Santander Commercial Banking

November 2017

Protecting Your Company Against Card Fraud

Many companies want to provide an array of card payment options to attract more clients and grow their businesses. But while expanding your company's payment options offers greater convenience to your clients, it can also put you and your clients at risk of card fraud. If you are currently—or considering—employing a full range of card payment options, it's important to know the fraud risks and protections of both card-present and card-not-present transactions.

Chip Cards and Card-Present Fraud

The **E**uropay, **M**astercard®, and **V**isa® (EMV®) cards, also known as chip cards, have long been the global card payments standard. However, the U.S. has only recently adopted chip technology. This lapse has made American cardholders a prime target for fraudsters. Barclays reported in early 2015 that, while the U.S. held only 24% of worldwide card volume, it accounted for a disproportionate 45% of the world's card fraud.[1]

The good news is that over the past two years, there has been a steep uptick in the use of EMV-chip credit and debit cards in the U.S. The key reason is that chip card transactions are more secure than traditional, magnetic stripe card transactions. Because the microchip in a chip card generates a dynamic one-time use code, it's nearly impossible for fraudsters to reuse the data to create counterfeit cards.

Another reason for chip card growth is the shift in liability for fraudulent card transactions. According to U.S. rules on card-fraud liability, any party—merchant or card issuer—that is not using EMV technology assumes the liability for any fraud that occurs in a card-present transaction. As a result, most merchants have upgraded their terminals to the new technology rather than risk potential liability.

Over the past two years, chip card issuance, usage, and acceptance have grown steadily. According to Visa[2], in June 2017:

- **62% of its credit and debit cards in circulation were chip cards.**
- **Visa chip payment volume was $58.4 billion, up 109% y/y.**
- **2.3 million merchant locations accepted chip cards, representing 50% of U.S. storefronts.**

The growing acceptance of chip cards has had a significant impact. Visa reports that merchants who upgraded their terminals to accept chip cards experienced a 58% decrease in fraudulent purchases between March 2016 and 2017.[3]

Heightened Risk of Card-Not-Present Fraud

While the rise of EMV usage in the U.S. has precipitated a significant decline in card-present fraud, it has not eliminated the threat of payment fraud altogether. As with any type of crime, fraudsters continuously look for vulnerabilities that can be exploited. Now that chip cards have increased protections against card-present fraud, fraudsters are concentrating their efforts on card-not-present transactions, such as those made online or by phone.

Countries that have accepted chip cards for a longer period of time have already experienced this phenomenon. When the U.K. shifted to chip cards, card-present fraud fell by 56%, but card-not-present fraud rose 79% over a three-year period.[4] Similarly, e-commerce card fraud in the U.S. rose 33% in 2016, following the transition to EMV technology.[5] Fortunately, there are measures that companies can take to reduce their risk of exposure in these types of transactions.

Protecting Against Card-Not-Present Fraud

Card-not-present fraud is a serious concern for merchants, given the steady rise in electronic and mobile commerce volume. According to eMarketer, U.S. retail electronic commerce sales will pass the $450 billion mark in 2017, and will continue to grow at double-digit rates through 2020.[6]

The following are some tips for merchants who want to capture their share of the growing electronic commerce market, but who also want to ensure that they are adequately protected against the increasing threat of card-not-present fraud:

- **Check with your company's gateway vendor to ensure that all transactions are subject to identity verification.** The Address Verification System (AVS) is an anti-fraud tool designed by bankcard processors to aid in the detection of suspicious credit card transaction activity. AVS matches billing address information provided by the cardholder with the cardholder's billing address on file at the credit card issuing bank. The processing network then sends an AVS response code indicating the results of the match to the payment gateway. Based on the AVS rejection settings, the transaction is accepted or rejected.
- **Confirm you have end-to-end encryption software on your virtual terminal.** Utilizing encryption and tokenization technology on your virtual terminal protects payment card data by removing it completely from the merchant environment. As a result, your point-of-sale (POS) system never holds the actual card numbers from the transactions you process. This software replaces card data with a randomly assigned number, called a "token," eliminating the need for merchants to store the data. In doing so, it shifts the burden of protecting the cardholder data from you to the software provider and allows the "token" to be used for other business and sales functions such as returns, sales reports, and analysis.
- **Place limits on online transactions.** For example, you can limit the number of times a cardholder can be declined each day for failing to provide proper authentication information to initiate a transaction. You can also prevent computer IP addresses from initiating multiple transactions from different cards with different names.

New Choices for Your Business

If you are looking to grow your company by diversifying your range of in-store and online payment options—while also protecting against various types of payments fraud—please contact your Santander Bank Merchant Services representative, who can provide solutions and advice to meet your payment needs.

[1] "Credit card fraud and ID theft statistics," Nasdaq, September 16, 2015
[2] Visa Chip Card Update: June 2017
[3] Visa Chip Card Update: June 2017
[4] "As Big Banks Prep for EMV, Fraud Relief Remains Far Off," American Banker, March 18, 2015
[5] "In wake of EMV switch, US e-commerce fraud soars," Finextra, March 30, 2017
[6] "UPS Raises Prices for Key Holiday Weeks," eMarketer, June 19, 2017

Santander

This information has been provided by Santander Bank, N.A. for general information purposes. Statements contained herein do not constitute endorsements or guaranties of information provided by the Institutions referred to herein, the Trade Portal or Trade Club. Nothing contained herein creates any client, advisory, fiduciary or professional relationship between you and Santander Bank, N.A. Neither Santander Bank, N.A. nor any affiliate, in connection with the information herein, is engaged in rendering auditing, accounting, tax, legal, advisory, consulting or any other professional service or advice to you. Finally, the information contained herein should not be considered a substitute for your independent investigation and your sound technical business judgment after consulting with your own professional advisors.Santander, Santander Bank and the Flame Logo are trademarks of Banco Santander, S.A. or its subsidiaries in the United States or other countries. All other trademarks are the property of their respective owners.