Your Guide to *E-Commerce Fraud Prevention*

TSYS®

E-Commerce Merchants Often Pay a Higher Price for Fraud

A survey of fraud experts conducted by the *Association of Certified Fraud Examiners* (ACFE) found that organizations around the world lose an estimated 5 percent of their annual revenues to fraud.[1] The opportunities for retail fraud increase as new access channels and payment methods — including mobile wallets, the EMV® rollout and digital channel applications — are introduced.[2]

In consumer-facing retail, fraud typically falls into the following categories:

- Fraudulent and/or unauthorized transactions
- Fraudulent requests for a refund or return bounced checks
- Lost or stolen merchandise, and the costs associated with redelivering these items, which can result in carrier fraud.

Be Proactive to Reduce Your Risk

Reducing your risk of e-commerce fraud requires a proactive approach. Your best defense is a strong offense. Merchants should take necessary precautions to protect confidential data. This will protect their business from a data breach and their customers from identity fraud. Even the smallest data breach can cause an average merchant crippling financial losses and damage to their brand's hard-earned reputation.

"Reducing your risk of e-commerce fraud requires a proactive approach because your best defense is a strong offense."

The Soaring Cost of Fraud and Data Breach

Falling prey to cybercrime can lead to devastating financial burdens. Fraudulent unauthorized card use in card-not-present (CNP) transactions can lead to the following financial losses:

- The cost of chargebacks by card issuers
- The expense of issuing credits or reversals to defrauded customers
- Revenue loss from a damaged reputation and eroded consumer confidence

An ounce of prevention is worth a pound of cure. The *2016 LexisNexis® True Cost of Fraud℠ Study* sheds light on the high cost of online fraud and merchants' struggle against its onslaught.[2] **The study reveals that there needs to be more awareness of the value of investing in a multi-layered approach to fraud mitigation. It also concludes that the right solution can justify the upfront costs as greater accuracy yields more positive results on the bottom line.**

"Remember, if an order seems questionable, trust your instincts and check it out."

Here are some terms you should know and guidelines that can help you to reduce the risk of e-commerce fraud and help keep your website safe:

- **PCI Compliance:** This refers to the Payment Card Industry Data Security Standard (PCI DSS) established by the Payment Card Industry Security Standards Council (PCI SSC) to help protect sensitive consumer data from being compromised. Merchants must be able to certify that the way they store, process and transmit cardholder data is in compliance with PCI standards.
- **PCI-Compliant Secure Tokenization:** This is done through your payment processor as a secure way to store customer card data. Your processor generates secure tokens for each customer and customer account that you can submit whenever a transaction occurs.
- **Address Verification Service (AVS):** This is used to verify the identity of the person attempting the transaction by checking the billing address provided by the user with the address on file at the credit card issuer. AVS can be used on all domestic transactions to ensure the addresses match.
- **CVC2 and CVV2 Verification Numbers:** These are found on most major credit cards to provide an additional level of security. They are a 3 or 4-digit number printed on the back of Mastercard®, Visa® and Discover® credit or debit cards and on the front of American Express® Cards. Merchants should ask for the code in all CNP transactions.
- **3-D Secure® authentication tools:** 3-D Secure stands for "Three Domain Secure" – the domains being the acquiring bank (retailer's bank), the issuing bank (the cardholder's bank) and the infrastructure that supports the 3-D Secure protocol. The 3-D Secure service is more commonly recognized by its various commercial names: Verified-by-Visa™, Mastercard SecureCode™, American Express SafeKey®, JCB International J/Secure™ and Discover/Diners ProtectBuy℠.
- **Enhanced Fraud Protection Services:** Automated transactional risk scoring can help you identify and prevent potentially fraudulent purchases by flagging customizable triggers.
- **Fraud Notices:** When prominently displayed on your website and order forms, fraud notices can deter online fraudsters.
- **Common Sense:** This is an invaluable tool. Remember, if an order seems questionable, trust your instincts and check it out. It's also a good idea to save voicemails and emails, and to record all customer calls. It's also helpful to call or email the customer to verify key data before confirming their order.

Best Practices for E-Commerce Security

The following list of best practices can help you protect your e-commerce website, your livelihood and your reputation.

- **Choose a secure e-commerce platform** with an administration panel that is only available on an internal network and completely removed from public-facing servers.
- **Use a secure connection for online checkout and make sure you are PCI compliant.** Use strong SSL [Secure Sockets Layer] authentication for web and data protection to authenticate the identity of your business and encrypt the data in transit.
- **Don't store sensitive data**. It is strictly forbidden by the PCI Standards.
- **Require strong passwords.** Longer, more complex logins will make it harder for criminals to breach your site from the front end. Help customers to help themselves by requiring a minimum number of characters and the use of symbols or numbers in their passwords.
- **Set up system alerts for suspicious activity.** This includes multiple and suspicious transactions coming through from the same IP address, multiple orders placed by the same person using different credit cards, phone numbers that are from markedly different areas than the billing address, and orders where the recipient's name is different than the cardholder's name.
- **Layer security.** Start with firewalls, an essential aspect in stopping attackers before they can breach your network and gain access to your critical information. Then add extra layers of security to the website and applications such as contact forms, login boxes and search queries. These measures will help ensure that your e-commerce environment is protected from application-level attacks like SQL (Structured Query Language) injections and cross-site scripting (XSS).
- **Provide security training to employees.** Employees need to know they should never email or text sensitive data or reveal private customer information in chat sessions as none of these communication methods is secure. They also need to be educated on the laws and policies that affect customer data and be trained on the actions required to keep it safe. Use strict written protocols and policies to reinforce and encourage employees to follow mandated security practices.
- **Use tracking numbers for all orders.** Issue tracking numbers for every order you send out to combat chargeback fraud. This is especially important for retailers who drop ship.

- **Monitor your website regularly.** Use a real-time analytics tool to observe how visitors are navigating and interacting with your website in real time to help you detect fraudulent or suspicious behavior. You can even arrange to receive phone alerts for any suspicious activity, allowing you to act quickly and prevent suspicious behavior from causing any damage. Your e-commerce site hosting company must regularly monitor their servers for malware, viruses and other harmful software with a plan that includes at least daily scanning, detection and removal of malware and viruses on the website.
- **Make sure your website host is backing up your site and has a disaster recovery plan.** Protect yourself against the loss of valuable information in the instance of power outage, hard drive failure or even a virus. To make sure your site is properly protected, back it up regularly (or make sure your hosting service is doing so).
- **Perform regular PCI scans.** Regular quarterly PCI scans by an approved scanning vendor can lessen the risk that your e-commerce platform is vulnerable to hacking attempts and help maintain PCI compliance. If you're using third-party downloaded software, stay on top of new versions with security enhancements. A few hours of development time today can potentially save your entire business in the future.
- **Patch your systems.** Patch everything immediately on the day a new version is released. This includes the web server itself, as well as any third-party code such as Java, Python, Perl, WordPress and Joomla!®, which are often targets for attackers. It's critical to install patches on all software such as web apps, X-cart, osCommerce and ZenCart®.
- **Consider a DDoS protection and mitigation service.** DDoS (Distributed Denial of Service) attacks are increasing in frequency, sophistication and range of targets. E-commerce sites can turn to cloud-based DDoS protection and managed DNS services to provide transactional capacity to handle proactive mitigation and eliminate the need for significant investments in equipment, infrastructure and expertise.
- **Consider breach protection.** TSYS® offers a unique data breach security program that's specifically designed to help merchants meet the expenses resulting from a suspected or actual breach of payment card data. This assistance plan reduces monetary exposure in the event of a cardholder data compromise. It is designed specifically to meet the expenses resulting from a suspected or actual breach of credit card data from a business.

In conclusion, knowledge is one of your best defenses against e-commerce fraud – by following these best practices you can help protect your business, your revenue and your customers from fraud.

[1]The 2016 ACFE Report to the Nations on Occupational Fraud and Abuse
http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

[2]2016 LexisNexis® True Cost of Fraud℠ Study, May 2016
http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx