Who's playing who?

The secret to securing online gaming is being able to identify good user behaviour.

NuData Security reports

The online gaming industry has a unique set of security challenges that other online businesses don't have to worry about. Unlike online businesses that sell an item to a buyer and who enjoy a predictable income stream, online gaming, whether it's pay-for-play card games or traditional betting, is by nature more erratic in terms of the flow of money and therefore a tempting target for fraud.

It is a booming industry that generates billions of dollars from players worldwide. British statistics show that 1 in 20 iPhones has a sports betting app. Technology has been the driving force behind the phenomenal growth of the online gaming industry. Unfortunately, while the internet makes it easier and more convenient to place bets, it also provides the means for more organised cybercriminals to defraud these sites and their good players. But as the industry booms, the threat of criminal activity looms. Cheating at cards has a long and infamous history. Is it any wonder that we see it happen in the virtual world, too?

This is not to say that the online gaming industry is a wild west in terms of security – it isn't. It is a mature market raking in huge revenues. And because statistics are at the heart of gaming, they've also developed incredibly sophisticated data analysis tools that can determine with high accuracy if, for example, a six-player poker hand is being gamed by one person with multiple accounts. But that just looks at one point in the player's history. Why settle for a snapshot when you can see it all play out from beginning to end?

Fraudsters aren't without their tools, either. By using methods to circumvent traditional detection like IP address, geolocation, third-party credit verifications, even using data analysis of other players, it means that despite the gaming industries best efforts, fraudulent deposits, cheating and collusion, chargebacks and money laundering persists.

Looking at the snapshot, analysing the game as it is played, is one tool in the arsenal. But there is another security layer that should be added, one that observes the players before the game starts and even across the lifetime of the player.

Looking at the snapshot, analysing the game as it is played, is one tool in the arsenal. But there is another security layer that should be added, one that observes the players before the game starts and even across the lifetime of the player. Building complex models of behaviour is the secret weapon about to sweep online security – a real game changer that will show the difference between a flesh and blood player from sock puppet accounts and scam artists.

Every human being has unique behaviours and habits that are dead giveaways but the gaming industry isn't interested in learning what a player's tells are. Behaviour-based security looks at hundreds of signals that allows us to confidently know when we are seeing the genuine player, signals such as how they hold their device, how they type or whether they use a mouse or a trackpad when playing. It is these non-identifying but wholly unique behaviours that create a player profile that can't be spooked and can't be fooled.

Let's take a look at what fraud looks like for the online gaming industry.

Credit card fraud occurs when stolen credit cards are being used to set up or fund betting. In some cases these stolen cards are used by a single player running several accounts in the same game so they can purposefully lose on the stolen card and funnel that money into their personal account, which can be cashed out later.

A single user running multiple accounts does not necessarily have to use stolen credit cards to perpetuate the scam. A typical scenario would have a six-player room filled with only two players, one who is unaware of the scam and another running the other five players, essentially guaranteeing that the scammer will win. The use of multiple accounts is not limited to intentionally scamming other players by rigging the odds. Many gambling sites offer an incentive for new players, matching an initial startup deposit or giving the players cash bonuses for completing a set number of games, too.

This all goes back to the users themselves and the accounts they create. Account creation is the first point of contact for legitimate users and would-be scammers alike. While robust data analysis can catch some of the scammers when the games are

There is too much money on the table to leave it to chance. Knowing which of your players are real and which are not before the game even starts puts the odds, finally, in your favour.

happening, wouldn't it be better to catch fake accounts before they can even start a game?

It isn't only the online gaming company that takes a hit. The legitimate player who is just there to play a hand of cards doesn't know they have been hit with the bad luck of being in the same virtual room as the scammer. And once they find themselves defrauded, customer retention becomes a huge issue. If a site becomes known for fraud, there is little a company can do besides invest in a costly rebranding and build anew.

Setting up accounts for online gaming is, by nature, more intensive than setting up an account for an e-commerce website. A first round of registration needs to confirm things like the user's birthday and checks are typically run against personally identifying information. But with the prevalence of data breaches flooding the market with exactly these kind of credentials, these sorts of checks are of limited use. If personally identifiable information can be faked or stolen, what is left? Behaviour.

The behaviour of a legitimate user signing up for and using a service will still be different from someone creating multiple accounts to perpetrate fraud. How the user goes on to use the site after account creation, outside of even game play, continues to build profiles very distinct from each other.

Behaviour-based fraud detection goes deeper than just figuring out which account has a human being on the other end, and which are one of an array of puppets. Behaviour-based security methods will also tell you if an account has been stolen from its owner or if a new account is being made by a customer with past gaming difficulties. Behaviour can even be leveraged into predicting a budding gaming addition by comparing the behaviour of past addicts against current users and taking the necessary steps to stop chargeback complaints, also known as first party fraud, from players who have gone overboard.

The takeaway of what behaviour-based security can offer the online gaming industry is considerable: a reduction of losses from fraud exposure due to chargebacks, increasing efficiency by blocking fraudulent accounts at account creation, reducing the review process, and growing player trust and satisfaction without interrupting the user experience. There is too much money on the table to leave it to chance. Knowing which of your players are real and which are not before the game even starts puts the odds, finally, in your favour. □

NuData Security predicts fraudulent transactions by identifying good users from bad, based on their online behaviour. By tracking over 18 billion behaviours anually, NuData harnesses the power of behavioural and statistical analysis, enabling its clients to predict fraud with 99% accuracy.

For more information, please visit **www.nudatasecurity.com**

NU Data Security