are compromising payment data. While the PCI DSS offers the most effective set of security requirements to protect payment data while stored, processed or transmitted, our future is focused on devaluing and desensitizing that data in the first place using technologies offered by EMV, Point-to-Point Encryption, and tokenization. Successfully removing sensitive data from our ecosystems, specifically from the merchant environment, will help ensure the payment card industry is a very unattractive target for criminals; after all, criminals cannot steal what we do not have.