PANOPTICON
LABORATORIES

Using Data in Video Games

The Five Ws of Analytics-Based, In-Game Fraud Detection

Online video games are favored targets for financially-motivated hackers, cheaters, and fraudsters, as the global games market reached nearly $100 billion in 2016 with no signs of slowing down. Cybercriminals' activities, if not aggressively combated, can diminish in-game revenues, hurt players' experiences, and even affect the long-term viability of the virtual world and the developer's IP.

The good news is that bad guys' activities leave a noticeable trail in the form of behavioral indicators that can be modeled to predict future events. The bad news is that many games are not logging the right data to make use of modern, analytics-based fraud prevention techniques.

Cybercriminals are professionals who work in rational, predictable ways as they attempt to carry out specific attacks that will result in maximum profits.

Publishers' main advantage in this fight against in-game cybercrime is the fact that criminals are professionals who work in rational, predictable ways as they attempt to carry out specific attacks that will result in maximum profits. Their methods vary between different types of games and will change over time, but the overall objective - to extract real money value from the game - will lead them to take actions that result in the establishment of patterns of behavior distinct from those of "good" or "normal" players who are there to have fun playing the game as the developers intended.

In order to see these patterns, you not only have to make sure that player activities are logged, but also that the right activities are tracked. **This report was developed to help video game publishers and developers ensure that they have the information necessary to combat in-game fraud and abuse.**

Q: WHO should I be tracking?

A: 100% of players, 100% of the time.

Log every session for every player. Anomaly detection relies on creating a mathematical baseline that defines good player behavior, then calls out patterns of activity that are inherently suspicious, or that diverge from the norm.

"WHO" TIPS:

- Make sure all in-game activities logged for players include timestamps, along with a unique PlayerID.
- Do not use Personally Identifiable Information (PII) elements things like email addresses or phone numbers as PlayerIDs.
- If you must use PII data as the unique ID, then be sure to hash or anonymize that information so it remains private and protected.

Q: WHAT do I need to know?

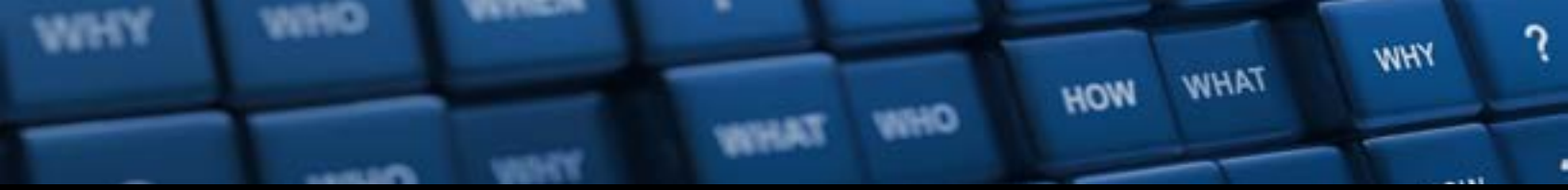
A: Genre + Monetization = Risk

Once bad guys figured out that there are financial advantages in following the money into successful video games, fraud and risk became a predictable outcome. It's useful to think about these risks in terms of genre and monetization.

First, you need to understand which fraud and risk types are prevalent for your game's genre. The same underlying gameplay systems and mechanisms that your players look for when deciding what games to play are the same ones that bad guys look for when tailoring their exploits and tools

In general, regarding genre:

- **MMOs** attract *Account Takeover* and various forms of *Gray Market* activity that impact the in-game economy
- **Casual and social games** attract *Bot Levelling* schemes that automate the creation of fully-levelled accounts for re-sale, reducing the amount of in-game monetization.
- **Competitive games** (Casinos, Sports, and MOBAs) attract *Cheating* and the professional cheat developers who have built businesses creating tools for them.



WHAT? cont'd

You also need to understand which fraud schemes target each type of monetization model:

- **Subscription and Buy-To-Play** fraud tends to focus on *Account Takeover*, due to the high cost of getting in-game.
- **Free-to-play** fraud, because of the simplicity of making new accounts, focuses more on activities that supply the *Gray Market*, since it's the items that are gathered over time or that are purchased via microtransactions that have the most value.
- All monetization types can sustain heavy losses from *credit card fraud*. Cards stored on accounts that are hacked can be misused in the in-game cash shop, and stolen cards can be used to purchase virtual items or currency, which are then liquidated for real money before the chargeback reaches the operator.

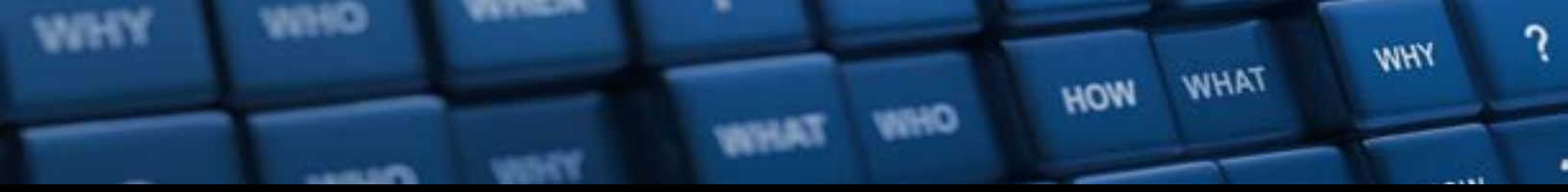
Q: WHEN should I start logging?

A: As early as possible.

Beginning to log during open beta is best. Cheats, hacks, and account takeover tools emerge as soon as the first week after a game's commercial release. This means that the bad guys are using the game's open beta period as an opportunity to refine their attack tools in advance of release. While operators use beta to look for bugs, they should also use this time to study harmful in-game activities as well, informing their countermeasures from what they learned.

"WHEN" TIPS:

- Be realistic: It's nearly impossible to stop 100% of all bad activities. Instead, focus your time and resources on the bad guys who are costing you the most money right now.
- Be vigilant: Professional cheaters and fraudsters you find and kick out will almost certainly try to return. They targeted your game because they saw an opportunity for profit.
- Be persistent: Every time you catch bad guys and kick them out, their operational costs rise. Your goal should be to make it financially imprudent for fraudsters to remain in your game, motivating them to move to other, softer targets.



Q: WHERE should I log data from?

A: All game-related servers.

Modern Games are logged on multiple servers. Video game developers likely have different systems for login/logout, account management, in-game world events, and cash shop transactions, all of which store log data in different ways.

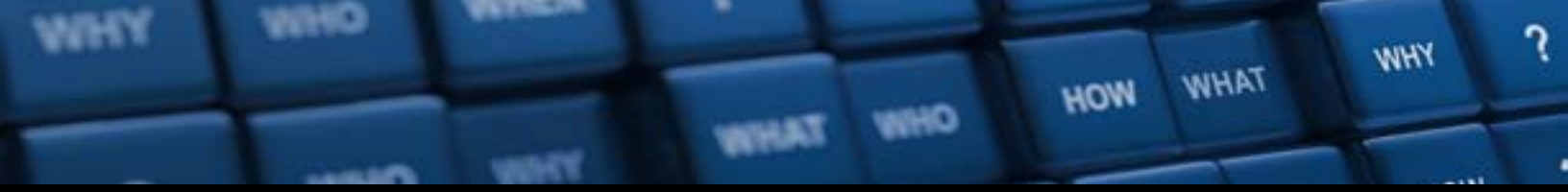
All are important, however the specific fraud and risk schemes that target a game's genre and monetization determine which data is most relevant from a fraud and risk perspective.

Mathematical feature identification is both a skill and an art!.If you choose to hire a data scientist, be sure they have experience in identifying bad actors in complex, diverse populations, and that their models create results that are clear, concise, and actionable by your support team.

Q: WHY should I log player activity?

A: To protect monetization.

- **Better retention** - When good players see the games they love actively fighting back against fraud, it improves their experience.
- **Better top-line revenues** - Players who feel a that game is unfair, or that it is riddled with bots, often leave (taking their money with them).
- **Better, more frequent monetization options for players** - Things like arbitrary level caps before a player can access the cash shop, or transaction limits once they get there (designed to help limit fraud losses) also hinder good players who are willing to spend money.
- **Improved developer/publisher/brand reputation** - Happy players complain less in forums or on social media; fraud schemes that make it into the press turn away curious players.
- **Decreased financial losses** and revenue uncertainty caused by unexpected credit card chargebacks and fees.
- **Lower support costs** - For fraud specialists, support staff, lawyers, etc.
- **Developers can spend their time doing what they do best**...making fun, new features instead of endlessly updating fraud rules or patching the latest hacks.



Q: HOW can Panopticon Labs help?

A: Watchtower: in-game cyber-security for online video games.

Even before games become successful, they almost always attract financially-motivated hackers, cheats and fraudsters in addition to an active and aggressive network of gray market sites dedicated to selling items, currency, and cheats at both the operator's and good players' expense.

To remove cybercriminals lurking in your video games, you have to be able to find them. But if you're not logging player data, you're erasing their tracks for them. By understanding the Five Ws of analytics-based fraud prevention, you ensure that you're tracking the right data to protect your online video games from the financial and reputational damages that result from in-game cyberattacks.

If you have the data, Panopticon Labs can help. We are the first and only in-video game cybersecurity company, built to protect online video game publishers from the financial and reputational damages that can result from cyber attack.

Through proprietary technology that is uniquely focused on gameplay itself, Panopticon sets a baseline of activity for every player who participates in online play. Upon discovering anomalous behavior, Panopticon alerts publishers with more than 98 percent accuracy, along with providing recommendations for incident investigation and immediate remediation.

For more information on Panopticon, visit www.panopticonlabs.com and follow @PanopticonLabs on Twitter.

PANOPTICON

LABORATORIES