Digital goods merchant guide to combat fraud.

As a digital goods merchant, you're always looking for ways to expand your online business opportunities. Whether you develop downloadable software, host online video games, or sell content such as MP3s, videos, or e-books, you're vulnerable to fraud. Check out our best practices to combat online fraud.

Screen Account Activities

Be mindful of drastic changes in customer activity or account inconsistencies.

Account inconsistencies
Typically, a user will have only one account accessed through one IP address or several similar IP addresses that use the same cookie. Watch out for suspicious activity such as one IP address or cookie accessing many different user accounts or one user account being accessed from multiple IP addresses or cookies in different geographic locations.

Similar naming conventions
Fraudsters often attempt to send many payments to a string of similarly named user accounts.

Multiple account access
We recommend disallowing multiple simultaneous account access as fraudsters often log in to an account at the same time to split tasks among themselves and move money as quickly as possible. Legitimate players on the other hand, rarely have this need.

Drastic changes in activity
If the frequency or amount of payments for an account increases significantly, it may be a sign of fraudulent activity.

Tips to fight online fraud

Track customers

Log customers' IP addresses whenever they sign in. You can also create a payment history for each customer and record all incoming payments including email and IP addresses. Based on the record, you can then track fraudulent activity and create a way to immediately lock out customers or IP addresses in conjunction with possibly fraudulent activities.

Set limits

Limit the number and the total amount of payments you'll accept from one account per day, week, or month to reduce your exposure to fraud. Allow only one PayPal account to fund a user account. Reason

being, accepting multiple sources of funding opens a window for fraudulent behavior. You could also limit the sending country or the geo-location of the buyer's IP address to expected countries.

Investigating suspicious activity

If suspicious activity occurs, your system should have a way to limit changes to account profiles and inventory, while you conduct an investigation.

Suggestions for Online Video Game Merchants

1. **Require users to set up an account and provide profile information to participate in your games.** Validate this information before a user can play and limit usage of gaming account if the user is not verified.
2. **Limit each player to one game account**. This helps limit the length of the audit trail of any given user's activity for ease of tracking.
3. **Track new player activity closely**. Develop a profile for new players and monitor how much money they start with, how much they purchase, and how often they withdraw. Flag and investigate accounts that stray from the norm.
4. **Blacklist offending players**. Do not allow banned players to sneak back in or hop to another server. Keep track by maintaining a running database of known bad IPs, usernames, cookies, buyers, accounts, addresses, and phone numbers.
5. **Do not allow characters and gifts to switch to other servers**. Keeping characters and gifts to one server helps you follow the trail of how they were created.
6. **Limit the exchange of in-game assets to prevent monetisation**. Find out what percentage of players actually use this feature within a game. Then consider whether the feature can be pulled from the game entirely or limited to a certain transaction amount.
7. **Do not give players the option of converting virtual goods or characters into cash**. Merchants who allow "cashing out" are an obvious attraction for fraudsters who want to convert their stolen digital goods into real currency. Only allow barter trade.
8. **Give items a lifespan** and make them depreciate with trades or time spent in the system.
9. **Create "gift tagging"** so assets can be tracked easily.
10. **Return funds to the original payment source if you buy back virtual goods**. For instance if a customer paid you using his credit card, return the funds back to the same account.