IPQS Expands Fraud Prevention Strategy to Combat the Rise in Upstream Fraud Attacks

IPQS builds on its industry momentum with new fraud leadership, advanced threat intelligence, and proactive fraud prevention.

IPQS advances its proactive fraud prevention mission through expert leadership and real-time threat intelligence.

LAS VEGAS, NV, UNITED STATES, June 15, 2026 /EINPresswire.com/ -- IPQS, an industry leader for real-time fraud protection services and digital identity validation tools, announced that Alexander Hall has been appointed as its Vice President of Fraud Strategy.

Hall joins IPQS after an impressive career filled with valuable experience helping businesses defend against increasingly advanced and automated cyberattacks. This news comes shortly after the Safeguard conference in Colorado, where Jordan Harris interviewed Hall for the celebrated Fraud Boxer Podcast.

> Fraudsters are aggressively moving upstream to target account creation”
>
> *Alexander Hall, VP Fraud Strategy*

Recently selected as the overall sponsor of the Merchant Risk Council (MRC) 2027 event, IPQS continues to build on its momentum, and Hall's addition reflects its ability to serve as a holistic provider in terms of providing solutions to fraud rather than acting merely as a data provider, given its approach of assembling a team of fraud experts.

Multi-System Fraud and Moving "Upstream." In the latest episode of Fraud Boxer, Hall described another important transition within the world of cybercrimes: multi-system fraud.

Fraudsters conduct simultaneous attacks on completely different systems, for example, when aging a mule account on one website, an iGaming portal, to later use in compromising the banking system, leading to extremely high average fraud event amounts ranging from hundreds of thousands to millions of dollars. "Fraudsters are aggressively moving upstream," said Alexander. "We historically armed ourselves at the checkout page, so criminals pivoted to

account creation, login access, and identity fabrication. To stop them, defenses must adapt from simple transactional rules to deep, continuous account-level behavior tracking."

Fraud Boxer Podcast host Jordan Harris interviews IPQS VP Alexander Hall.

Defeating Threats in 90 Days: Less Time With Passive Honeypots. To further combat these vulnerabilities upstream, IPQS is now focusing on its own honeypot network.

Rather than using the standard process of collaborating with fraud consortiums and waiting for the hefty 14 to 90-day delay for chargeback data, IPQS is acting as an advanced warning system. This is due to its honeypot network, which uses 10,000 machines with thousands of passive instances, including email, database, and web server vulnerabilities. Automated scrapers or other malicious bots will be able to target these fake vulnerabilities, allowing IPQS to monitor and capture the fingerprints, IP data, behaviors, and personal information of any threat in real time, while posing no risk to any of IPQS's clients' data or money.

The Fraud Boxer Podcast Interview below will take you through a complete interview covering multi-fraud system networks, email intelligence, and proactive defense measures:

Amber Kahr
IPQS
+1 800-713-2618
email us here