Home Office

ECONOMIC CRIME QUARTERLY

April 2025

Introduction

Welcome to the Economic Crime Quarterly, covering updates from Q1.

Spotlight

It has been a busy start to 2025, Lord Hanson chaired a successful Joint Fraud Task Force in March and recently spoke at the Global Anti Scams Summit.

There has been significant progress in the world of AI, with AI-enabled fraud reports on the rise. You can read more about this and the way AI is unfolding across the globe on page 3.

We have now delivered a total of 96 of the 146 ECP2 milestones (84 complete and 12 complete as ongoing BAU) with a further 21 in progress.

Newsletter Highlights

If you wish to discuss this newsletter in more detail or contribute to the next issue, please contact us at HOECSET@homeoffice.gov.uk.

Please do feel free to share this newsletter across your network.

Lord Hanson chairs the Joint Task Force

The Joint Fraud Taskforce (JFT) is a partnership between the private sector, government and law enforcement to tackle fraud collectively.

On 18 March, Lord Hanson chaired a successful JFT, with attendance and representation from major tech companies including Meta, X, and Match Group.

Both the Economic Secretary to the Treasury and Baroness Jones of Whitchurch (DSIT) attended. They emphasised the importance of not only private sector collaboration, but also the significance of cross governmental partnership to effectively tackle fraud.

Ministers thanked the tech and telcos sectors for their responses following the Mansion House speech and agreed to continue working further and faster to improve counter fraud efforts.

Key Highlights

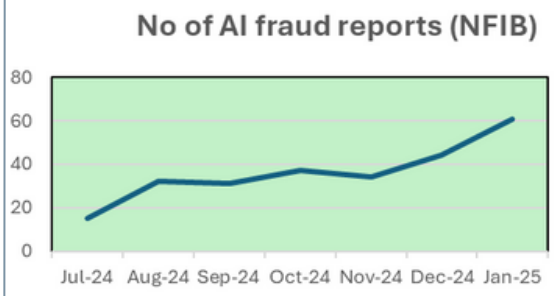
- The new Fraud Strategy engagement plan was set out which will rollout throughout the spring ensuring that voices from all stakeholders are captured
- A call out to the sector to engage with the workshops to ensure the next strategy is full of ambitious and actionable objectives
- JFT members encouraged to support the Stop! Think Fraud campaign
- The next JFT will be held in June

For further information and to view previous JFT minutes see here.

AI: Trends and Insights

The Headlines

- Reports of **AI-enabled fraud continue to rise** but remains a small proportion of all Action Fraud reports (~0.2%). Investment scams, fraudulent services / documents and romance scams are the most reported.
- The **Stop! Think Fraud** website now reflects deepfakes, such as CEO scams and voice cloning and includes advice on agreeing a safe phrase with family and trusted friends.
- **The joint DSIT / HO 'AI Harms Review'** continues to examine the harms from AI. Fraud and money laundering are in Phase 1. We've set out the harms and are now working on mitigations. Many thanks for the input received so far, it's much appreciated.
- We've been part of the HO team working on **AISI prompt testing**, which tests model compliance with criminal text-to-text prompts for financial crime and other harms. We are pleased to report that we will be the pilot for testing text to image / video prompts!
- In their latest SOC threat assessment, Europol highlight the impact of AI on organised crime, both as a catalyst for crime and as a driver for criminal efficiency. Similarly, the NCA's National Strategic Assessment features AI as cross cutting threat enabler.



Podcasts and Videos

Using AI for scambaiting is increasingly popular, check out Kitboga on YouTube and his army of chatbots to waste scammers time.

The Center for Human Technology have a podcast episode exploring the DeepSeek hype and how AI is learning to reason.

AI in the News

For a unique approach to tackling AI enabled investment scams, see Canada's own take on 'S!TF' with their campaign video, titled 'We're Not All F**ked' and fraud prevention campaign.

In January the release of Chinese LLM, DeepSeek, hit the headlines, shaking up the tech industry with low cost of development and high user downloads. Testing by cybersecurity companies (Qualys, Cisco and Enkrypt AI) has shown it is much worse than other commercial LLMs at blocking harmful content or identifying jailbreaks.

Prominent figures and businessmen targeted by an AI voice clone of Defence Minister Guido Crosetto

The Spanish government approved new legislation to combat deepfakes by imposing penalties on companies that don't adequately label content created by AI.

Fraud prevention and protection case studies

OPERATION HENHOUSE

433 people have been arrested in a UK-wide campaign against fraud, coordinated by the National Economic Crime Centre and City of London Police.

The activity, which was the fourth iteration of the multi-agency Operation Henhouse, ran across February 2025 and resulted in:

- **433** arrests
- **156** voluntary interviews
- **471** cease and desist notices
- Account freezing orders against **£4m**
- Seizures of cash and assets worth **£7.5m**

Every single UK police force and Regional Organised Crime Unit took part in the operation. They were joined by national agencies including the Financial Conduct Authority, National Crime Agency and National Trading Standards.

Several National Crime Agency investigations, into high harm transnational frauds, all of which involve its Complex Financial Crime Teams, are ongoing.

The results represent a **91% increase** on last year's cash seizure figures, and **28% increase** on last year's cease and desist figures under Operation Henhouse.

They show that through coordinated action, forces nationwide can tackle what is a complex and quickly evolving threat.

What is the Dedicated Card Payment Crime Unit?

It is a unique, proactive and fully operational police unit with a national remit, formed as a collaboration between UK Finance, the City of London Police and the Metropolitan Police Service.

Fraud is a truly terrible crime which takes many forms and can affect anyone. We are determined to meet the scale of the issue head-on.

The ongoing success of Operation Henhouse demonstrates the excellence of police and law enforcement partners, and the real-world impact of their activity to crack down on this truly pernicious crime.

We will continue to work closely with them to highlight the importance of the Stop! Think Fraud campaign, and to introduce a new expanded Fraud Strategy, as part of our Plan for Change.

The Rt Hon Lord Hanson

Fraud prevention and protection case studies

Click here to read more about Operation Henhouse.

The Police Service of Northern Ireland seized over £444,000, charged two people for fraud and money laundering offences, and engaged with 42 victims of fraud.

Police Scotland officers arrested a man and four women in connection with a multi-million-pound investment and money laundering investigation.

Essex Police executed six warrants, made 18 arrests, conducted 14 voluntary interviews with suspects, and froze or seized £890,000 in assets. Three individuals have already been charged.

In Merseyside, more than £2.7 million in suspected criminal cash and assets was seized or forfeited, including £900,000-worth of high-value watches. The force also issued five account freezing orders totalling over £128,000. .

Kent Police financial investigators returned nearly £1 million to a victim who was tricked out of the money in an investment scam. The force made more than 20 arrests, and seized £279,000 in cash and assets.

In Hampshire, officers arrested 13 people, voluntary interviewed five people, issued 33 cease and desist notices and served an additional 18 cease and desist letters. Alongside this, four account freezing orders were issued, totalling over £71,000.

Fraud prevention and protection case studies

BANKING PROTOCOL

Multiple parties were involved in the protection of a vulnerable victim in Leeds recently, including Leeds Anti-Social Behaviour Team, Social workers, DWP, West Yorkshire Police (WYP) safeguarding and Leeds Building Society.

The incident took place in a Leeds building society branch when an elderly vulnerable male customer with learning disabilities entered and asked for a withdrawal above an agreed cap.

The society colleagues were concerned that the elderly male was being financially exploited, as there were two people waiting outside the branch for him, and a change in activity was noted on the account.

The branch immediately instigated banking protocol: a partnership between industry and law enforcement where branch staff inform the police if they believe a customer is a potential victim of fraud. Whilst the suspects outside the branch had gone when the officers arrived, the victim advised more suspects were at his home address. WYP attended his home and officers made two arrests. It was also believed by WYP that the home address was being used for cuckooing.

After collaboration with Leeds Anti-Social Behaviour Team, Social workers and DWP, the victim has now been moved to supported living accommodation and his home address has been secured by the landlord to stop further issues.

The public can take steps to help protect themselves. It is essential that they continue to report fraud to Action Fraud, and follow advice found on the Stop! Think Fraud website. Every report helps the NCA and policing identify and support victims, prevent future fraud, repatriate losses, and target the criminals, wherever they are.

DID YOU KNOW?

Cuckooing occurs when a vulnerable individual is exploited in their home by groups or individuals so they can use the property for criminal purposes.

SARs Digital Service Delivery Update

Work to deliver the SARs Digital Service (SDS) continues with access now having been given to an initial pilot group of users within the UKFIU.

Since the start of the year the group has been testing a limited amount of the SDS's functionality. Feedback from these users has been helping to shape future developments, enabling the SARs Digital Transformation Programme to iron out glitches and consider suggestions for improvements.

Test users were initially able to view individual SARs by entering ID numbers. Now they can search across the available data in the SDS - which includes more than a million SARs submitted through the service's reporting channels - using simple search terms, such as names, addresses, phone numbers and dates of birth.

This early Search and View functionality will be made more widely available to the UKFIU this summer, before access is given to partners in Law Enforcement Agencies (LEAs) and Other Government Departments (OGDs) later in the year.

There will be a short testing period when onboarding partners, with a small number of pilot users, before making the service available to everyone.

Agile Delivery

This approach is in line with the SDS's delivery as part of an Agile programme, implementing the service in an iterative way. This is the recommended approach for delivering digital services across government and, rather than developing the whole of a service and launching it to users, aims to go live at an early stage with minimum functionality.

New features are built and delivered to meet users' needs as the programme progresses, learning from the experience of the early usage. This means everyone involved can have input into the way the service is developing - and any defects are relatively minor and can be corrected quickly. It also makes it easier to respond to, and accommodate, any change to business requirements or priorities.

The new SDS won't benefit all users to the same degree at the same time, but everyone's feedback will be valuable to help steer future development.

Data Transfer

The SARs accessible in the SDS are currently those submitted through the new channels, but an important part of the programme's work is also to transfer legacy data to the new service.

SARs submitted via older reporting channels are scheduled to be transferred during the late spring/early summer, meaning elements of the whole SAR database (details reporters have submitted) will be searchable when the service is delivered to partners.

The Law Society engages with Lord Hanson and the Fraud Strategy

The Law Society of England and Wales is pleased to support the launch of Lord Hanson's updated Fraud Strategy to include policies to protect businesses against fraud.

We have had discussions with the Home Office Fraud Policy Unit (FPU) to consider the wider fraud implications and work through the Economic Crime Task Force. The Home Office met with our Economic Crime Task Force to discuss the strategy and explore how the profession can further support the initiative going forward.

Following our discussions, the FPU has identified the following types of fraud that are being perpetrated against law firms:

- Payment diversion fraud (for example, following business email compromise or by spoofed email) in which a conveyancing client is instructed to send their payment to a different bank account)
- ID theft or synthetic ID in the client due diligence process
- Invoice fraud through vendor impersonation
- Investment frauds soliciting legitimate legal services to imply legitimacy
- Phishing attacks and using compromised data to take control of accounts directly or to use in other frauds

As highlighted in the recently published National Strategic Assessment of Serious and Organised Crime 2025 by the National Crime Agency (NCA), these types of fraud are not unique to the legal sector and affect many other sectors. Alongside the Solicitors Regulation Authority (SRA), the Law Society is committed to proactively providing advice to law firms, for example, by working with the NCA and Land Registry on conveyancing fraud and payment diversion fraud, as well as raising awareness around pension liberation fraud.

Our work on the digital trust ID framework and the National Economic Crime Centre public-private partnerships on AI fraud and client due diligence were also acknowledged in our discussions with the FPU. In relation to cyber resilience and fraud, the FPU intends to work with the Law Society Technology and Law Committee and joint Law Society and Bar Council cybersecurity working group.

We will be playing an active role in raising awareness and educating members of the public and solicitors about how they can be used to enable fraud unwittingly and become a participating victim.

We look forward to engaging in various roundtables hosted by the FPU throughout the year, ensuring that law firms have robust systems in place to mitigate the risks and protect themselves and their clients.

Ian Jeffery
Chief Executive Officer, Law Society of England and Wales

UK hosts milestone Border Security Summit

On 30 March – 1 April, the Home Secretary welcomed international partners to Lancaster House for the Border Security Summit: Organised Immigration Crime (OIC), a pivotal three-day event aimed at strengthening global cooperation against the Organised Criminal Groups (OCGs) driving illegal migration.

Bringing together senior Ministers and law enforcement officials with representation from 40 countries across Europe, Asia, and beyond, the Summit focused on developing unified strategies to disrupt the operations of criminal networks facilitating dangerous and illegal border crossings.

The Summit began with an evening reception at the National Gallery, offering a platform for informal dialogue ahead of formal discussions. The following day, Lancaster House played host to the Ministerial Day, attended by senior representatives of over 50 countries and international organisations. Concluding with a Law Enforcement Engagement Day, co-hosted by the Director General of the National Crime Agency (NCA) Graeme Biggar and the UK's Border Security Commander, Martin Hewitt CBE QPM.

A key theme running throughout the Summit was the importance of tackling the illicit finance that underpins organised immigration crime. Delegates discussed how criminal groups use international financial systems to move and hide money. By working more closely together and strengthening legislations, countries can do more to find and stop these money flows.

The summit also welcomed representatives from Meta, X, and TikTok discussing how to jointly tackle the online promotion of irregular migration. Several bilateral meetings took place between several countries which played a key role in deeping cooperation with international partners and allowed for more focussed one-on-one discussions, laying the groundwork for long-term collaboration.

Overall the summit marked a significant step forward in tackling organised immigration crime. By strengthening international partnerships and enhancing intelligence sharing, it has laid the foundation for greater security at the UK's borders and more effective global cooperation in addressing this shared challenge.

Home Office hosts the Global Anti Scams Summit

Global Anti Scams Summit

GASA (the Global Anti-Scam Alliance), Cifas, Euro Consumer and the UK Home Office hosted the Global Anti Scams Summit (GASS) London 2025 on 26 and 27 March at the Queen Elizabeth II Centre.

This was the world's largest fraud prevention event ever and bought together over 700 policy makers, industry experts, law enforcement and civil society.

Key focuses of the summit:

- International cooperation and collaboration needed to tackle fraud and scams.
- Plenary sessions and workshops discussed the threats posed by fraud and the opportunities for greater collaboration to stop fraud at source.
- Sessions also covered how we can harness the power of data, regulatory change and public private partnership, as well as the challenges and opportunities posed by AI and other emerging technologies.

Lord Hanson publicly launched the development of a new expanded Fraud Strategy which is a key manifesto commitment.

He also announced UK support for the next Global Fraud Summit.

This will be hosted by the UN Office on Drugs and Crime (UNODC) and INTERPOL in collaboration with the UK. It will be held early next year in Vienna and will be a pivotal moment in advancing a global response.

The Summit will invite a diverse range of participants, including all United Nations member states and INTERPOL members, along with representatives from civil society, the private sector, and international organisations.

Forward Look

June TBC  **Joint Fraud Taskforce**

Summer TBC  **Public Private Steering Group**