Smart Card Alliance Brief
January 24, 2014

Large Scale Payment Data Breaches Highlight Need for U.S. Card Issuers and Retailers to Move More Quickly to Smart Chip Payment Technology

U.S. loses $5 billion a year to card fraud

Recent large-scale payment data breaches are contributing to the significant card fraud problem in the U.S. The U.S. loses $5 billion a year to card fraud, accounting for about half of global card fraud despite only generating about a quarter of the total volume of purchases and cash[1]. This is due to the ease with which criminals can obtain credit and debit card account information from insecure magnetic stripe cards and create counterfeit cards. As a result, the U.S. is quickly becoming a fraud target, as most of the rest of the world (80+ countries) has already made the move to chip-based payment cards. To combat this growing fraud problem, U.S. card issuers and retailers need to move more quickly towards adoption of smart chip payment technology.

Smart chip payment technology, also referred to as EMV, is an open-standard set of specifications for smart card payments and acceptance devices. The specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. Smart chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards.

Smart chip cards significantly enhance payment security in four areas:

First, the chip card includes a secure microprocessor chip that stores payment card data placed there by the issuer during the personalization process and can perform cryptographic processing during a payment transaction. This payment data is stored securely in the card's chip and is impervious to access by unauthorized parties. The microprocessor chip is used instead of the magnetic stripe during each EMV payment transaction and helps to prevent card skimming and card cloning, the most common ways magnetic stripe cards are compromised and used for fraudulent activity.

Second, in a chip card transaction, the card is authenticated as being genuine, and the transaction generates a dynamic data element or cryptogram that is authenticated online or offline, according to issuer-determined risk parameters.

Third, even if fraudsters are able to steal account data from chip transactions, this data contains a one-time use cryptogram and does not include other data needed for magnetic stripe transactions. This means that the data cannot be used to create a fraudulent transaction in an EMV chip or magnetic stripe environment.

As described above, each of these transaction security features helps to prevent fraudulent transactions. In addition, the inability to create counterfeit cards with stolen chip card data will greatly devalue the data retailers accumulate from payments transactions, making this data less valuable for criminals to steal.

And lastly, chip cards can also address card-not-present (CNP) fraud, with cardholders using their smart chip cards and individual readers to authenticate Internet transactions.

While the U.S. is one of the last countries to migrate to chip cards, the major payment brands American Express, Discover, MasterCard and Visa have announced their plans for moving to a smart chip-based payments infrastructure in the U.S. Acquirers have met the April 2013 deadline for processing chip-based transactions and have started deploying EMV to their merchants as part of the normal upgrade path. Next, card issuers and retailers will face a fraud liability shift. After October 2015, the party that has made investment in EMV deployment will be protected from financial liability for card-present fraud losses. Despite this date drawing near, progress in terms of chip card issuance and installation of EMV chip-compliant acceptance terminals remains slow. While some merchants and issuers have started towards chip readiness, the estimated 10 to 15 million chip cards issued to date[2] represent less than 2 percent of U.S.-issued cards.

As breaches like Target continue, consumers and the media are becoming more aware of the vulnerabilities of magnetic stripe cards and will begin to demand more secure chip cards and retail locations where they can make chip-based payments. Now is the time for card issuers and merchants to move much more quickly towards a chip-based payments infrastructure.

The Smart Card Alliance provides many resources for the payments community to accelerate their path to chip payments and acceptance. The Alliance's www.EMV-Connection.com is a dedicated website where all industry participants can get information about the fundamentals of chip cards and payments and assistance with planning their migration to the technology. The Smart Card Alliance recommends reviewing the white paper, "Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?" as a first step.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S., Latin America, and the Caribbean. For more information please visit http://www.smartcardalliance.org.

[1] Nilson Report, 2013

[2] According to industry sources