TRACKIER®

IGAMING FRAUDS

IGAMING FRAUD PREVENTION AS IT EVOLVES

www.trackier.com

TRACKIER®

IGAMING FRAUDS:

IGAMING FRAUD PREVENTION AS IT EVOLVES

- The year 2020 saw a rise in the popularity of online gambling. Gambling websites benefited greatly from the pandemic lockdowns that encouraged people to engage in in-home activities.
- However, as things gain more clout with gamblers (or players), scammers and con artists start to take notice.
- All forms of cybercrime have seen a 300 percent increase in value as a result of rising internet usage in general.
- Online gambling is a multi-billion dollar industry that is encouraging more and more business owners to use online fraud prevention to safeguard themselves.
- That makes it more crucial than ever for gambling websites to safeguard their clientele from the negative effects of online gambling fraud.
- But those working in the vertical are aware that they are on shifting ground. Players' habits change as a result of new regulations and a dynamic market.
- It all contributes to an environment that is difficult and challenging. Even without taking into account fraud attacks, that is.

This is why, at Trackier, we wanted to give iGaming businesses peace of mind on that front.
Never again wonder how to shield your business from fraud attacks.
All the answers are in our downloadable guide.

WHAT IS IGAMING FRAUD?

- Any fraudulent attack against online gaming operators, casinos, or bookmakers is considered iGaming fraud.
- Due to the nature of the iGaming business, scammers have developed very specialized techniques for trying to game the system, cheat, and take advantage of loopholes.

Some of these iGaming attacks are debatably fraudulent, while others, like the following, are clearly unethical: the creation of multiple accounts under various names, the use of stolen IDs to get around KYC checks, and the use of spoofing technology to get around IP blocks.

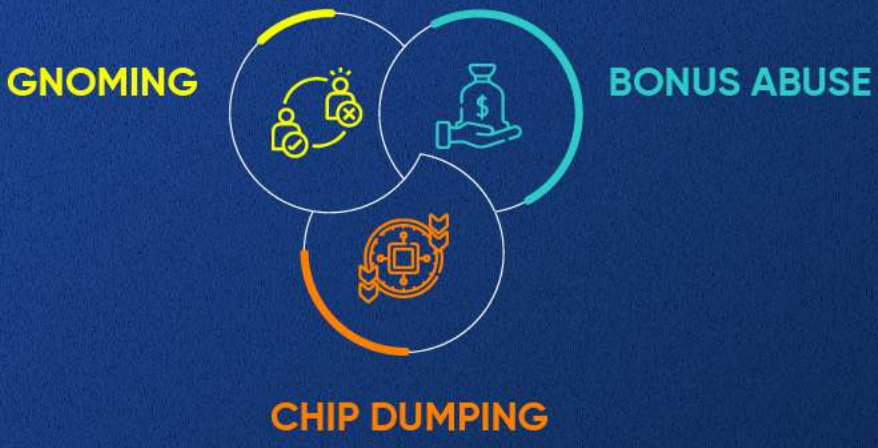
TYPES OF IGAMING FRAUD

When it comes to the variety and breadth of attacks, iGaming fraud is quite exceptional. These include:

1 MULTI ACCOUNTING

- Players set up multiple accounts under various names in order to cheat at games (collusive play) or to take advantage of bonuses that are provided as part of marketing promotions.
- In an effort to avoid being discovered, fraudsters frequently set up multiple accounts using various devices and IP addresses.

There are several schemes that fraudsters may use once they have control of multiple accounts:



GNOMING: This is the process of opening multiple accounts with the same bookmaker. In its least harmful form, gnoming may be used to circumvent maximum bet limitations. In other cases, these fake accounts may be used to more directly influence outcomes.

BONUS ABUSE: Fraudsters create numerous fake accounts in order to take advantage of special offers for new customers. Fraudsters will often withdraw funds and abandon these accounts quickly once they've served their purpose, making the threat of account closure negligible.

CHIP DUMPING: A common method of fraud in online poker, where the fraudster controls multiple accounts at the same poker table in order to manipulate the game in favor of one of those accounts, thereby winning chips from the other players at the table.

2 BONUS ABUSE

- As mentioned above, the marketing campaigns offering referral bonuses or new user signup bonuses incentivize fraudsters to create multiple accounts.
- In this scenario, the gambling platform is the one that is going to be paying out of pocket for fraud. This is one of the more basic online gambling scams that takes advantage of online casinos' making offers to new account holders.
- Bonuses can include free money for your first bet, coupons, or discounts. These types of deals help gambling sites attract new customers, and in a competitive environment, they can help you stand out from your competitors. However, they're not without risk.
- Fraudsters can set up multiple accounts using different email addresses, devices, or IP addresses. These bonuses may not be worth a lot, but it's free money to the fraudster and money you've just given away for nothing.

3 AFFILIATE FRAUD

Another area where marketing spends can backfire against casinos: affiliate fraud.

Because iGaming sites are restricted in the ways they can market their companies, they often rely on affiliates. However, unscrupulous fraudsters can set up false expectations and send bad quality traffic that eats away at marketing budgets with very low ROI.

Marketers who reward affiliates for directing visitors towards their site are often the victims of:

- Spammed referral links: which bring in low-quality players.
- Bot automation: whereby fraudsters use software to imitate human behavior and generate fake clicks and transactions.
- Maliciously diverted traffic: which sends unwilling visitors to the page, increasing bounce rates and corrupting analytics.

In some cases, the affiliate fraudsters will go as far as cloning the operator's website and hosting it on a domain name that looks similar. More advanced techniques include malicious browser extensions that swap legitimate affiliate URLs for their own and even inject ads with referral links into ad-free web pages.

4 CHARGEBACK FRAUD

- **iGaming sites often act as e-wallets, where players can deposit funds using credit cards. Fraudsters use other people's cards, which may work but incur chargeback fees.**
- Chargeback fraud is where customers exploit a form of insurance on their credit card that (ironically) protects them from fraud.
- A chargeback gambling transaction can be initiated by a customer when they've lost a lot of money. They can call their bank, or credit card issuer, and claim their card was stolen or used without their permission.
- The bank can then opt to reimburse their losses directly from the bank account of the online gambling website, even if the website challenges the circumstances.
- In this instance, it helps the gambling site's case if it can show it takes steps to prevent stolen credit cards from being used.

5 SELF-EXCLUSION FRAUD

- **This kind of fraud is becoming more prevalent and can be very challenging to detect using legacy systems. Even with the best of intentions, it is very challenging for companies to protect every player.**
- A fraudster opens an account, sometimes uses it to play, and self-excludes it.
  They open a second account with the same operator or those that fall under the same license as the parent company.
- They deposit large amounts and play volatile games at their max bets.
  If they lose, they blackmail the operator into getting a refund by claiming their self-exclusion was not respected.

6 CREDIT CARD FRAUD

- **For fraudsters who get their hands on a stolen credit card, online gambling sites can be a great place to drain the funds on that card. It can be as simple as opening an account, depositing the funds, and cashing out immediately.**
- Other credit card frauds generally have some down time for them to make money - they need to make purchases from stolen credit cards, and on-sell the items they've bought. In this instance, even if they play a few hands of poker and lose, they still walk away with a lot more money than they had initially.
- Stolen credit card credentials are commonly bought and sold on the dark web, so this is a very real risk for online gambling websites.

7 GAME-SPECIFIC FRAUD:

- **Then, of course, there are all the "exploits" that are specific to certain games, such as matched betting, chip dumping at poker tables, or gaming.**

HOW CAN MERCHANTS PREVENT ONLINE GAMBLING FRAUD?

Due to its nature, online gambling will always be appealing to scammers.
However, there are steps you can take to reduce the dangers of online gambling, and they can have a big impact.

Knowing who your customers are in detail is a general theme that aids in the prevention of online gambling fraud.
Once you know this, customers cannot set up multiple profiles or use credit cards that are not their own, so chargeback fraud can be disputed.

There is a range of techniques you can use to properly identify customers: You can use a variety of methods to accurately identify customers, such as:

- Promoting the use of two-factor authentication and strong passwords
  As a result, it is much more difficult for fraudsters to gain access to other people's accounts.
- Employ identity-verification services that can recognize user information like IP addresses, email addresses, and geolocation.
- Use fraud prevention software that can analyze user browser behavior to conduct risk assessments and flag users who engage in suspicious behavior.

Browser fingerprinting is an effective method for preventing online fraud. Every user of your web application can leave behind an online fingerprint that can be used to track their browsing history and behavior over time.

In order to prevent fraudsters from hiding their identities, browser fingerprints are made to remain constant regardless of whether a visitor uses a VPN or switches to private browsing mode.

Preventing multiple accounts is one extremely helpful use of browser fingerprinting for gambling websites.

Users can be verified using their fingerprints as they log into their accounts, ensuring that only one profile is being used at a time.

Furthermore, you have the option to prevent fraudsters whose fingerprints have previously been connected to fraudulent activity on your website from ever logging in.

TRENDS IN IGAMING FRAUD 2022

iGaming fraud, like all kinds of fraud, is adaptive. This means it evolves constantly and you must stay on top of the latest trends. Here are the ones to keep an eye on next year:

SYNTHETIC IDS

- Fraudsters now avoid KYC checks by using synthetic IDs, which is the fastest-growing form of fraud in the US.
- They combine false information with legitimate identification documents, which makes them more difficult to spot than completely false profiles.
- The US Federal Reserve estimates that the issue of fake IDs increased by 85–95 percent just in 2019 and grew even faster during the COVID-19 pandemic.
- The ease with which fraudsters can access real ID documents on the dark net due to the constant flow of data breaches may account for the rise in popularity of the practice in recent years.

SELF-EXCLUSION FRAUD

- Fraudsters are more aware as authorities tighten their enforcement against iGaming businesses to safeguard consumers from gambling addictions.
- By designating themselves as "problem gamblers" on the iGaming site and using a different account to continue gambling, they are aware that they can effectively blackmail iGaming companies.
- Essentially, this is a multi-accounting issue that can be resolved with the right tools, but iGaming companies have reported an increase in these cases over the past few years, and it's expected to remain a problem in 2022.

DEEPFAKES FOR VIDEO ID

- Video deepfakes are yet another technological advancement that ended up in the wrong hands.
- Fraudsters are using deepfakes to get around video ID verification systems set up as part of a KYC process as technology becomes more accessible.
- Not all iGaming sites have the resources to check whether the videos are genuine or not, even though video ID verification providers are constantly updating their systems.

CONCLUSION

The strategies employed to reduce fraud in the industry must evolve as the iGaming landscape does year after year.

iGaming fraud, like all kinds of fraud, is adaptive. This means it evolves constantly and you must stay on top of the latest trends. Here are the ones to keep an eye on next year:

As evidenced by the recent increase in self-exclusion, operators regrettably frequently fall behind fraudsters who are quick to exploit new attack vectors and agile. The good news is that, in the prevention camp, companies like Trackier are always striving to develop new tools, share insights, and refine rules that will eventually defeat the fraudsters.
The good news is that solutions like Trackier, which are constantly working to improve and create new tools as well as share knowledge to prevent fraudsters, exist and help iGaming businesses thrive.

We firmly believe that iGaming operators should at least have peace of mind when it comes to scaling their operations while minimizing the costs, resources, and losses due to fraud, even if the industry sometimes feels unpredictable.

You can check out our **Anti-Fraud tool** to understand how we prevent fraudsters from affecting our partners' businesses.

Partner with us today and turn your imagination into innovation with **Trackier!**