

COMBINING INDUSTRY STRENGTHS TO PREVENT EVOLVING THREATS

BY SCOTT OLSON

With often sophisticated abuse and fraud causing financial and credibility damage to the online casino and gaming industry, ranging from in-game social abuses, promotion abuses, cheating and identity theft to financial abuses, across-the-board defence mechanisms to prevent and reverse industry losses is vital. It is therefore necessary to assess the techniques to combat that fraud, how device-based fraud management is an essential tool for any Internet casino, and how competitors can work together to address a common threat to the entire industry.



Fraud rates in excess of 10 percent of total revenues is not unheard of in the online gaming industry, and many online casinos struggle simply to keep chargeback rates to a level that doesn't either jeopardise their access to certain payment types or create such a high payment processing fee structure that their profitability is severely reduced. The issue to analyse here concerns not only the various types of online fraud against casinos, but also the techniques to combat that fraud, how device-based fraud management is an essential tool for any Internet casino, and how competitors can work together to address a common threat to the entire industry.

Why are casinos such an attractive target and why are fraud rates so difficult to get under control? The answer to the first question is obvious. Where else can an attacker find an online bank, casino and efficient money transfer mechanism all in one place? Online casinos are simply one of the most effective places for cybercriminals to take their newly stolen credit instruments and to turn them into financial gain.

Unfortunately, for the operators of online casinos, the fraud doesn't simply stop at the use of stolen credit cards. The spectrum of abuses facing online gaming sites are varied and don't lend themselves to standard fraud management techniques. These abuses include a variety of problems:

- **In-game social abuses** such as offensive language and in game spam
- **Promotion abuses** create multiple accounts to take advantage of site monetary promotions
- **Cheating** can include in game collusion and chip dumping
- **Identity theft** in the form of using a stolen identity to

create a new account and taking over an existing casino account to gain access to their funds

- **Financial abuses** include credit card fraud, money laundering, friendly chargebacks, and fully organised fraud rings.

Let's first examine how a credit card deposit from a stolen credit card can make its way through an online poker site. First, the online criminal uses the stolen credit card to create a new account and make an initial deposit. Typically, that criminal has other associates in a broader fraud ring that help him move this money through the system. What happens is that the criminal will sit at a table with a mix of legitimate players and his associates. Player X proceeds to lose all of the money from his initial deposit to both his associates and to other legitimate players. It is essential for them to involve legitimate players as it makes it extremely difficult for the online gaming site to distinguish legitimate players from the criminal associates. At this point the process is repeated at other tables where the people take their winnings and proceed to lose them to the next tier of associates in their fraud ring. Ultimately, the money has moved through several layers of tables and it is eventually safe to transfer it out from "clean" accounts that have had no history of fraudulent deposits or other activities.

Combating financial fraud is all the more difficult because criminals are using the Internet to their fullest advantage in their techniques. First, not only are there large fraud rings where virtual partners work online to defraud their target companies, but the tools of the trade are widely available through the Internet. Hacker chat sites share information and techniques on how to defraud targeted casinos. Large online databases where credit card numbers and all essential personal information are traded actively: These databases not only guarantee the validity of more than 90 percent of the card numbers, they also provide CVV2 numbers, mother's maiden names, addresses, recent car colors and all numbers of other relevant personal information.

The essential truth of how the online threat has evolved is that there is a thriving illegal online network and commerce industry providing the tools to defraud online businesses. The criminals are becoming more organised and working together. This makes it extremely difficult to effectively combat the threat alone.

It is helpful to look at the avenues available to online gaming sites to combat fraud. Certainly, when a fraudulent

account is discovered, it is banned and any funds in that account are brought back into the casino. At this point, the options for the online gaming site are limited. How can an online casino prevent the same individual or group of individuals that they just banned from coming right back with different personal information and all new accounts?

AVENUES OF DEFENCE

Essentially, there are three avenues available to use to reduce the damage caused by repeat offenders and organised fraud rings that systematically target an online gaming site, and they have varying levels of effectiveness. Let's examine what we would do in a real-world scenario and see if that has applicability in the online world. In the real world, if a group of individuals were repeatedly breaking into a casino, law enforcement would be immediately engaged to find and stop the crime ring and prevent them from targeting the casino again. Additionally, the casino itself would identify the criminals and actively look for and prevent them from coming back into the casino.

On the Internet, the first recourses available to a brick and mortar casino are simply not effective. Law enforcement online is essentially non-existent as a deterrent to crime. The problems with this approach abound. Very often the criminals aren't in the same country as the online gambling site, making it extremely difficult to coordinate law enforcement efforts required to associate the real-world individual with a temporary virtual identity. Additionally, if law enforcement is lucky enough to find the offender, they have a difficult time prosecuting the individual as they reside in a different jurisdiction. Therefore, extradition may be impossible and local laws may not take as hard of a stance on online crime.

If law enforcement isn't an option, then one would logically move to the option of restricting future access by identifying those individuals the next time they attempt to create an account. Unfortunately, on the Internet, how does one accomplish that? Most fraud management systems are based completely upon identity information and financial information. All of this information is supplied by the individual, which makes it easy for the online criminal who has had an account banned to simply create a new one completely undetected.

Fraudsters cleverly hide behind multiple identities and accounts. Use of stolen financial instruments, friendly chargebacks, abusive chat, spam, bonus and promotion

>> OVER TIME, COMPUTERS ESTABLISH A POSITIVE OR NEGATIVE REPUTATION BASED ON HOW THEY ARE ACTUALLY USED. IF A DEVICE CAUSES A PROBLEM ON ONE GAMING SITE, THIS FACT CAN BE BROADCAST SO THAT OTHER SITES CAN DECIDE HOW THEY WANT TO REACT TO THE NEW INFORMATION. BY LINKING A COMPUTER'S REPUTATION TO ITS ONLINE ACCOUNTS, FRAUD MANAGERS CAN SEE EXACTLY HOW A PARTICULAR COMPUTER HAS BEEN USED IN THE PAST AND ARE BETTER EQUIPPED TO EXPOSE AND PREVENT THE FRAUDSTERS FROM NEW ACCOUNTS, EVEN WHEN THEY ARE TRYING TO ENTER A WEB SITE FOR THE VERY FIRST TIME >>

abuse, collusion, cheating and other abuses are costing online gaming sites millions of dollars a year. Prevention requires the ability to expose and stop fraudsters from entering a site in the first place.

One of the biggest reasons fraud managers continue to struggle with online fraud and abuse is because their fraud management techniques are focused primarily on personal identifiable information (PII). When abusive behaviour is identified, nothing prevents the individual from coming back. Without even leaving their chair, they come right back using the same computer to create a new fraudulent account and repeat the undesired behaviour. This is why it is essential for casinos to seriously consider adding device-based recognition and fraud management techniques into their arsenal.

WEB OF ASSOCIATIONS

Device reputation allows fraud managers to see the relationship between all devices and accounts on their network. This, by itself, is extremely valuable. Why would one device be associated with 100 accounts? When you identify a bad account, stopping all other related accounts at the same time helps you get ahead of the problem.

Over time, computers establish a positive or negative reputation based on how they are actually used. If a device causes a problem on one gaming site, this fact can be broadcast so that other sites can decide how they want to react to the new information. By linking a computer's reputation to its online accounts, fraud managers can see exactly how a particular computer has been used in the past and are better equipped to expose and prevent the fraudsters from new accounts, even when they are trying to enter a Web site for the very first time.

LAYERED APPROACH

Device reputation can also enhance other risk management techniques. Take for example, a transaction scoring service that stops 10,000 transactions based on stolen credit card reports, invalid address, and other valid reasons. What do you think the chances are that these failed deposit attempts came from 10,000 unique computers? Why would you continue to process transactions from a computer that has submitted hundreds of high risk transactions all under different identities? Device visibility allows sites to stop accepting transactions from bad computers.

More valuable still, in identifying the bad device to prevent future deposit attempts, you will likely see that this computer got some transactions through. In this way, device reputation strengthens the transaction scoring system by seeing high risk transactions that the risk scoring service missed.

As you can see, without device reputation fraud managers are only looking at half the picture. The inclusion of device reputation augments an online gaming site's existing fraud detection solutions, providing a multi-layered defense needed to combat online fraud and abuse.

NETWORK EFFECT

While device intelligence can be used to tell the good guys from the bad, the defining power of the device reputation-based defense lies in the sharing of reputation data among online entities. And perhaps the more compelling argument for a new paradigm governed by device reputation is that the

larger the shared network of companies using reputation management software, the more robust and the more detailed the reputations are in its universe. The ability to tap into an extensive web of associations to see which devices and accounts are linked across the Internet provides tremendous value for fraud managers who are trying to connect the dots to stop organised fraud.

With a network of online communities using device reputation for security, word travels fast. Imagine the benefit of knowing a device trying to deposit money on a poker site is associated with an account with evidence of stolen credit cards and chargebacks on another online gaming site. If a device identified with past fraudulent behaviour is linked to another device or account across a network of device reputation subscribers, that particular computer can be shut down before it can repeat the fraudulent behavior.

A network with the ability to uniquely identify each device, expose associations with other online accounts, monitor that relationship over time, and continually share data with other online networks is an incredibly valuable tool.

STOP FRAUD BEFORE IT HAPPENS

The bottom line is device reputation takes the guesswork out of fraud management. Internet security representatives have a clearer picture to make quicker, better informed decisions based on confirmed evidence to catch fraud that would otherwise be missed. With device reputation, online gaming sites can enhance their arsenal to fight fraud and abuse, and in doing so, increase operational efficiencies and reduce barriers to entry to significantly increase revenue.

In an era of rampant identity theft, device reputation removes the mask of fraudulent and unwanted behavior to stop fraud and abuse before it happens. **CGI**

SCOTT OLSON



Scott Olson is the vice president of marketing at iovation, an online fraud management company. He is a recognised thought leader in IT Security and is a frequent speaker at industry events such as Combating Cybercrime, RSA, and Digital ID World.

Scott holds a BSE in Electrical Engineering from Duke University and an MBA from the University of Texas at Austin. In 2007, he received the Distinguished Young Alumni award from the Duke University Pratt School of Engineering. Scott is a Certified Information Systems Security Professional (CISSP).