

Combating cybercrime



Dr Akif Khan of **CyberSource** and **Greg Pierson** of **iovation** talk to *eGaming Review* about the ways in which their companies are fighting fraud within the online gaming arena



Dr Akif Khan is the director of products and services at **CyberSource**. He has become an industry thought leader and influential speaker in the online fraud arena. Advising online merchants all over the world, Dr Khan has witnessed the latest challenges faced by organisations in multiple geographies and market sectors.

MANAGING THE THREAT of online fraud is a tricky business; overly stringent precautionary measures can put players off, while seemingly lax security can affect client confidence, particularly where payments are involved. Offering unobtrusive fraud-prevention measures while reassuring the customer is increasingly important as fraudsters come up with new ways to attack gaming sites. **CyberSource's** Dr Akif Khan and **iovation's** Greg Pierson tell *eGaming Review* about the latest developments in fraud prevention and how their companies are keeping the bad guys at bay.

eGaming Review (eGR): How does fraud prevention affect legitimate clients, and what measures can be taken to avoid the loss of good custom?

Dr Akif Khan (AK): Some fraud-screening tools can operate too rigidly, resulting in good customers being turned away unnecessarily. To help avoid the loss of good custom, egaming merchants should invest in an automated solution that enables them to build rules specific to their customers' behaviour. In addition, focus should be given to recognising good behaviour rather than just trying to spot bad behaviour. Having an adaptable fraud solution, rather than a 'one size fits all' approach will help to prevent the loss of legitimate customers while still minimising fraud.

Greg Pierson (GP): The impact of fraud prevention on legitimate customers varies tremendously depending on the risk-mitigation techniques used and the approach taken when responding to potential threats. Ideally, fraud management should be invisible to your customers, preventing threats in the background, in real-time, while protecting the identity and privacy of your customers.

We suggest looking for solutions which offer low false-positive rates so that good players are not mistaken for bad ones, along with solutions which do not interrupt the player experience, but provide efficiencies in the review process, are highly scalable

and enable you to respond to requests appropriately.

eGR: What unique services does your offering provide to guard against fraud efficiently and comprehensively?

AK: The most effective way to protect businesses from online fraud is to use a combination of anti-fraud tools, gathering as much information about each transaction as possible.

CyberSource Decision Manager includes over 200 validation tests and services (such as device fingerprinting, velocity checking and IP geolocation) to help egaming companies catch fraudulent behaviour sooner and more accurately. Each order is simultaneously compared with data collected from thousands of merchants worldwide, to highlight anomalies that may signal fraud.

GP: **iovation** provides a real-time service which exposes the reputation of computers that connect to your business. We have a database of over 350 million unique computers from every country in the world and our shared platform allows gaming sites to benefit from the traffic, relationships and information provided by thousands of global fraud analysts, representing more than 300 major online brands. Besides knowing when a bad device touches your site, our multi-layered approach also looks at transaction anomalies, velocity rules, profile risk and associated accounts and devices to identify fraudsters. Combining fact-based evidence with inference of risk helps sort the good from the bad at transaction time with nearly zero false-positives.

On average, our gaming customers see a 40% uplift on fraud stopped by leveraging global information, as opposed to just looking at the activity on their own site. In the past 90 days, our platform has stopped 5.6 million fraud attempts. Of these, four million were caught because of activity within individual sites, with the remainder identified through activity on other sites. If a device has defrauded several other gaming sites, why not use this information to avoid the problem in the first place?



eGR: What new forms of fraud have been noted in 2010, and how can these be guarded against? What do you do to keep one step ahead of fraudsters?

AK: Fraudsters are always finding new ways to commit fraud. During 2010 we've seen an increase in the number of fraud attacks involving botnets. Fraudsters have long been able to use proxy servers to circumvent IP geolocation checks, but the latest evolution of this trend is organised criminals distributing malware onto innocent people's computers via phishing sites or email attachments.

This malware effectively turns the computer into a proxy server through which the fraudster can send transactions, unbeknown to the genuine user of the computer. When a criminal has infected a large group of computers it is known as a 'botnet', which becomes a valuable commodity to rent out to other fraudsters to use, as it enables them to hide their location behind a large network of proxy servers.

One way that egaming merchants can guard against this is to use a vendor with strong device fingerprinting and proxy piercing capability.

GP: So far this year, we are seeing high levels of attempted credit card fraud, collusion, affiliate fraud and account take-overs. Sharing information is key to staying ahead of the fraudsters. Our platform allows gaming sites to benefit from the knowledge of traffic and experience at other sites. Moreover, our platform helps sites benefit from all the fraud management tools and resources across all the business we protect.

eGR: How important is technology to the prevention of crime and fraud in the egaming sector, and what kinds of technologies have been developed recently in response to fraud?

AK: Technology is a critical component in winning the battle against fraud. The most recent innovations in CyberSource's toolset include powerful device fingerprinting capabilities that enable merchants to accurately and uniquely identify a computer that is being used to transact on their website. This is done passively without interfering with the customer experience, and helps egaming merchants spot fraudsters who are registering multiple times under different identities, for example.

Another cutting-edge feature is the ability to pierce through proxies to establish the true IP location from which the transaction data is originating. If a fraudster was sitting in, say, Vietnam but routing transactions through a proxy in, say, France, this technology would be able to accurately identify their true location and not be fooled by the proxy. This has proven to be exceptionally useful for our merchants.

GP: Technology is necessary to manage risk at scale and optimise operational efficiencies. But technolo-

gy, people and processes have to work together. We continually add new rules and capabilities to our platform, giving our subscribers greater flexibility and control over the activity on their website by incorporating deep intelligence about end-user devices, associated accounts, and shared history. Alerting sites the moment a bad device touches their business and identifying risks in real-time based on device characteristics and behaviour has already flagged nearly 16 million fraudulent transactions for our clients in the first six months of this year.

eGR: To what extent is the increasing role of alternative payment methods becoming integral to online crime?

GP: The attack surface has increased significantly with the proliferation of alternative payment methods. Every new payment method, like every new feature, creates potential new ways for bad guys to damage your business and exploit your customer base. Multi-layered risk-mitigation strategies and sharing across verticals, geographies and fraud teams is critical.

eGR: How important is choosing the right payment provider in the prevention of fraud?

AK: Merchants should choose a provider that can offer a comprehensive fraud-management solution worldwide. Each business is unique, so it is critical that both organisations work together to define requirements and determine the most suitable approach, whether this is supporting an in-house fraud team or fully outsourcing. Merchants should also work with a provider that offers global coverage and understands ecommerce across the world, not just in the local region. After all, fraudsters are not limited by geographical boundaries.

GP: Choosing a payment provider, or a complimentary set of payment-service providers, is an important decision. Some solutions leave the risk for you to manage, some leverage sophisticated anti-fraud technologies, while others assume the risk. Payments are just one aspect of your business subject to fraud and abuse. No combination of payment-service providers is going to help you stop fraudsters from returning to your site to set up new accounts. Nor will payment-service providers help you uncover account take-over attempts, underage players, chat abuse, chip dumping and other fraud and abuse attempts outside of the payment process.

Specific end-user interactions need the right level of protection, based on what is at risk. The mix of tools you use and the flexibility of individual solutions can help you customise an approach appropriate for individual points of interaction and their associated risk. Ultimately, it's about balancing risk with customer experience, revenue, and other factors that are important to your business. ❖



Greg Pierson is the co-founder and chief executive for iovation, and the visionary leader behind using device reputation to help businesses know which online visitors to trust to reduce fraud, abuse, and protect good customers.