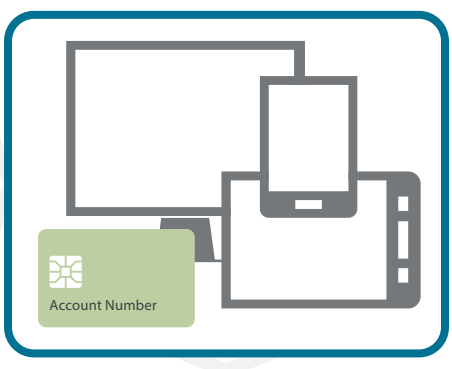
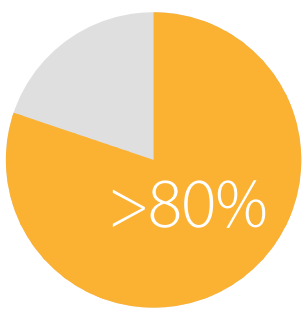
U.S. Payments Security Evolution and Strategic Road Map

Security Landscape

The U.S. electronic payments security landscape is changing more quickly than ever before due, in part, to new and emerging payment technologies. These technologies help enhance the consumer experience while proactively addressing increasingly sophisticated fraud methods. While fraud is at or near industry-wide historic lows, payment data continues to be an attractive target for criminals who desire the financial opportunity of using or selling stolen payment account data.



Over 80% of U.S. payment fraud caused by electronic cardholder data theft.



Payment Fraud and Underlying Risks

There are two primary types of payment fraud that result from data breaches:

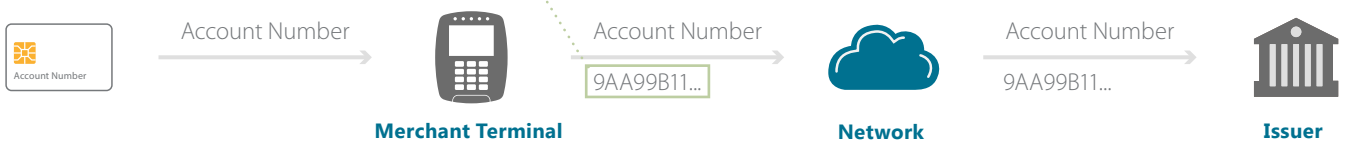
- Counterfeit fraud occurs when sensitive payment account data is stolen and used to create a counterfeit payment card that is used at the point of sale.
- Card-not-present (CNP) fraud occurs when payments data is stolen and then used for fraudulent transactions in remote-access payment channels, such as eCommerce and phone/mail orders.

Comprehensive Approach to Payments Security

While chip cards will help reduce counterfeit fraud at the point of sale, there remains a need to address the card-not-present space through additional technologies. Simply put, there is no one silver bullet. Securing the payments ecosystem requires continuous investment and innovation in new technology including chip, tokenization, and point-to-point encryption. An industry-wide approach using complementary technologies reduces the risk of payment account data being stolen and makes data less valuable if stolen.

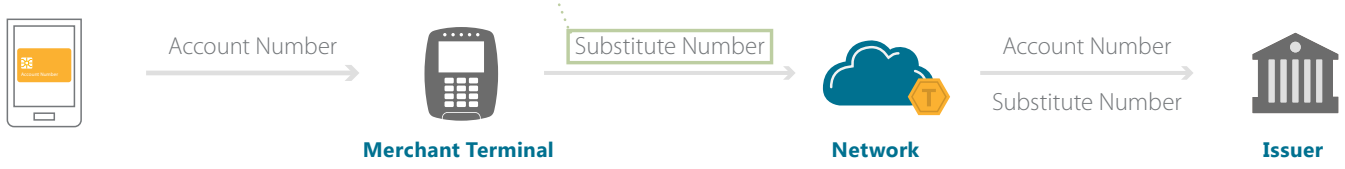
Chip

A small computer chip in the card generates a one-time use code for every payment transaction. This code is different every time a transaction is made, and the card issuer can verify if it's the correct code. If the card data and the code are stolen, the information cannot be used by criminals to create counterfeit cards and commit fraud.



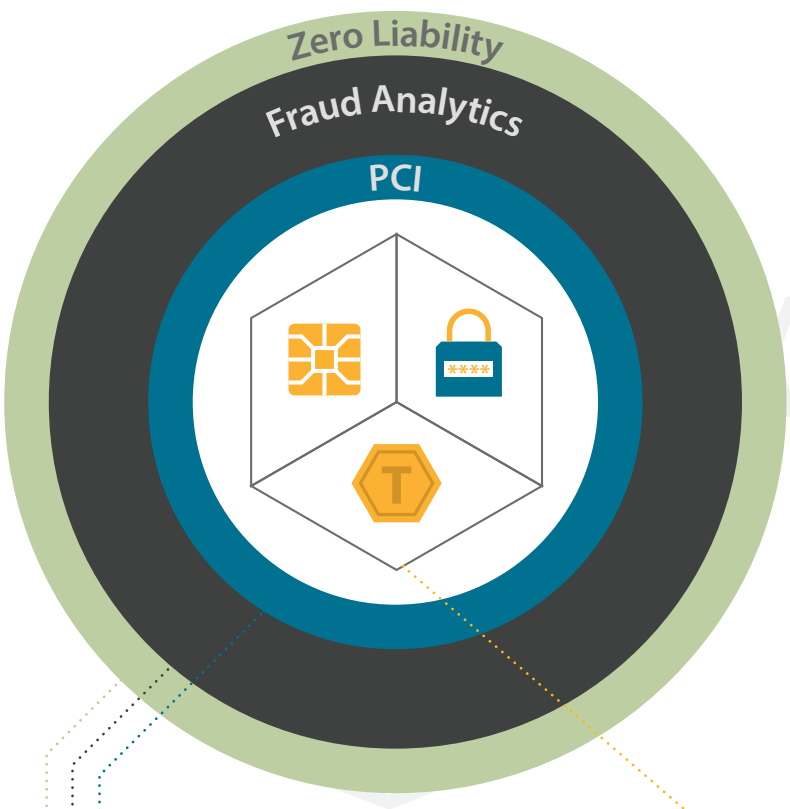
Tokenization

Tokenization replaces your account number with a unique substitute number. If this substitute value is stolen, the criminal's ability to use it for fraudulent transactions is limited.



Point-to-Point Encryption

Point-to-Point Encryption is the process of converting payment data into unreadable data from the time the card is swiped, tapped or dipped at the merchant terminal until the transaction is complete.



Interconnected Technologies

Chip, Tokenization, and Point-to-Point Encryption are being deployed in combination with fraud analytics and are supported by industry standards, such as Payment Card Industry (PCI) Data Security Standards. Together, these technologies can significantly reduce payment fraud in the U.S., and around the world, and help protect and reduce risks to the U.S. payments industry from cyber security threats.

PCI
Secures data at the point of transaction

Fraud Analytics
Predictive analysis that helps identify fraudulent transactions

Zero Liability*
Cardholder not responsible for unauthorized charges

Chip
Uses a one-time code to prevent counterfeit fraud

Tokenization
Replaces the account number with a unique substitute number to prevent card-not-present fraud

Point-to-Point Encryption
Secures data during transmission

The Payments Security Taskforce (PST)

In order to ensure that the industry successfully addresses the threats of today while anticipating the challenges and opportunities of the future, the U.S. Payments Security Taskforce (PST) was assembled in early 2014. The taskforce includes a diverse group of participants in the U.S. electronic payments industry including payment networks, banks of various sizes, credit unions, acquirers, retailers, point-of-sale device manufacturers and industry trade groups.

Among the participants are American Express, Bank of America, Capital One, Chase, Citi, Credit Union National Association, Discover, First Data, Global Payments Inc., Independent Community Bankers of America, Kroger, National Association of Federal Credit Unions, Marriott, MasterCard, Navy Federal Credit Union, Sheetz, Shell, Subway, US Bank, Vantiv, VeriFone, Visa Inc., Walgreens, and Wells Fargo & Company.

Looking To The Future

Members of the Payments Security Taskforce (PST) have collaborated to publish a strategic road map for U.S. payments security and are committed to driving progress against the road map.

U.S. Payments Security Evolution and Strategic Road Map

December 11, 2014

To view the Roadmap and learn more, please visit:

visa.com/pst or **news.mstr.cd/1vH7POt**

**Zero Liability differs across payment networks. Please reference zero liability policies for each card brand: American Express (https://www.americanexpress.com/us/content/fraud-protection-center/types-of-fraud.html); Discover (https://www.discover.com/credit-cards/member-benefits/security-center/keep-secure/understand-fraud.html); MasterCard (http://www.mastercard.us/zero-liability.html); Visa (http://usa.visa.com/personal/card-benefits/credit-card/zero-liability.jsp)*