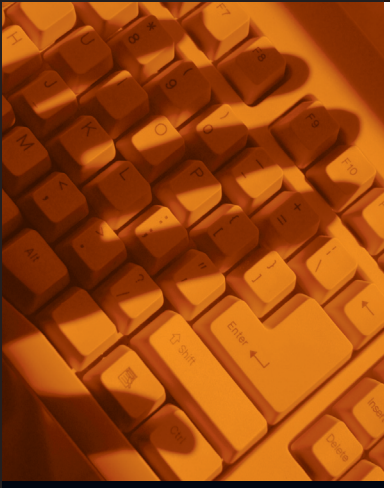

SAFETECH™
Fraud and Security Solutions

Proactive Fraud Prevention for Online Retail

No matter what your industry, fraud is a part of it. Did you know that merchants are paying $139 billion annually in fraud losses alone, according to the 2010 LexisNexis True Cost of Fraud Study? So how do you retain legitimate sales while preventing fraudulent transactions? Before a transaction is even completed, merchants should have in-house fraud prevention tools already in place, determining both the location and device identification of your customers. Partnering with the right payment processor is also an important factor as they most likely possess the in-house capability to route your transaction data through an internal risk-inquiry system for analysis and verification of any custom rules you have implemented. Educating yourself on the various different types of fraud, fraud prevention strategies and best practices is also an important strategy in your fight to combat fraudsters and fraudulent activity.

A list of the most common types of online fraud, fraud prevention strategies and a brief description of each can be found below.

Types of Fraud Present in Online Retailing

Malware Attack – Malicious software (trojans, botnets, worms) that has the purpose of stealing identities or data from unsuspecting businesses or consumers. Malware can be used to collect financial data, contact data or passwords to commit fraudulent purchases or set up fraudulent lines of credit.

Pharming – Systematic redirection of a consumer's Web browser to a fraudulent Web site. That Web site may have the look and feel of the actual merchant Web site, but is designed to capture the consumer's information for malicious use.

Phishing – Fraudulent e-mails sent to consumers disguised as a credential verification request from the merchant. Similar scams exist that involve text messaging (SMSishing) and voice mail scams (vishing).

Amateur Fraud – Unsophisticated fraudsters use stolen consumer information to make one-off purchases on merchant Web sites. These amateur fraudsters tend also to use similar shipping address information and common data elements (such as billing address and customer name information).

Card Testing – The use of a merchant's Web site to actively test the validity of stolen credit cards. This is a common scheme where a low ticket item or service is purchased in an effort to test whether or not the stolen card is still active.

Fraud Prevention Strategies

Set Purchase Limits – Limit the amount that can be spent on the Web site in a 24-hour period and/or the total number of a given product that can be purchased in that same time period. Fraudsters hit hard and fast and will try to max out the stolen credit cards they have.

Scan Overnight Shipping Requests – Be cognizant of requests for overnight shipping, including the items selected for shipment. High-ticket items with overnight shipping requests can be a primary source of fraud, especially when coupled with the purchase being made late in the merchant's business day.

CHASE™
Paymentech

SAFETECH™
Fraud and Security Solutions

Pay Attention to the Time of Day – The adage "nothing good ever happens after midnight" applies to e-commerce as well. Pay particular attention to the location of the consumer (use IP mapping/ proxy piercing technology) and be wary of orders placed late at night or early in the morning.

Ask a Secret Question – Offer a secret question/ answer at the time of registration and specify it to prompt periodically when the user attempts to log into their account. This can help prevent account takeovers.

Manage Password Management – Force users to change their passwords periodically to fight phishing scams.

Notify User of Account Changes – Merchants should send an e-mail notifying their users about any changes made to their account.

Employ Velocity Checks – Control the number of cards that can be used by a registrant and the total number of orders accepted in a given day. Be wary of any consumer who attempts to use three or more cards to make a purchase in a short period of time.

Auto Accept/Reject – Utilize fraud technologies capable of comparing data elements in real time. For those orders where further review is required, consider using a solution that allows for secondary review rules that can call out to external phone numbers and/or address validation services.

Minimize Manual Review – Keep manual review to a minimum through the use of real-time fraud detection tools. Leverage tools that provide greater visibility into order data, purchase history and geolocation information to prevent the acceptance of fraudulent orders.

Use Proxy Piercing/IP Geolocation – Prevent fraud with technologies that are able to pierce proxy or other identity obscuring attempts by the consumer. The merchant can see the actual location of the purchaser by state or country relative to the information provided during the purchase.

Apply Device Fingerprinting Technology – Fingerprinting devices associated with online purchases can provide tremendous visibility/insight into fraud patterns. Multiple computers placing multiple orders are generally detectable by multi-layer device fingerprinting technology.

Implement Multi-Merchant Order Linking – Software designed to look at over 200 data elements while comparing that information against other order data in real time. Fraudulent-use patterns can be tied back to other orders that would otherwise go unnoticed by the human eye.

Adopt Dynamic Risk Scoring – Deploy a solution that provides a real-time assessment of the validity of a purchaser that includes constant rescoring of the order billing information compared against any new or historical transaction information. The order billing information may be any combination of the following: name, card number, billing/shipping address, IP address, e-mail, phone number, device ID/location, velocity and purchase patterns.

Maintain Positive and Negative Lists – Protect good customers from unnecessary scrutiny and place known or suspected "bad" customers on a negative list. Pay particular attention to changes in core data elements associated with "good" customers and follow up with a review.

Apply Custom Business Rules – Merchant-specific business rules created and stored in virtual Software-as-a-Service-based environment can be highly predictive of fraudulent patterns when used in conjunction with many of the "core" fraud tools described above.

It is also just as important to have the right procedures in place to help you prevent fraud from the onset. Following is a list of order acceptance best practices to equip you with the tools you need to protect your cardholders from the moment they enter their payment information.

Did you know that merchants are paying $139 billion annually in fraud losses alone?

CHASE™
Paymentech

SAFETECH™
Fraud and Security Solutions

ORDER ACCEPTANCE BEST PRACTICES

- Establish an automated screening process. Rules-based screening of incoming orders will speed up the decision process by approving good orders up front and screening out those requiring manual review.
- Provide consultative customer service and accommodate dissatisfied customers. This can reduce chargebacks. This could include offering refunds (partial or full) or discounts.
- Do not allow customer service representatives latitude in identifying possible fraud. Use a specific set of questions designed to verify customer information as well as formal fraud tools. In other words, remove the "human element" from the equation and focus on the facts.
- Deter amateur fraudsters by using basic industry-standard fraud prevention tools, such as Address Verification Service (AVS) and Card Verification Numbers (CVNs).
- Perform regular chargeback analyses. Pay attention to the various chargeback codes and group by category. Not all fraud chargebacks are classified as identify theft (i.e. services/ merchandise not received).
- Do not offer "suspected fraud" order status messaging – it can give fraudsters the intelligence they need to continue stealing from your Web site.
- Accept every order (except those with credit card declines).
- Cancel those deemed to be fraudulent by sending an e-mail to the e-mail address provided during the order process.
- Provide a customer service telephone number to rejected customers. Legitimate consumers who are falsely identified as fraudulent will tend to pick up the phone to complete their purchase.
- Fraudsters who attempt to call can typically be identified by asking for the billing and card verification number data used to make the purchase and validating that information against formal fraud prevention measures used internally.

Ultimately, the potential for fraud is present anywhere data is entered, stored or transacted. Having the right fraud tools in place and partnering with a payment processor that can assist you in providing a secure space for your payment transactions can significantly reduce your risk of fraud – protecting both your bottom line and your professional reputation.

Before a transaction is even completed, merchants should have in-house fraud prevention tools already in place.

CHASE™ Paymentech