**No.85**
*April 2025*

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN- SPONSORED**

# Anti-Scam learnings from GASS London

HardenStance attended the Global Anti Scam Alliance's Global Anti Scam Summit (GASS) in London on March 26th. Here are the key takeaways:

- Around the world, government and industry recognizes that it has to step up and do a lot more to protect consumers against scams. They are assuming greater responsibility for disrupting scammers' business models as well as providing more timely, more helpful, support to consumers before, during and after scam attempts.
- Barriers to information sharing are still a big obstacle to government and industry acting decisively and consistently against scammers. The International Banking Federation, the Global Signals Exchange (GSE), Meta, GSMA and the UK's National Crime Agency (NCA) nevertheless shared encouraging examples of progress.
- We don't need "less" regulation or "more" regulation. Forget the commercial and political bluster - we need better regulation to help better protect consumers.

## Over 700 live attendees (+700 virtual attendees)

I was among over 700 in-person attendees at the Global Anti Scam Alliance (GASA) in London on Wednesday March 26th along with over 750 also registered online. Mike Haley, CEO of CIFAS, a UK-based fraud prevention community, called it "the largest ever meeting of the global counter fraud community." HardenStance came away thoroughly energized about how we can all get smarter about defending against online scams and about protecting consumers across industry sectors and national markets. Here are the five key takeaways from Day 1:

**#1 Politicians and regulators can no longer delegate responsibility for online fraud protection to industry alone. They are increasingly assuming more responsibility based on a more informed view of the scale of online fraud and the full extent of the damage it is inflicting on economies and societies.**

- *"We need criminal justice outcomes for the victims of scams. This is not acceptable any more. It requires political as well as business and other leadership." The Rt Hon Lord David Hanson, Minister of State with responsibility for fraud, UK Home Office.*
- *"In July 2024, President Marcos ordered scam hubs in the Philippines to be shut down. What they're doing is economic sabotage. More than 20,000 illegally trafficked people operating them have since being rescued and 3,000 individuals have been arrested." Alexander Ramos, Undersecretary, Cybercrime Investigation and Coordination Centre, The Philippines.*
- *"UK consumers lose $1.2 billion a year to fraud but if you factor in the effects of depression among victims the total cost is £9 billion. Many victims of investment scams never invest again so this is a bigger business problem." Rocio Concha, Chief Economist & Director of Policy, "Which?", the UK's consumer champion.*
- *"When consumers don't have confidence in buying online, it affects the economy." The Rt Hon Lord David Hanson, Minister of State with responsibility for fraud, UK Home Office.*

**#2 There is renewed enthusiasm for removing barriers to intelligence sharing among key counter fraud stakeholders – and some progress is being made.**

- *Nathaniel Gleicher, Meta's Global Head of Security Policy and Counter Fraud, pointed to the Fraud Intelligence Reciprocal Exchange (FIRE) programme, launched last October, whereby Meta is sharing fraud related intelligence with UK banks. This pilot has now been extended to FS-ISAC, the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system.*
- *The Global Signals Exchange (GSE) was formally launched on January 1st 2025. Founded by Google, the Global Anti Scam Alliance (GASA) and the DNS Research Federation (DNSRF), GSE's mission is to aggregate the threat intelligence of all its members and serve as a clearing house across different sectors of industry. It allows members to share threat intelligence in a way that fits with their organisational constraints, challenges and objectives, including discriminating between those organizations that can and cannot view their data. Other organizations have joined or are joining. Meta's Nathaniel Gleicher confirmed in his talk that Meta is one of those also joining GSE. He stated that "currently specific communities are building their own unique block lists. GSE allows us all to share and amplify the impact."*
- *Following pilots in October 2021 and February 2022, the UK's National Crime Agency (NCA) announced a partnership in July 2024 with NatWest and Lloyds among seven banks. This allows sharing of customer data in what Reuters called "the largest project of its kind worldwide" to tackle criminal gangs, money laundering and 'dirty money' flowing through the country.*
- *Vivek Badinrath, Director General of the GSMA, shared how since July 2024, UK telcos and banks have been collaborating through the Scam Signal API. Developed with the GSMA, this allows banks access to UK telco customer information relating to fraudulent activity. It enables the banks to make better decisions on whether to allow or block transactions.*
- *"We can share much more than we currently do without infringing GDPR. We at the International Banking Federation have this as a priority. We are going to publish everything we do and publicise how we can better collaborate." Hedwige Nuyens, CEO, International Banking Federation.*

**#3: The case made for either "less" or "more" regulation tends to be loaded with either political ideology or commercial self-interest. Left unchallenged, neither is helpful to disrupting fraud. What we actually need is better regulation that is more effective at protecting consumers. As has always been the case, this simply requires introducing new regulations that will work – and amending or getting rid of existing ones that don't.**

- *"Government-mandated scam alerts are not necessarily all that effective. If people get bombarded by things, they often ignore them." Jayde Richmond, General Manager, National Anti Scam Centre at the Australian Competition and Consumer Commission (ACCC).*
- *"We will do more independent fact-checking independent of the platforms to stop deep fakes that are wreaking havoc. Content creators need to be more transparent about any alterations they make. This needs to be done without infringing legitimate freedom of expression." Alexander Ramos, Undersecretary, Cybercrime Investigation and Coordination Centre, The Philippines.*
- *"We need information sharing platforms and to address what is blocking information sharing like GDPR. We need to be able to break those issues down, including legal and cross border legal issues." Manie Van Shalkwyk, Executive Director, Southern African Fraud Prevention Services.*

- *"Since October last year we've supported thousands of high profile public figures , for example by allowing the legitimate personas to access their accounts via video selfies. Adversaries adapt to our tools very quickly, though, so speed of deployment of our solutions is key. This was a global pilot but we couldn't roll it out at the same time in Europe because it took an extra six months to assure compliance." Nathaniel Gleicher, Meta's Global Head of Security Policy and Counter Fraud.*
- *"Should we think of instant payments as free, as a basic right? No! Because instant payments can mean instant fraud. When banks pick up the liability, their prices go up so consumers do end up paying. We need friction to tackle this so banks and regulators need to collaborate to create that friction." Hedwige Nuyens, CEO, International Banking Federation.*
- *"Regulators shouldn't get in the way of creativity. They shouldn't just mandate" Oliver Hanmer, Head of Supervision and Compliance Monitoring, UK's Payments Systems Regulator (PSR).*

**#4**: **Stressing the need for end users to protect themselves has too often served as an excuse for inaction by government and industry stakeholders. This part of the problem needs a lot less emphasis now. And the messaging industry does target at consumers also needs to be updated.**

- *"The most educated consumers will fall for fake videos. We need to go beyond education of consumers." Manie Van Shalkwyk, Executive Director, Southern African Fraud Prevention Services.*
- *"We have to change the dialogue. We have to talk about criminals not victims. We shouldn't be talking about something the victim did or didn't do. That framing is still prevalent but it's wrong now." Jayde Richmond, General Manager, National Anti Scam Centre at the Australian Competition and Consumer Commission (ACCC).*
- *"We have to recognize that it's not the citizen's fault." The Rt Hon Lord David Hanson, Minister of State with responsibility for fraud, UK Home Office.*
- *"We need to meet people where they are. They can get confused by some scam messaging. So we've moved from scary messaging to simple guidance at the right point in time. So simple messaging like 'slow down and stop', things like that. Jayde Richmond, General Manager, National Anti Scam Centre at the Australian Competition and Consumer Commission (ACCC).*
- *"We can't just arrest our way out of the problem We also have to focus on forcing scammers to adapt in ways that weaken them. We have to change their calculus from one with no consequences to one with consequences." Nathaniel Gleicher, Meta's Global Head of Security Policy and Counter Fraud.*
- *"We need to make fraudsters pay. We must find ways to reverse the transaction." Johannes Vallesverd, Senior Advisor, Norwegian Communications Authority.*
- *Olli Bliss, Business Development Manager, F-Secure, spoke to the importance of understanding the scam 'kill chain' as the basis for offering users real-time guidance on their devices at especially vulnerable moments in their online activity.*

**#5**: **Just as we strive to plan for post breach recovery in enterprise cybersecurity, we should aim for better recovery for consumer victims of fraud:**

- *"We can improve the victim's experience by careful data sharing between organizations. This can ensure a victim only has to report their experience once, not eight times to eight organizations." Jayde Richmond, General Manager, National Anti Scam Centre at the Australian Competition and Consumer Commission (ACCC).*

## More Information

- **Virtual Event**: Register for HardenStance's two-day "Telecom Threat Intelligence Summit 2025", taking place on June 10th and 11th 2025.
- **White Paper**: "Proven Ways to Block CLI Spoofing Scams" (March 2025)
- **Briefing**: "Telco Strategies for Consumer Security" (January 2025)
- **Briefing**: "Threat Intel in Telecoms (TTIS 2024)" (August 2024)

## About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security and is the organizer and host of the Telecom Threat Intelligence Summit. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The GSM Association, MEF, OASIS, ETSI. The Cyber Threat Alliance. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. www.hardenstance.com

## HardenStance Disclaimer