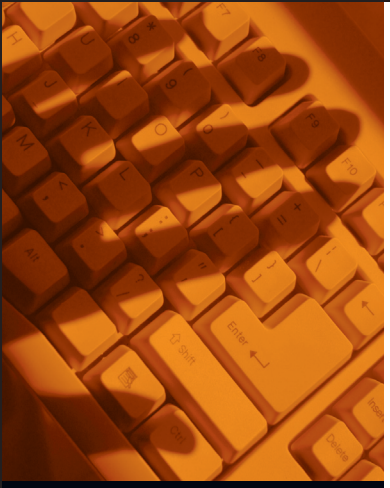
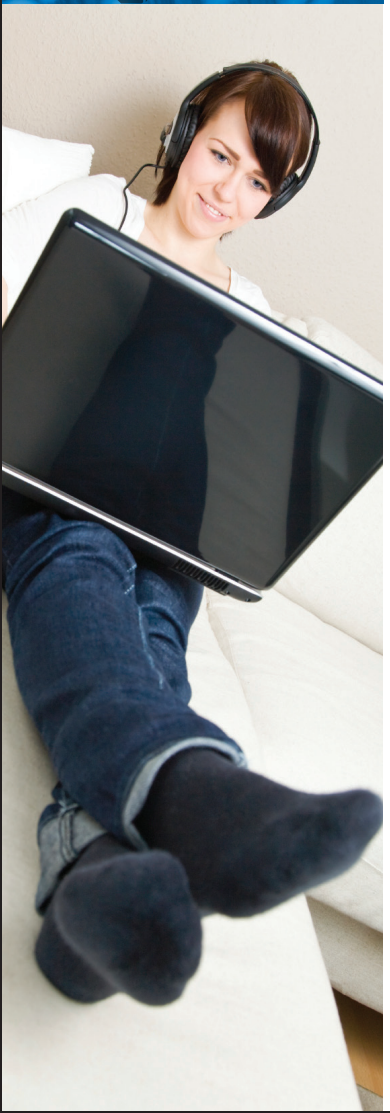


SAFETECH™
Fraud and Security Solutions



Strategies to Protect Your Gamers and Your Revenue

Creating and running a massive multiplayer game hosting thousands of online gamers is far from child's play. In fact, host companies expose themselves to many challenges when accepting electronic payments. While online payments are a necessary part of conducting a gaming business, it is important to understand how fraud can impact bottom line revenue. Fortunately, Massive Multiplayer Online (MMO) providers have ways to help defend themselves from payment fraud, including solutions specifically designed to help protect MMOs and their users – keeping everyone safe when connecting to, and paying for, their favorite online worlds.

Educating yourself on the various different types of gaming fraud, fraud prevention strategies and online 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 gaming fraud, fraud prevention strategies and a brief description of each can be found below.

Types of Fraud Present in Online Gaming

Questing – Performing tasks within the game to earn virtual currency. Fraudsters will "quest" in key areas of the game to earn virtual currency as quickly as possible. Virtual currency can then be used to buy virtual goods (for sale later) or bartered for real money.

Pharming – The 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 credit card details for malicious use.

Phishing – Use of fraudulent e-mails sent to game users disguised as a credential verification request from the game itself. This is a very common method for identity takeovers.

Power Leveling – Bot-like play (robotic play) in an effort to increase the status of a user profile to rapidly obtain virtual currency or sellable virtual goods quickly. This is one of the most common fraudulent activities that may include several fraudulent users of the same credentials from different parts of the world.

Virtual Currency Accumulation – Laundering, currency inflation and rapid transfers of currency are all issues with virtual currency offerings. There are sweatshops throughout the world with individuals paid to quest, farm or power-level in an effort to accumulate more virtual wealth.

Design Fraud – Creation of high value/high-risk products for fraudulent sales (ties to inflation) and/or low-value (under the radar) products that can be sold in high quantities. There are two types of design fraud: individual designers looking to defraud the system and users looking to sell the goods for real world money.

Account Takeovers – Seizing of account credentials with the focused goal of draining the account of all sellable virtual items or virtual currency.

Stolen Card Usage to Buy Virtual Currency – Stolen cards are frequently used to buy virtual currency within the game. This is a much quicker

CHASE™
Paymentech

SAFETECH™
Fraud and Security Solutions

way to accumulate wealth (depending on the game settings) and is a pervasive problem in the virtual world.
A. Money laundering – high degree of real-world currency transferred through PayPal® or prepaid debit cards.
B. Fraudsters buy across many accounts to spread out their activities.
C. Fraudsters buy products and sell to others.
Pop-up Bartering Web Sites – This is a very common fraud method where fraudsters will create Web sites offering virtual currency or virtual products to buyers from all over the world. Many of these sites originate in China where little regulation exists. These sites pop up fast, look legitimate and close down as fast as they are created.
Overpriced Virtual Goods Scams – Careful consideration must be given to the virtual economy including supply and demand, appropriate pricing for products sold within the game and purchase activity. Items priced too high (for example) are usually a sign of fraud.

Fraud Prevention Strategies

E-mail Validation – use e-mail validation as a way to verify the registration information provided at the time an account is created. Force the user to respond to an e-mail activating their registration. This will aid in preventing systematic account creation by fraudsters.
Secret Question – Have a secret question that can be used at the time of registration and is periodically used when users attempt to log in to their account. This will help prevent account takeovers.
Password Management – Force users to change their passwords periodically to fight phishing scams.
Account Change Notification – Game providers should take great care in notifying their users about any changes to their account (via e-mail notification).
Control Virtual Currency Purchase Limits by Account – Control/limit the amount of virtual currency that can be purchased in a given day by a specific user.
Set Limits – Limit Special offers (discounts, virtual currency, products, etc.) and who can participate.
Use Captcha Technology – Use of a virtual "word" displayed at the time of registration does a good job of cutting down on systematic account creation. This practice is common in the social networking, gaming and event sales spaces.
Velocity Checks – Control number of cards that can be used by a registrant, purchase limits within the game and frequency of visits at certain times of the day.
Monitor Friends/Buddy Lists – Fraudsters tend to associate with other fraudsters. Monitor friend lists to look for patterns of negative activity. Merchants can often find "fraud rings" by looking at known associates.
Auto Accept/Reject – Do not refuse a registration for the game without human review.
Manual Review – Keep manual review to a minimum through the use of real-time fraud detection tools. Do not exceed 10 percent review as an average.
Usage Patterns – Pay particular attention to usage statistics and how users are interacting with each other. Fraud patters can become evident through careful review of activity within the virtual world itself.
Use Proxy Piercing/IP Geolocation Technology – A lot of virtual fraud can be prevented by utilizing technologies that are able to pierce proxies or anonymizing attempts by the user. The merchant can see the geolocation of the user in question by city, state, country or region relative to the information on file as part of the original registration.
Use of Device Fingerprinting Technology – Use of technology to fingerprint devices associated with registration, use and virtual currency/product purchases can provide tremendous visibility/insight into fraud patterns. Device ID used in conjunction with proxy piercing technology can generally peer beyond botnet "slave" computers to determine the location of the command and control the computer behind the fraud. Multiple computers using similar login credentials can be quickly detected and stopped with this technology.

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

CHASE™ Paymentech

SAFETECH™
Fraud and Security Solutions

More importantly, valid consumers who have "enslaved" devices will not be rejected from making legitimate purchases.

Use Multi-merchant Order Linking – Technology 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. Fraud "personas" can be established linking one or more data elements across multiple transactions over time.

This persona concept views transaction history as a whole looking for fraudulent patterns instead of focusing on individual transactions.

Dynamic Rescoring – Use of technology that provides an initial assessment of the fraudulent nature of a user/purchase, including constant rescoring of the original data based on any new orders/elements passed through the system. This type of solution allows gaming companies visibility into changing fraud trends within the game including account takeovers. What appears good one day may turn bad the next.

ONLINE GAMING BEST PRACTICES

- Have a clear description of the game or service offered.
- Have a clear, prominent description of the terms of sale and refund policy – including length of subscription, virtual currency/credit purchase limits, billing intervals, etc.
- Avoid chargebacks by working with the users. Many cases involve children using their parent's credit card and customer service personnel can educate parents on card usage within the game or games.
- Instruct customer service representatives to follow a scripted process for verifying customer information.
- Use address Verification Service (AVS) to eliminate amateur fraudsters with simple AVS checks in the U.S.
- Implement Card Verification Numbers (CVN) as they can be a reasonable detector of amateur fraud on global transactions.
- Perform chargeback analysis by paying attention to the various chargeback codes and group by category. Not all fraud chargebacks are classified as identify theft (i.e., product/service not as described).
- Clearly display the company/game name on the consumer's credit card statement. Companies who attempt to anonymize themselves tend to have a higher degree of chargebacks.

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

Ultimately, the potential for fraud is present in any world – real or virtual. The right fraud tools and payment processing partnership are key assets. They can assist you in providing a secure space for your online gamers and significantly reduce your risk of fraud – protecting both your bottom line and your professional reputation.

CHASE™ Paymentech

PCNP-065 0211 ©2011, Chase Paymentech Solutions, LLC. All rights reserved.