Avoiding Credit Card Fraud at Your Business – Part 2

According to the Nilson Report, U.S. credit card fraud accounts for more than $4 billion in losses in 2014 alone. For businesses that accept card-not-present (CNP) and eCommerce payments, fraud is expected to increase even more. But, there are steps you can take to protect your business.

Both Europe and Canada have realized a significant increase in fraudulent activity at CNP and eCommerce businesses since EMV was implemented. For this reason, MSP Consulting is recommending businesses take additional steps to avoid fraud. In Avoiding Credit Card Fraud, Part 1, we explained a few simple ways to help reduce the risk exposure at your business. In part 2, we will build upon the steps and precautions outlined in our first article on the subject.

The best precaution to take when trying to avoid fraud is to know your customers. Many times this may not be practical, especially for eCommerce sales, however below are steps that should be considered to help decrease fraud exposure. MSP Consulting can discuss any of the options below and help determine what fraud avoidance methods may be most beneficial to your business.

Require Card Code (CVV)
The CVV code is the three or four digit security code on the cardholder's credit card and is used for chargeback and fraud protection. If required, the code entered by the cardholder must be correct or the transaction will be declined. Providing the CVV code with the sale helps to confirm the cardholder is actually the person authorizing the sale, which may be most useful for eCommerce sales. It is important to remember the CVV Code cannot be stored for future use - this is against federal law. Providing the CVV does not impact your processing fees.

Require Billing Street Address (Address Verification System – AVS)
When the billing address is provided, the Address Verification System can confirm if the address provided matches the billing address on file with the credit card Issuing bank. A positive AVS response can help confirm the cardholder is in fact the person authorizing the sale. When used with the CVV code, statistics show that fraud can be reduced significantly for eCommerce payments. At a minimum, CNP businesses should always require the billing zip code with each sale as this will help reduce processing fees.

Shipping to a Verified Billing Address
To maximize fraud avoidance and increase chargeback protections, merchandise must be shipped to the billing address that was verified. Shipping to an address other than the billing address will void chargeback protections. This is a common fraud technique.

Require Signed Proof of Delivery
For shipped merchandise, always obtain proof of delivery via certified mail. The signature of the recipient will aid in chargeback disputes, however, it alone will not ensure winning the dispute.

International Sales
Businesses must be especially cautious with international sales. Since address verification is not supported in most countries (AVS is only supported in the US, Canada and the United Kingdom), a business cannot verify the billing address on file using AVS. As such, international sales and shipping are subject to the business' own risk. For this reason, it is encouraged to only do business with known international customers. Other recommendations include calling the cardholder's phone and investigating if the cardholder is valid prior to making the sale.

Require User Credentials for eCommerce
For eCommerce sales, requiring customers to register and create a unique user ID and password can help a business manage fraud. Customer activity can be tracked and "questionable" accounts may be deactivated. For repeat customers with accounts in good standing, less scrutiny is needed on their sales, while new customers can be monitored and even limited in their activity. For instance, a repeat user in good standing may be permitted to ship to a non-verified address - new users may only be permitted to have the option to ship to their verified billing address, until they build trust with your business.

Use of CAPTCHA on Websites
This acronym stands for "Completely Automated Public Turing Test To Tell Computers and Humans Apart." An unusual name, but a very useful tool in protecting websites from bots aimed at hijacking the website. Bots are used by fraudsters for many unscrupulous purposes, including testing stolen credit cards, so all eCommerce website should be protected with this useful tool. More details about CAPTCHA can be found at http://www.captcha.net.

Fraud Scoring Systems
One of the more robust fraud management techniques are fraud scoring systems. These tools can be implemented to "rate" each transaction to determine the risk level of a sale and aid businesses in identifying and avoiding high risk sales that may turn out to be fraud. Fraud scoring systems use a wide range of input to critique a sale, including IP filtering, geography filtering, sales thresholds, proxy detection and even social media information.