

THE POWER OF DEVICE REPUTATION

Sharing device intelligence provides online gaming sites multi-layered defense against fraud and abuse.

WHAT IF YOU KNEW the reputation of a computer the instant it connected to your network? Would it be valuable to know that a computer has passed stolen credit cards on multiple other sites? What if you could get this intelligence without exposing the identity of your customers? Sound like a wistful dream? It's not. In fact, a number of online gaming sites are currently using device intelligence to prevent almost any fraud and abuse you can imagine.

The relative anonymity supported by the Internet makes it extremely difficult to distinguish between the 'real me' versus someone pretending to be me. Fraudsters cleverly hide behind multiple identities and accounts. Use of stolen financial instruments, friendly chargebacks, abusive chat, spam, bonus and promotion 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 your 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 behavior 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 behavior.

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 hitting a Website 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



Prevention requires the ability to expose and stop fraudsters from entering your site in the first place.

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.

AUTHORPROFILE



Greg Pierson is founder and CEO of iovation, a fraud management company based in Portland, Oregon.

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 organized 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 iGaming site. If a device identified with past fraudulent behavior is linked to another device or accounts 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. ■