Protecting your past, present and future cardholder data with Commidea and Foregenix

By Ian Rutland and Benj Hosack

Since the PCI SSC was formed in 2004, merchants have been making great leaps forward in securing the way they handle cardholder data. Commidea was founded in 1992, predating the existence of PCI DSS, yet one of its key drivers has always been to make payments secure for merchants. The company has enjoyed a long working relationship with Foregenix which specialises in discovering and neutralising ‘rogue’ or unprotected cardholder data residing on a merchant’s system. Despite the progress being made by merchants in achieving PCI DSS compliance, both companies acknowledge that there are two less publicly discussed but equally as important threats concerning data compromise. Past data most commonly refers to information that has resided on a retailer’s system for a number of years. This is often left unprotected and can contain the ingredients necessary to build a clone card. Future data does not currently reside on a retailer’s systems but will face threats from increasingly well funded, organised and intelligent criminals.

Past data
Many merchants have been processing card transactions before the formation of the PCI DSS council and almost all predate wide use of data encryption. Most are likely to have a large amount of unprotected, or legacy, cardholder data residing on their systems. Benj Hosack - “A staggering percentage of the people whose systems we investigate following a data breach were unaware that they were actually storing the data which was lost. All of our findings support the card schemes’ guidance of ‘if you don’t need it, don’t store it’, as far too much unnecessary data is stored by most businesses. Using products like FScout Enterprise helps to ensure that all stored past data is identified and secured.” FScout Enterprise searches for and detects unprotected cardholder data. It is a rapid, accurate, scalable solution and is ideal for carrying out regular checks for leaked cardholder data stored on servers, desktops and laptops, as well as confirming scope for a company’s PCI DSS compliance program. Ian Rutland - “Products such as Commidea’s Ocius Sentinel point-to-point encryption payment solution are now available and actively ensure that merchants do not store future data on their systems. However, there remains a backlog of data which is highly vulnerable to attack. In addition to market leading encryption methods, Ocius Sentinel also uses Tokenisation to ‘replace’ this sensitive data. A unique code is assigned to specific cardholder data as it is processed. This allows the merchant to continue to use this information for other business applications without retaining the sensitive cardholder data the criminal desires. Commidea recommends a dual-pronged approach using solutions such as FScout Enterprise and Ocius Sentinel to protect past and future data.

Present data
Over the past seven years, protection of cardholder data in the face-to-face retail environment has become more sophisticated, however, so too have attempts to obtain it illegally. As a result the financial and time costs of maintaining PCI DSS, considered substantial by most large firms, can be crippling for many smaller businesses. Ian Rutland - “Commidea looked at the face-to-face payment processing environment and saw a real need for a solution that placed data security at its very core. Ocius Sentinel was created to address this by reducing both the cost and time burden of achieving and maintaining PCI compliance for merchants. Ocius Sentinel is the UK’s first Payment Application Data Security Standard (PA-DSS) approved solution which employs point-to-point encryption. Cardholder data is encrypted at the point of card entry and not decrypted until it arrives inside the secure environment of Commidea’s PCI DSS Level 1 certified processing infrastructure, prior to transmission to the acquiring bank. As a result all sensitive card data is effectively removed from the merchant’s system.

Future data
The future threats to cardholder data are largely unknown. However, what is certain is that they will become more sophisticated and more targeted. Ian Rutland - “We have seen this pattern emerging already. Whereas 10-20 years ago data criminals would commonly work alone, now we face collective, organised and intelligent gangs of data criminals funded and run in much the same way as a legitimate business.” Benj Hosack - “PCI DSS enables a business to identify its assets and provides clear guidelines on how to protect those assets (cardholder data). The threat of a data compromise will not end, although once a business achieves and maintains PCI Compliance, the threat of a data compromise will be significantly reduced. Attackers are more inclined to focus their efforts on weaker, less secure systems than spending significant time and effort on more secure systems. As a result, using systems and tools such as Ocius Sentinel and FScout, merchants are able to significantly reduce the risk of data compromise in their business.” Ian Rutland - “The best way to maintain optimum protection is to have a point-to-point encryption solution in place like Ocius Sentinel which proactively protects cardholder data and to combine this with regular scans as a security buffer against any unlikely data leaks.”

The good news for merchants is that regular and effective use of Ocius Sentinel and FScout will ensure there is considerably less to worry about. For further information on Ocius Sentinel, contact marketing@commidea.com.

For all Foregenix enquiries, please contact info@foregenix.com.