WhoisXML API Joins the Global Anti-Scam Summit (GASS) London 2025

Posted on April 29, 2025

Alexandre François (Product Marketing Director) and David Hagberg (Strategic Partnerships Director) represented WhoisXML API at the Global Anti-Scam Summit (GASS), held in Westminster, London, U.K., on 26–27 March 2025. They joined more than 1,000 in-person and virtual attendees at the event, which aimed to bring together a community of fraud fighters and build a framework for tackling fraud and scams—two growing problems worldwide, in both developed and developing countries.

The event brought to light the urgency of fighting against cybercrime, especially since Internet users are up against highly organized and determined fraud groups. In fact, one in four individuals globally has fallen victim to fraud and scams, with fraudsters having amassed nearly US$1.03 trillion in 2024.

GASS London highlighted some of the most common trends in adversarial techniques and how the online community can rally against them. We'll recap these trends, along with our key takeaways, in this post.

The Many Faces of Fraud

Fraud fighters are unanimous in their assertion that fraud and scams occur regardless of borders—criminals overseas target locals elsewhere through techniques like phishing, smishing, and SIM swapping. We'll detail some of the types of scams tackled across multiple sessions during the event in the table below.

Type of Scam	How It Works

Romance scams	Also known as “online dating scams,” these prey on individuals looking for companionship or romantic relationships. Scammers typically create fake profiles on dating apps or social networking sites—some even use email—to build emotional connections with their targets. Once trust is established, scammers fabricate stories requiring financial assistance, such as urgent medical bills, or travel expenses to meet their victims.
Investment scams	These scams trick people into investing in fake or worthless business opportunities while promising high returns with little to no risk. Scammers may pressure targets into investing before the opportunity is lost, creating a sense of urgency that can push victims into investing.
Shopping scams	These scams involve threat actors creating fake online stores that sell goods at very low prices or counterfeit products. They take payments but do not ship the items bought.
Employment scams	This type of scam targets people looking for jobs. Scammers post fake employment opportunities on legitimate job boards or via email, aiming to extract sensitive information or ask for upfront payment, which legitimate employers typically do not require.
Youth-targeted scams	Young people seeking connections online have become increasingly vulnerable to scams, specifically in videogame rooms, social media, and online forums. They have a tendency to overly share personal details with strangers they meet online, who may end up asking for money or other favors under the guise of an emergency or as a way to deepen the friendship.
Celeb-bait	This is a type of scam that impersonates public figures in social media ads to promote products, services, or investment schemes. In 2024, Meta announced it will use facial recognition to detect and remove ads that impersonate celebrities.

Common Adversarial Techniques

The scams mentioned above have proliferated over the years, with some becoming so common that government agencies like the Federal Bureau of Investigation (FBI) began issuing routine advisories warning people against them.

These types of scams are powered by various fraud techniques that have evolved throughout the years, and some of these methods were mentioned during GASS London.

SIM-swapping fraud, for one, increased by 1,055% in 2024 in the U.K., with criminals diverting U.K. SIM cards to other countries to scam locals. This technique allowed scammers to intercept one-time passwords (OTPs) and other verification codes sent via SMS, thereby bypassing two-factor authentication (2FA) and taking over a user's account.

The advancement of artificial intelligence (AI) has also benefited scammers. These days, threat actors can use AI to generate well-written and highly targeted phishing messages that can convince vulnerable individuals. Related to this is the use of deepfake to enhance their impersonation tactics. In fact, Jon Clay, Vice President of Threat Intelligence at Trend Micro, warned about a future where autonomous AI agents could enable 24 x 7 automated scam operations.

Fighting against Fraud

In his keynote speech, Lord Sir David Hanson of Flint, Minister of State with Responsibility for Fraud, Home Office, said, “We have to reduce scams and fraud; reduce it and stop its growth in areas that have yet to be determined downstream. We need to, as has been said by colleagues here this morning, hold criminals accountable for their actions, pursue them relentlessly, and make sure we get criminal justice outcomes for the victims of these crimes.”

In line with this urgency to bring scammers to justice and minimize the occurrence of crimes, the U.K. government outlined a strategy that aims to reduce fraud through six focus areas:

- Data sharing
- Tech and telecom company accountability

- International cooperation
- Economic impact
- Public awareness
- Emerging threats, such as AI

Some of these priorities were recurring themes in the fight against fraud at GASS London.

Collaboration and Intelligence Sharing

GASS London emphasized the importance of cooperation between law enforcement, government agencies, ISPs, registries, telecommunications service providers, brand protection companies, payment operators, cybersecurity companies, and other public and private stakeholders.

Intelligence sharing among these sectors plays a major role in the fight against fraud and scams, as each stakeholder only sees a part of the puzzle. Alexandre François, WhoisXML API Product Marketing Director, concurs, saying, “One of the unique aspects of intelligence signals is that they become more powerful and valuable when shared. It takes collaboration and coming together to see the fuller picture so security and anti-fraud professionals are empowered to better fight scams or any other cybercrime, for that matter.”

Speakers at GASS London revealed that some collaborative efforts have already taken place. The Global Signal Exchange, for example, is a cross-sector partnership initiated by Google, GASA, and DNSRF, designed to serve as a clearinghouse for real-time data sharing related to online scams and fraud.

Banks, telecommunications service providers, and tech companies have also taken the initiative in sharing intelligence. Telecom data is helping banks better understand risks, detect scam activity faster, and respond in real time. As a result, payment networks like Mastercard can track the flow of payments across the broader network and detect different types of scams by analyzing the endpoints and frequency of transactions.

According to Adam Speakman, Head of Fraud Systems and Controls at the Lloyds Banking Group, collaborating with tech and telecom service providers gave banks “better insight into the risk of where the money is being sent.”

Artificial Intelligence

The escalating use of AI in fraud and scams was another highlight. Several discussions centered on strategically leveraging AI to detect and understand sophisticated scams and, more importantly, put scammers in a weaker position.

Employing AI for advanced fraud behavior monitoring is one method, as AI’s pattern recognition capabilities can be valuable in detecting subtleties in communication and transaction patterns that may indicate fraudulent activity (e.g., cold messages typical of scams).

AI and related new technologies have so much potential, and it takes a forward-looking cybersecurity community to take advantage of these modern tech advancements.

One promising avenue that recently emerged involves deploying AI chatbots to engage and waste the time of scammers. These scambaiting bots are trained on real scam call scripts and equipped with realistic artificial voices to keep scammers occupied in lengthy conversations, thereby preventing them from targeting actual victims.

Fraud Reporting

Aside from technological defenses, another best practice for fighting fraud and scams is reporting fraud. This is often underestimated, but each reported incident serves as an early warning sign that could potentially prevent more victims from suffering financial losses.

Encouraging the public to report fraud is crucial and further aligns with the event’s call for cross-sector collaboration. Every report, whether filed with law enforcement, financial institutions, or fraud-reporting platforms, contributes to a larger pool of data that can then be analyzed to quickly identify and stop widespread scam campaigns.

Targeting Fraud Infrastructure

Finally, there were discussions about disrupting scam operations on a large scale. In one example cited by Abigail Bishop, Head of External Relations (Scam Prevention) at Amazon, the combined efforts of Amazon, Microsoft, and Indian law enforcement agencies led to the shutdown of a massive scam network comprising 76 fraudulent call centers. She also emphasized that “tens of thousands of fraudulent websites and phone numbers on an annual basis are taken down through the power of information sharing with our partners.”

This aligns with what WhoisXML API Strategic Partnerships Director, David Hagberg, says about criminal infrastructure. “Scammers always rely on infrastructure to operate. This often includes websites and behind them domains, subdomains, and IP addresses. Meticulously tracking these digital footprints can help the fraud-fighting community dismantle scam operations at scale.”

About WhoisXML API

WhoisXML API is a leading provider of cyber intelligence solutions that can significantly empower fraud fighters in targeting and disrupting scam infrastructure.

Our predictive threat intelligence data feeds leverage AI predictive analytics capabilities, enabling organizations to detect potential scams, phishing, and fraudulent domains at the time of registration. We understand the power of collaboration and, as such, ensure seamless integration by providing data sources in well-parsed and unified formats.

We maintain strong collaborative relationships with major data providers worldwide, including domain registries and registrars, ISPs, and security agencies. Our network of data aggregators enables us to provide comprehensive, accurate, and up-to-date domain, IP, and DNS information.

For several years now, WhoisXML API has been recognized as an Inc. 5000 honoree and one of the Financial Times Top Fastest-Growing Companies. Our solutions are trusted by more than 52,000 users, including Fortune 500 companies, leading security firms, and organizations across various industries.