

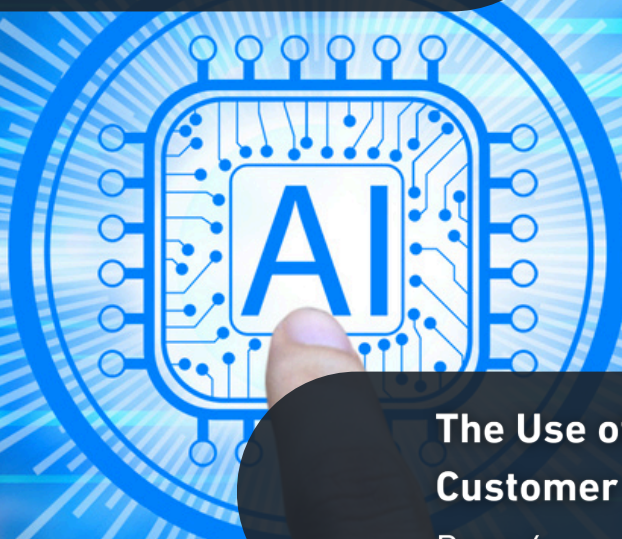
SIA

**SARs IN ACTION
MAGAZINE**



**UKFIU Support Fight Against Illegal Wildlife
Trade and Environmental Crime**

Page 3



**The Use of AI to Bypass
Customer Due Diligence Checks**

Page 6

**National Crime Agency
Operation DESTABILISE**

Page 10



A United Kingdom Financial Intelligence Unit
publication aimed at all stakeholders in the
Suspicious Activity Reports regime



Message from the head of the UKFIU



Vince O'Brien Deputy Director

Hello and welcome to the 30th issue of the UKFIU's magazine SARs in Action.

In our first issue of 2025, we highlight the support offered by the UKFIU in the fight against Illegal Wildlife Trade (IWT) and environmental crime and provide

a summary of the analysis conducted by the UKFIU Strategic & Statistical Analysis Team on SARs linked to IWT.

This is followed by a summary of the Amber Alert published by the NECC Illicit Finance Cryptoassets and Tech Enablers Team, which details the use of AI to bypass customer due diligence checks.

We take a closer look at the work of SARs Digital Service Delivery, their progress so far and what they have coming up in 2025.

The NCA, multi-agency Operation DESTABILISE disrupt two prominent Russian speaking networks, laundering billions of dollars annually.

And finally, we introduce the first of our new feature, "Dear UKFIU," where we look to answer your questions around SARs.

➔ Who is the magazine aimed at?

- All law enforcement; this includes senior investigating officers, frontline police officers and police staff
- Reporters
- Regulators
- Supervisors
- Trade bodies
- Government partners
- International partners

➔ Contents

UKFIU Support Fight Against Illegal Wildlife Trade	3
Illegal Wildlife Trade in Suspicious Activity Reports	5
The Use of AI to Bypass Customer Due Diligence Checks	6
SARs Digital Service Delivery Moves Into New Phase	8
Case Studies	9
National Crime Agency's Operation DESTABILISE	10
Dear UKFIU	12

➔ Opinions expressed in articles provided by partners are not necessarily the view of the UKFIU/NCA. The UKFIU exercises the right to edit submitted articles.

UKFIU SUPPORT THE FIGHT AGAINST THE ILLEGAL WILDLIFE TRADE AND ENVIRONMENTAL CRIME

Europol Financial Intelligence Public-Private Partnership (EFIPPP)

Illegal Wildlife Trade (IWT) and Environmental Crime are global challenges that threaten the biodiversity, ecosystems and the future of the planet. Recognising these challenges, the UK Financial Intelligence Unit is steadfast in its efforts to combat these crimes. The UKFIU have signed up to a number of initiatives to show our commitment to tackling this criminality.

In [Issue 25 of SARs In Action](#), the UKFIU highlighted two initiatives it supports:

1. Project Anton

UKFIU is key partner in Project Anton, a public-private partnership (PPP) led by Scotiabank and supported by FINTRAC (the Financial Transactions and Report Analysis Centre of Canada), The Royal Foundation's United for Wildlife and other international organisations. This initiative focusses on improving the detection of financial indicators linked to wildlife trafficking and increasing the reporting of this topic in suspicious activity reports.



2. United for Wildlife Statement of Principles

The UKFIU has also signed the United for Wildlife Statement of Principles for a Multilateral Approach to Combatting Illegal Wildlife Trade. These Principles emphasize international collaboration to detect and prevent the financial activity that sustains wildlife crime.

New International Partnerships

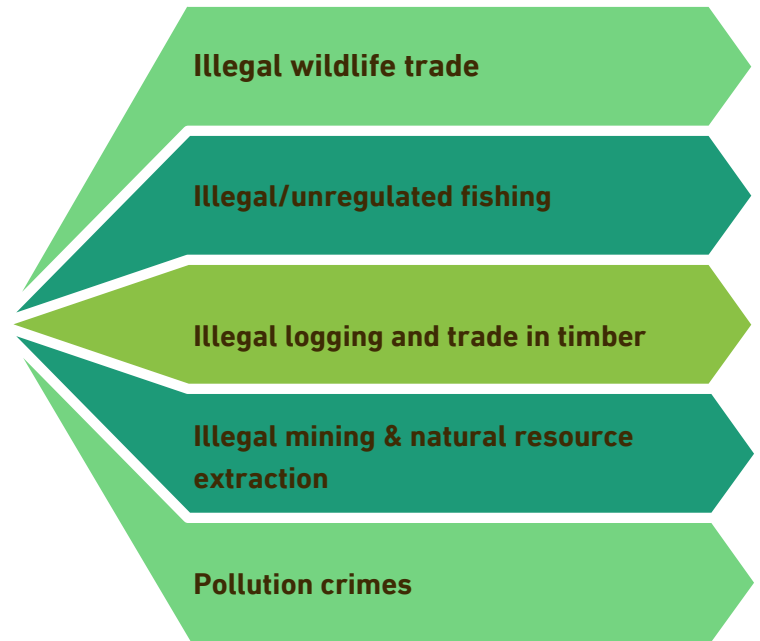
Since Issue 25, the UKFIU have further reinforced its commitment to tackling this criminality by signing up to further international initiatives.

1. EUROPOL Financial Intelligence PPP IWT Work Stream

The UKFIU is now a member of Europol's IWT work stream, a PPP being led by FINTRAC, with the support of Deutsche Bank. This PPP builds on Project Anton, tailoring its focus to the European context. The aim of this work stream is to produce resources to support the detection of financial transactions associated to IWT. The UKFIU works in partnership with the National Wildlife Crime Unit (NWCU) as part of this project to strengthen the collective response.

2. Egmont Group Environmental Crimes Project

The UKFIU is also contributing to the Egmont Groups Environmental Crimes Project under its Information and Exchange Working Group. This project aims to create awareness among FIUs of environmental crimes and their financial implications. A concept note outlines the projects focus on five key areas of environmental crime and the associated laundering of illicit proceeds:



Addressing the Financial Drivers of Environmental Crime

Europol,¹ has highlighted that environmental crime is highly lucrative and can be as profitable as illegal drug trafficking. However, the sanctions to dissuade this criminal activity are much lower and the crimes themselves are harder to detect. These factors make it highly attractive for organised crime groups.

The UKFIU is actively working to enhance the global understanding of environmental crime in these projects by identifying intelligence gaps, best practices to address vulnerabilities and fostering international cooperation.

Collaboration for Greater Impact



To achieve success, the UKFIU have enlisted the support and expertise of several UK law enforcement agencies to collaborate on these initiatives. The UKFIU will continue to collaborate with international partners, refine detection techniques and build stronger frameworks to disrupt the financial networks enabling these crimes.

¹ <https://www.europol.europa.eu/crime-areas/environmental-crime>

ILLEGAL WILDLIFE TRADE IN SUSPICIOUS ACTIVITY REPORTS

UKFIU Strategic & Statistical Analysis Team

Illegal Wildlife Trade (IWT) is one of the largest illegal trades in the world, worth approximately US \$20 billion per year and is increasingly linked with organised crime. Forms of illegal wildlife crime include the hunting and poaching of protected or non-domesticated species and plants, often for horns, ivory, bones, skins or meat. These derivatives are then sold to be used for food, medicines, as pets or ornamental displays.

In 2023, the UKFIU signed The United for Wildlife Statement of Principles for a Multilateral Approach to Combatting Illegal Wildlife Trade. This statement of principles acknowledges support for financial intelligence units (FIU) and other worldwide government bodies to detect and prevent financial activity that sustains wildlife crime.

The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) was established in 1975 and is a multilateral agreement among governments to regulate or ban international trade in species under threat. This convention has 184 members and trade is regulated in more than 38,000 species.



Analysis of Suspicious Activity Reports

The UKFIU conducted an analysis of IWT in suspicious activity reports (SARs). Between April 2020 and March 2024 IWT SAR submissions made up less than 0.2% of all SARs submitted to the UKFIU. Although there has been a slight increase in SARs relating to IWT over the years, submissions remain minimal in comparison to all SAR submissions per financial year. Given the size and scale of the IWT threat within the UK and globally, there is a realistic possibility that there are knowledge gaps around the identification of IWT and its indicators within financial activity, which is affecting reporting.



Following the launch of the new SAR portal, under the new reporting sectors, the banking sector submitted the majority (78.6%) of IWT SARs during financial year 2023/24. This is followed by the financial services sector (14.3%). It is likely that these sectors are most exposed to IWT related financial activity in comparison to other sectors, given the size of the sectors within SARs and the general economy.

Keywords such as *wildlife*, *endangered*, *trafficking* and *exotic animal* are seen frequently within IWT SAR submissions. However, there is minimal reference to UK specific IWT threats, such as glass eels and peregrine falcons. SARs referencing 'jewellery' and 'medicine' have also been identified, indicating the onward use of IWT within the UK.

THE USE OF AI TO BYPASS CUSTOMER DUE DILIGENCE CHECKS

NECC Illicit Finance Cryptoassets and Tech Enablers Team

Amber Alert

In October 2024, the Joint Money Laundering Intelligence Taskforce (JMLIT) published an Amber Alert¹ (0752-NECC) covering the use of Artificial Intelligence (AI) to bypass customer due diligence (CDD) checks.² The Alert was commissioned by the Public Private Crypto Forum, due to media coverage corroborated by industry partners. Accounts successfully created using AI are likely to be used for criminality, such as money laundering or terrorist financing.

The Alert, written following interviews with selected financial institutions, cryptocurrency exchanges and third-party specialists, noted the increasing sophistication and scale of such AI enabled attempts and provided examples of AI enabled:

Fake identity documents



Deepfake videos



Face swaps



The Alert

- Provided an overview of the threat and trend towards increasing sophistication
- Highlighted specific examples and case studies
- Outlined risk indicators that have been identified

¹ This Amber Alert has been shared with the JMLIT+ membership and is not publicly available.

² CDD describes measures firms have to take to identify and verify the identity of, customers and their beneficial owners. CDD and know-your-customer (KYC) are sometimes used interchangeably.

Positive Outcome

One website, which was identified as offering AI generated fake identity documents (including UK passports and driving licenses) for as little as US \$15 (approx. £12.50), has been taken down by the National Crime Agency (NCA).



Improving Understanding



A public private partnership time-limited cell (working group), exploring the use of AI to bypass CDD checks, is likely to be setup in early 2025. The cell will aim to improve understanding of the scale of such AI enabled attempts and update partners with the latest threats and indicators.

If you or your institution identifies activity which may be linked to the detail in this article, and there is a proceed of crime, you may wish to make a Suspicious Activity Report (SAR). **If you decide to make a report in this way, you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference [0752-NECC](#) for this Alert within the relevant field on the NCA SAR Portal.**



SARs DIGITAL SERVICE DELIVERY MOVES INTO NEW PHASE WITH A NEW YEAR

SARs Digital transformation

The SARs Digital Transformation Programme started 2025 with news that almost one million SARs have now been submitted through the new reporting channels.

It marks the start of an exciting year for the programme and follows a busy end to 2024, which finished with a test version of some of the improvements being made available to a group of users in the UKFIU. This group is currently testing the functionality and helping to shape future developments.



Transferring Legacy Data

Another important piece of work for the programme is the transfer of legacy data to the SDS. This is progressing and core elements of SARs submitted via the older reporting channels are scheduled to be transferred in the late spring/early summer.

“Extensive design, user research and infrastructure work continues to take place, involving those who will use the SDS which has been invaluable to the development of the service. The project team are grateful to all those who have taken time to provide feedback and give vital insights. All of this is helping us deliver a service that will bring long-term benefits in the prevention and disruption of money laundering, terrorist financing and other criminal activity.”

Martin Sidaway, SARs Digital Transformation Programme Director

Ongoing Progress

The SARs Digital Transformation Programme will provide further updates on its progress as it continues to deliver the SDS.

If you have any queries or feedback for the SARs Digital Transformation Programme, please email: SARsITTransformation@NCA.gov.uk

CASE STUDIES



A reporter submitted a suspicious activity report (SAR) suspecting their customer was the victim of a fraudulent foreign currency exchange trading scam. The customer had transferred in excess of £200,000 to suspected fraudsters and wished to send close to £40,000 more, in the belief that their money would then be returned to them. The reporter conducted open source research, identifying information suggesting the fraudsters had tricked others into repeatedly sending them credits. The UKFIU disseminated the SAR to the relevant law enforcement agency (LEA) who conducted a safeguarding visit to the customer and provided cyber scam advice. The customer agreed to not send further money to the fraudsters. The LEA also arranged a referral to a specialised cybercrime unit who were able to provide comprehensive advice and support to the customer in all aspects of the case.

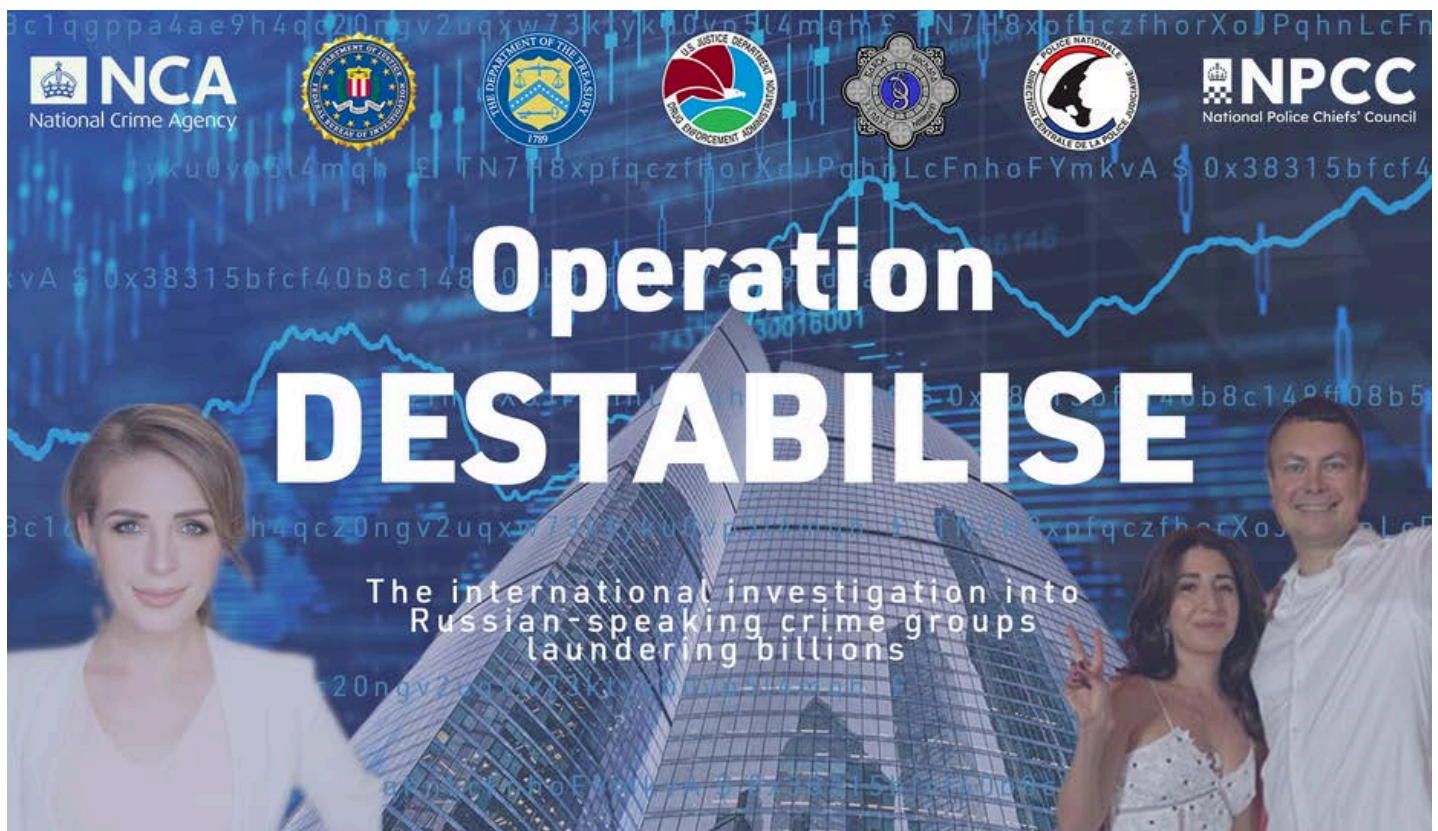
A reporter submitted a defence against money-laundering (DAML) SAR to return funds while exiting their relationship with a business. The reporter held concerns that the business account was being used to launder the proceeds of crime from other accounts. The account was receiving high value credits that were quickly dispersed to subjects linked to organised crime groups (OCGs). The reporter was also unable to verify the origin of credits with no evidence they resulted from legitimate business activity. The UKFIU refused the DAML SAR and fast-tracked the intelligence to the relevant law enforcement agency (LEA) who launched an investigation into the business and confirmed these funds were the proceeds of crime. As a result, the LEA was able to obtain an Account Freezing Order (AFO) and subsequent forfeiture of the account balance exceeding £74,000.



NATIONAL CRIME AGENCY OPERATION DESTABILISE

Operation DESTABILISE Tactical Lead

Operation DESTABILISE is a National Crime Agency (NCA) led international investigation into a series of Russian speaking networks laundering billions of dollars annually. The networks, known as the Smart Group and TGR, operate globally, offering services including swapping 'street cash' generated from the sales of drugs for cryptocurrency, to bypassing international sanctions on behalf of their illicit clients. Smart Group is led by Ekaterina Zhdanova (pictured left) and George Rossi (pictured right) leads TGR, alongside his second in command Elena Chirkinyan (pictured centre right).



The Networks have laundered for ransomware actors, the Kinehan organised crime group, oligarchs and international controller networks amongst others. Smart Group was also used to fund Russian espionage operations and TGR was involved in the transfer of funds linked to a sanctioned Russian media organisation.

The networks operated at scale, using the traditional banking sector and cryptocurrency markets to launder. UKFIU reporting enabled the identification of how the networks were abusing these sectors. This was critical to supporting the success of Operation DESTABILISE, especially at the early stages of the investigation.

The UKFIU also facilitated liaison with relevant overseas partners, enabling the further collection of financial intelligence. Additionally, the Joint Money Laundering Intelligence Taskforce (JMLIT) played the key role of consolidating reporting from across Operation DESTABILISE lines of effort and disseminating a concise report to members to prevent these networks from further abusing the financial sector.



The NCA worked with a series of UK and overseas partners to disrupt the networks. In December 2024, the US Office of Foreign Asset Control (OFAC) announced nine designations on TGR and members of Smart Group. Simultaneously, the NCA announced the results of Operation DESTABILISE, a three year investigation into the networks, detailing the arrest of 84 linked individuals and the seizure of £20 million. Through the NCA, OFAC and other partner activity, the networks have been disrupted at every level, from cash couriers to international controllers.

DEAR UKFIU.....



Q: Anonymous

Dear UKFIU,

I've submitted plenty of SARs but have never had any response or feedback from the NCA or the police to indicate they've started an investigation, why is that?

A: UKFIU Agony Aunt

Michael, UKFIU Senior Engagement Officer, Reporter Engagement Team



Great question! The UKFIU receives more than 800,000 SARs every year. After a period of 7-10 days, the majority of SARs are made available to specially trained and accredited law enforcement officers across the United Kingdom. This distributed model for SARs means that the intelligence derived from the reports can be used in a wide range of investigations, and not just financial crime investigations. SARs also remain available and searchable by law enforcement for six years from the date of submission, meaning the SARs database currently contains more than 4.5 million SARs.

Given the volume of SARs received annually, the number of SARs held on the database, the wide range of investigations SARs can be used in, and the often-sensitive nature of those investigations, it is not possible for reporters to receive a response or feedback on every SAR submitted. However, the UKFIU does publish a series of [Reporter Booklets](#) every year containing case studies of where SARs have supported investigations undertaken by law enforcement. You can keep up to date with the latest Reporter Booklet by following the UKFIU on [LinkedIn](#) or [X](#).

It's also important to remember that the NCA is not a crime reporting agency and SARs are not crime reports. There is no guarantee your SAR will lead to an investigation. SARs are for reporting knowledge or suspicion of money laundering or terrorist financing, therefore in addition to a SAR you may have to report a suspected crime directly to an appropriate law enforcement agency e.g. the police or HMRC. Where you do report a crime alongside a SAR, it's best practice to include the crime reference and the organisation you reported the crime to in the required field on the SAR Portal.

"Dear UKFIU" will be a new regular feature where we answer questions posed by you. If you have a question for the UKFIU Reporter Engagement Team that you would like to see answered in a future issue of SARs in Action, please email it to UKFIUEngagement@nca.gov.uk.

SIA

SARs IN ACTION

You can download previous copies of the SARs IN ACTION magazine from the National Crime Agency's website www.nca.gov.uk



UKFIU

UK Financial Intelligence Unit



Episode 20

AVAILABLE HERE

THE UKFIU PODCAST

Educational podcast series discussing areas of interest related to the SARs regime and economic crime.



Our podcasts can be found on Spotify, Audible, Amazon Music and most streaming sites.



Updates can also be found on our LinkedIn page and on X (formerly Twitter) at [NCA_UKFIU](https://twitter.com/NCA_UKFIU).

