

SARs IN ACTION

Issue 19 - April 2023

Page 23

SARs Annual Report 2022

Page 5

Modern Slavery and Human Trafficking

Page 3

New SARs Portal

Page 18

UK Art Market Sector



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 19th issue of the UKFIU's magazine *SARs in Action*.

We open the issue with an analysis from the NCA's National Assessments Centre (NAC) on Modern Slavery and Human Trafficking (MSHT).

This analysis has informed intelligence gaps around the roles of online platforms in MSHT and refers to episode 2 of the UKFIU's podcast in which indicators of MSHT were discussed for reporters. Issue 18 of *SARs in Action* also contained an article on indicators of sexual exploitation and page 7 of this edition of the magazine highlights a good law enforcement outcome following the publication of this article.

Elsewhere in this issue, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) comment on the illegal wildlife trade following the issuing of an operational Alert related to this. We also look at SARs related to cryptocurrency, trust or company service providers and Police Scotland describe how they use SARs and the process their Serious and Organised Financial Crime Intelligence Unit go through between receiving SARs to using intelligence to fulfill their duties to protect people, places and communities in Scotland.

Further updates related to the UKFIU can also be found in this issue including the publication of the SARs Annual Report, the new SARs confidentiality breach line, Arena training and an increase in the threshold amount specified in the Proceeds of Crime Act. We also have two new podcast episodes on Evolving Payments and Banking Firms and the UK Fraud Communications Toolkit, available now on most streaming sites.

➔ Who is the magazine aimed at?

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

➔ Contents

New SARs Portal.....	3
Modern Slavery.....	5
News in Brief.....	8
Illegal Wildlife Trade.....	9
Cryptocurrencies and SARs.....	11
Trust or Company Service Providers.....	13
How Police Scotland use SARs...	15
Case Studies.....	17
The UK Art Market Sector.....	18
The Financial Crime Information Network.....	20
Bribery and Corruption Risks.....	22
SARs Annual Report 2022.....	23
Modern Slavery Event.....	24
Threshold Change.....	25
SAR Confidentiality Breach Line...	26
UKFIU People Stories.....	27

➔ 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.

NEW SAR REPORTING IS LIVE!

We are excited to share that as of 22 March the first six reporting organisations have started to use the new SAR portal to submit SARs.

This is a significant milestone for the Programme, as it is the first live application on the new NCA Tier 1 cloud environment. Moreover, every submission made on the new SAR portal will improve the quality and structure of the SAR data, which will ultimately enhance the use of SARs to better protect the public.

The hard work, collaboration and dedication of everyone involved has ensured that we have achieved this key milestone, and it will enable improved exploitation of the SAR data to prevent and disrupt money laundering and other criminal activities.

As well as the new SAR portal, we have also gone live with a new Bulk API technology which allows our high-volume SAR reporters to submit SARs reliably in bulk using more modern reporting technology that allows for enhanced data quality. We expect the first live SARs to be submitted in April.

Where can I get support to understand what is changing for me?

We have published three new user guides and an FAQ document on the 'Suspicious Activity Reports' page on the NCA website.



For reporters:

- 1 [Click here](#) for an overview of the new SAR Portal and how to submit SARs.
- 2 [Click here](#) for guidance on how to register to the new SAR portal.
- 3 [Click here](#) to access the FAQ document.

For NCA officers, law enforcement or government departments:

- 1 [Click here](#) for an overview of how to view and analyse SARs when submitted using new reporting channels.
- 2 In addition to the user guide, we will shortly be circulating a recorded 'Awareness Session' webinar, which provides an overview of the key changes as a result of the Reporter Release.

What happens next?

Building on the first release, the next phase of the SARs IT Transformation will enable the decommissioning of the legacy SARs IT systems. The ambition is to merge 17 applications into one to deliver a single, integrated SARs digital service for the UKFIU, the NCA, reporters, law enforcement partners, and other government departments.

We have recently commenced a Discovery phase, in accordance with guidance issued by the Government on best practice delivery of digital services. During this phase, we are engaging with user communities to ensure that we are addressing the contemporary business needs, whilst exploring technologies that best support future solution options.

As we deliver the rest of the end-to-end digital service we will continuously improve the service to maximise the value from SARs data in our efforts to protect the public and disrupt organised crime.



For any questions about the work we are doing or how it will impact you, please contact SARsITTransformation@nca.gov.uk

MODERN SLAVERY AND HUMAN TRAFFICKING

The NCA's National Assessments Centre (NAC) has recently conducted analysis to inform strategic intelligence gaps around the role of online platforms in the recruitment of Modern Slavery and Human Trafficking (MSHT) victims.

The analysis has identified that it is highly likely that the majority of MSHT recruitment, both within and to the UK, is enabled by online spaces.

It is almost certain that the scale of online recruitment in MSHT is increasing. However, this is almost certainly reflective of wider societal trends in internet usage rather than trends unique to MSHT offending. This includes a growing number of people identifying employment opportunities and romantic relationships online, in addition to the continued proliferation of social media and other online platforms in the UK and key MSHT source countries.



This trend has almost certainly been accelerated by the global COVID-19 pandemic and the resulting growth in the use of online platforms to communicate in professional environments.

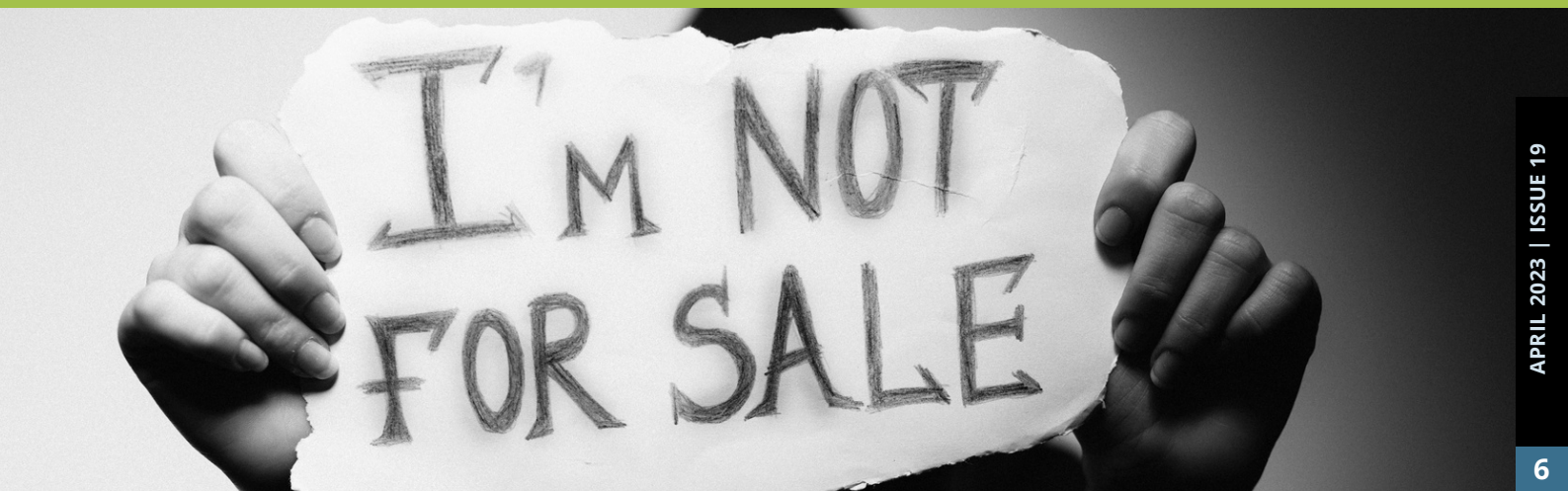
- ① It is **highly likely** that **social media, classified ads sites based in source countries, and end-to-end encrypted (E2EE) messaging apps are the most commonly used** platforms by MSHT organised crime groups (OCGs) during recruitment.
- ② It is **highly likely** that **social media is the most attractive platform for MSHT OCGs during recruitment**, providing a number of opportunities for MSHT OCGs, including target discovery and private communication with victims.
- ③ It is **highly likely** that **classified ads sites based in source countries**, including those that advertise sexual services, are used at scale by MSHT OCGs during recruitment. These sites primarily **enable lured recruitment, whereby OCGs are able to post fake job adverts for an extended period of time**. This enables potential victims to contact offenders and ensure that OCGs are constantly sourcing new potential victims with minimal effort.



Adverts on classified ads sites primarily consist of vague work opportunities in the UK, offering higher wages than those in source countries. Furthermore, despite purporting to be a company or organisation, adverts often lack further contact details, such as a website or email address, or further details around recruitment policies and procedures.

Potential victims are therefore required to contact offenders directly via mobile, enabling the offender to displace contact onto more private communication methods, such as messaging apps.

- ④ It is highly likely that MSHT OCGs, across all forms of exploitation, use E2EE messaging apps during recruitment. In the majority of cases, messaging apps complement face-to-face initiated contact, or contact initiated by other types of online platforms, by enabling the on-going deceptive or coercive messaging that persuades a potential victim to travel to (or within) the UK.
- ⑤ It is highly likely that MSHT OCGs will **increasingly rely on online recruitment over the next three years**, continuing the trend of the last three years.



Next steps

UK law enforcement's understanding and response to the role of online platforms is highly likely to be enhanced by a sequential strategy consisting of three distinct phases:

- ① Enhance the intelligence picture
- ② Identify and risk score priority online platforms, and
- ③ Engage and educate platforms to mitigate risk through the 3Ps (Prevent, Prepare and Protect) strategies.

Once the scope of online platforms is better understood on a national scale, using existing strategies to identify priority platforms will almost certainly ensure that UK law enforcement's resources are directed towards the most impactful platforms.

Once priority online platforms have been identified, a coordinated and centralised UK law enforcement strategy targeted at the enablers of recruitment is likely to partially disrupt OCGs' ability to recruit using online spaces. This includes engaging with priority online platforms to describe the enabling functions of their platform and making them more difficult for OCGs to infiltrate, while also encouraging open communication channels, information flows, and education of the MSHT threat.

Episode 2: How SARs reporters can help combat MSHT

SAR reporters can assist in identifying instances of MSHT by checking out episode 2 of the UKFIU podcast (available on most streaming sites) and also the guidance documents on the NCA website – 'Indicators of MSHT in the Accountancy Sector' and 'Indicators of MSHT in the Legal Sector' – which include potential red flag indicators attributable to all sectors.



[CLICK HERE](#)

If the indicators assist you in identifying suspicious behaviour in relation to money laundering, then please use the **glossary code XXMSHTXX** in your SARs. This helps analysis and the fast tracking processes in place to protect the public. In parallel, if you suspect MSHT is taking place, then please contact the police and, in an emergency, dial 999; for non-emergency dial 101. Additional advice can be sought from the **Modern Slavery helpline on 0800 0121 700**.

Following publication of Issue 18 (December 2022) of the SARs *In Action* magazine, the UKFIU was contacted by Norfolk Constabulary enquiring about an article in that issue.

The piece in question, headed 'Potential indicators of sexual exploitation', related to information provided in an Amber Alert issued by the Joint Money Laundering Intelligence Taskforce (JMLIT) and the National Economic Crime Centre (NECC). Norfolk Constabulary were keen to speak to the author of the Alert as they felt that they could attribute the vast majority of the red flag indicators within the Alert to potential victims in an investigation of their own.

POTENTIAL INDICATORS OF SEXUAL EXPLOITATION

The following relates to information provided in an Amber Alert issued by the Joint Money Laundering Intelligence Taskforce (JMLIT) and the National Economic Crime Centre (NECC) in August 2022.

UK law enforcement's understanding of the sexual exploitation threat has increased dramatically in recent years, particularly in relation to the key drivers, enablers and coercion methods underpinning the sexual exploitation business model.

In this article we provide a number of red flag indicators which, in combination, may demonstrate a heightened risk of potential sexual exploitation activity to persons over the age of 18. This refers directly to both offender and victim financial behaviours. **The presence of a single indicator should not be interpreted as being indicative of sexual exploitation; these indicators are not exhaustive and there may be others not highlighted.**

It is also worth clarifying that the provision of sexual services within the UK is legal and victims of sexual exploitation are highly likely to represent a small minority of those working in the sex industry.

A distinction should also be made between adult services websites (ASWs) providing advertising for sexual services, and websites that provide generic classified advertising space, including the advertising of sexual services. This may assist with account monitoring, and institutions should recognise the potential significant and wide-ranging impacts that immediate account closure may have on an independent sex worker. As such, **payments solely to ASWs should not be interpreted as a definitive indicator of potential sexual exploitation, and further investigation is necessary.**

Remember – if you suspect someone may be engaged in modern slavery/human trafficking (MSHT) offending or is a potential victim there are a number of ways to report your concerns:

- In an emergency if you believe there is an **immediate threat to life/a crime in action** phone 999.
- For non-emergencies call the police on 101 or the Modern Slavery Helpline on 0800 0121 700. Alternatively you can file a report at www.modernslaveryhelpline.org/report
- If you identify activity which may be indicative of the activity outlined, and your business falls under the regulated sector, you may wish to submit a SAR to the UKFIU. Please include the SAR glossary code X0MSHT0X and reference number 0634-NECC. This latter number relates to the JMLIT Alert.

Transaccional/general

- Regular payments to ASWs or escort agencies that advertise sexual services.
- Multiple payments to ASWs from the same account may indicate that the account holder is in control of a number of potential victims.
- A significant proportion of account activity taking place overnight, particularly between 22:00 – 07:00, including payments to ASWs, cash credits, ATM withdrawals or for travel and accommodation.
- Payments received from numerous third parties for rounded values, particularly those including a payment reference from clients suggesting sexual services have been provided.
- Receipt of multiple credits, both in cash and faster payments, from multiple locations or IP addresses linked to different locations across the UK. This may suggest that the account holder is being moved across the UK to provide sexual services, or that the account holder manages multiple venues associated to potential sexual exploitation.
- Funds transferred to a third party shortly after payments into the account. It may be that the payment references for the credits into the account may provide indication of sexual service provision.
- Multiple credits into the account received from numerous locations across the UK and, once consolidated, transferred in bulk to another third party account, either in the UK or overseas.
- Regular credits into an account, often with payment references including female names not consistent with customer account details, or sexual services.
- ATM withdrawals of suspected client payments, leaving minimal balances.
- A lack of expected account payments, such as salary payments or household spending.

Behavioural indicators

These indicators can suggest organisation/control of the account holder's activity by another person/s.

- Multiple account holders registered at the same address and/or use of the same telephone number, IP address or device to access multiple accounts for mobile and online banking.
- Multiple devices accessing a single mobile or online bank account.
- Coaching through account set-up, whether via video on-boarding or in-branch, or a third party acting as a 'translator', 'guardian', and friend or 'relative'.
- Open source investigation of a prospective account holder identifying multiple links to advertising on ASWs, such as a telephone number associated to multiple adverts and/or profiles.

Travel and accommodation

Patterns of travel and accommodation bookings can demonstrate the movement of potential victims into and across the UK. They can also highlight more organised and large-scale sexual industry, indicating the presence of an organised crime group.

- Payments to budget airlines to and from locations typically identified as source countries for potential victims of MSHT, particularly where the traveller's name does not match the name of the account holder, or the account holder has made multiple bookings on behalf of other people.
- Frequent payments for UK airport/port car-parking, particularly with no subsequent overseas travel exhibited on the account.
- Regular payments to toll roads and ancillary vehicle travel spending such as petrol costs, payments at service stations etc., both within and outside of the UK.
- High volume and/or frequent transport costs on the same card, particularly where the timings and locations of payments do not correspond with a single person using the card, e.g. transport in London, followed by payment for transport in Birmingham shortly afterwards.
- Concurrent card payments to transport providers, such as TFL, app-based taxi companies and rideshares predominantly occurring between the hours of 22:00 – 07:00.
- Ad-hoc and last minute payments for accommodation, particularly hotels, B&Bs and short-term property rentals.
- Payments for multiple accommodation providers, including hotels, B&Bs, and short- and long-term property rentals.
- Payments for accommodation not following expected patterns, e.g. multiple payments on the same dates for accommodation across the UK, or payments for accommodation within close proximity to the registered address of the account holder.
- Registered addresses of the account holder inconsistent with the customer profiles.
- Numbers of account holders registered to one address inconsistent with the house size. This may suggest multiple sex workers operating within an unlicensed House of Multiple Occupancy.

Ancillary expenditure

The following indicators, when observed at high frequency or volume, can suggest that the provision of sexual services has increased in scale, and that there may be numerous victims under a controller or facilitator. Whilst these indicators can also be seen within legitimate escort agency business models, they can, in combination with other factors, also provide an indication of sexual exploitation.

- Payments to cosmetic and beauty service providers (pharmacies, cosmetic suppliers and tanning salons), bulk purchasing of contraception and erotic clothing providers. There have also been anecdotal reports of bulk purchasing of gym memberships.
- Multiple mobile phone, SIM and contract payments not in line with the account holder's stated occupation.

SARs In Action, Issue 18

It is anticipated that as many of the red flag indicators are present in Norfolk's enquiry, that this will aid their argument that the offender/s have financial coercion/control over the potential victim's account.

ILLEGAL WILDLIFE TRADE

Barry MacKillop
Deputy Director
Intelligence Sector
Financial Transactions and Reports Analysis Centre of Canada



Canada's financial intelligence unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), recently [published an Operational Alert](#) with money laundering indicators related to the illegal wildlife trade, meant to assist businesses in identifying and reporting financial transactions related to the laundering of proceeds of crime from this appalling and cruel crime. This, in turn, will facilitate the production of actionable financial intelligence in support of law enforcement investigations in Canada and abroad.



FINTRAC's Operational Alert was developed in support of Project Anton, a new international public-private partnership aimed at improving awareness and understanding of the global threat posed by illegal wildlife trade, and targeting the laundering of proceeds from this crime domestically and internationally.

This initiative was named in honour of Anton Mzimba, Head of Security at the Timbavati Private Nature Reserve and a Global Conservation Technical Advisor, who was murdered in 2022 for his passionate commitment to protecting and conserving wildlife.

Project Anton is led by Scotiabank in Canada and supported by The Royal Foundation's United for Wildlife network, which was founded by His Royal Highness Prince William, FINTRAC, Australian Transaction Reports and Analysis Centre (AUSTRAC) Fintel Alliance, the South African Anti-Money Laundering Integrated Task Force, the UKFIU, Western Union and numerous other government, law enforcement and non-governmental organisations in Canada and around the world with unique knowledge, expertise and tools in combatting illegal wildlife trade.

FINTRAC would like to recognise all of its partners, including the UKFIU and the UK National Wildlife Crime Unit, for their valuable input on our Operational Alert and significant engagement on Project Anton.

Illegal wildlife trade is a crime that poses a serious environmental, economic, security and public health threat in Canada and around the world.

It is a **major and growing threat to the global environment and biodiversity**, imperiling endangered species already on the edge of survival, and threatening fragile habitats, communities and livelihoods. Illegal wildlife trade can also have **significant public health impacts**, as the circulation of animal parts increases the chances of disease transmission and can be a path for future pandemics.

The Financial Action Task Force has identified illegal wildlife trade as a major transnational organised crime, which generates billions – some have estimated approximately 20 billion USD – of criminal proceeds each year.



According to the Wildlife Justice Commission, illegal wildlife trade is considered a lucrative, **low risk and high reward criminal activity**, and often involves fraud schemes, tax evasion and other serious crimes that facilitate the illicit enterprise. The Commission has also found that OCGs involved in wildlife crime are often involved in other domestic and internationally connected criminal activity such as human trafficking, drug trafficking, firearm trafficking and money laundering.

A 2020 report by the United Nations Office on Drugs and Crime highlighted that suspected illegal wildlife traffickers from 150 countries had been identified, illustrating that wildlife crime is a global issue. This demonstrates the importance of establishing a committed global network of public and private sector entities to combat this appalling crime.

Project Anton will facilitate the ongoing engagement and sharing of information between partners domestically and internationally, where authorities permit, and **enhance collective knowledge** of money laundering methods, typologies and indicators as more information and intelligence is gathered from the reporting from businesses.

Ultimately, by following the money and generating actionable financial intelligence for law enforcement in Canada and around the world, **Project Anton will assist in identifying, pursuing and prosecuting perpetrators – and broader networks – linked to illegal wildlife trade.**

CRYPTOCURRENCIES AND SARs

As part of its remit to undertake strategic assessments using SAR data, the UKFIU recently analysed cryptocurrency SAR volumes.

Cryptocurrency SAR volumes show an overall downward trend since September 2021. The decrease follows moves by a number of banks to restrict direct payments to cryptocurrency exchanges, following concerns over levels of fraud, particularly investment fraud.

The decrease in cryptocurrency SAR volumes pre-dates the crash in cryptocurrency values that occurred in May 2022.

Despite this fall in banking cryptocurrency SARs, the banking sector continued to submit the largest proportion (60%) of SARs referring to cryptocurrency. 2021 saw a number of banks restrict direct payments to cryptocurrency exchanges, in response to rising levels of fraud, in particular investment fraud.

Through SAR analysis, it was seen that cryptocurrency exchanges primarily reported either the receipt of fraud funds or customer interaction with darknet marketplaces. However, it must be stressed that SARs are indicators of suspicion rather than confirmed criminal activity. Reporter risk appetite can play a role in the decision to submit a SAR and therefore impact on SAR volumes.

Non-banking reporters of SARs

Analysing cryptocurrency SARs from reporters outside the banking sector is not straightforward. When reporters register with the UKFIU for SAR submission they self-select the most appropriate industry sector listed within the UKFIU database.

However, due to its relative newness, there is currently no specific SAR sector category for those dealing in cryptocurrency. Cryptocurrency reporting is therefore primarily split across two UKFIU categories: 'Electronic Payment' and 'Other'. 'Other' is a 'catch-all' category selected by reporters who consider that no suitable category currently exists for their specific activities.



Cryptocurrency SARs within these two groupings are primarily reported by three types of reporter:

- trading platforms dealing exclusively in cryptocurrencies (cryptocurrency exchanges)
- 'hybrid' digital platforms which allow customers to hold, transfer and trade both fiat and cryptocurrencies; and
- crypto-friendly electronic money institutions which continue to allow direct transfers to cryptocurrency exchanges.

In suspicious activity reported by cryptocurrency exchanges, reports relating to fraud accounted for just over 50% of their SARs.

Approximately one quarter of cryptocurrency fraud SARs related to investment fraud, where the victim had been scammed into setting up a cryptocurrency wallet, with the promise of significant returns on their investment. In many cases the wallet is then controlled by unknown actors, and the funds withdrawn without the victim's consent.

The other main suspicious activity reported in cryptocurrency exchanges' SARs was the direct or indirect transfer of cryptocurrency to or from addresses associated with darknet market places.

Due to the global nature of cryptocurrency exchange operating models, many of their SARs related to overseas account holders, with no apparent UK connection.

Reporter Engagement

The UKFIU Reporter Engagement Team meets every quarter with several Financial Conduct Authority-regulated cryptocurrency firms at the Crypto Currency Working Group (CCWG). Typically these meetings bring together stakeholders from different providers that share insights into the sector, and the UKFIU provides industry best practice to assist the operational effectiveness of the SARs regime and allow law enforcement to better exploit the intelligence.

The UKFIU will be working with representatives from the CCWG in 2023 to invite guest speakers from law enforcement, who have specialties relating to the crypto sector, to meetings.

TRUST OR COMPANY SERVICE PROVIDERS

The UKFIU regularly conducts SAR reviews to provide an overview of the SARs submitted by the different sectors under anti-money laundering (AML) supervision.

The UKFIU recently looked at the Trust or Company Service Providers (TCSPs) sector to understand the changes in SAR data associated with this sector in detail and to review the quality of SARs submitted by this sector.



A TCSP is defined under Section 12(2) of the Money Laundering Regulations as a firm or sole practitioner which by way of business provides any of the following services; forms companies or other legal persons; acts or arranges for another person to act as a director, secretary, partner or nominee shareholder; provides registered office, business address, correspondence or administrative address; acts or arranges for another person to act as a trustee for an express trust or similar and a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

TCSPs can provide a number of services including:

- ▶ Formation services (company or trust)
- ▶ Nominee services (director, partner, secretary or shareholder)
- ▶ Address services (registered, trading, administrative or correspondence).

The National Risk Assessment 2020 categorises the TCSP Sector as **high risk from money laundering** and low risk from terrorist financing.

TCSPs can be exploited, either wittingly or unwittingly, to enable the laundering of significant illicit flows through companies, partnerships and trusts. They often offer services which can enhance the attractiveness of companies and partnerships to criminals, for example increasing anonymity or creating complex structures.

Although UK companies and partnerships can be set-up directly with Companies House with comparative ease and low cost, approximately half of corporate entities are still established through TCSPs. TCSPs offer a convenient method to establish a company for legal purposes, but many of their services can be exploited by criminals, including the use of nominee directorships, UK mail forwarding services and providing a registration address for hundreds of companies at single addresses.

This is particularly attractive for those establishing a UK company from overseas, since the company must have a UK registered officer to serve as its official address but is not required to operate in the UK or have a UK bank account.

SAR volumes

The TCSP sector is proportionately a small reporting sector among SAR submissions representing 0.02% of all SARs submitted for the 2021/22 financial year.

However, SARs for this sector are increasing year-on-year. This could have been influenced by a number of policy changes introduced to tackle the vulnerabilities faced by the sector, including:

- ① Policy changes, including The Persons of Significant Control register expanded in 2017 requiring Scottish limited partnerships (SLPs) to file their beneficial ownership information.
- ② The Department for Business, Energy & Industrial Strategy Corporate Transparency and Registration Reform programme and their Limited Partnership reform programme improving accuracy and usability of data on the companies register, helping to understand who is setting up, managing and controlling corporate entities.
- ③ The introduction of discrepancy reporting in January 2020 as part of the EU's 5th Money Laundering Directive (5MLD), improving the quality of beneficial ownership data held on the Person of Significant Control register.
- ④ Expansion to include trust registration as per the 5MLD to require registration of UK express trusts and two further sorts of trusts.

Another influencing factor could be the work the National Economic Crime Centre (NECC) has undertaken with law enforcement partners including HMRC. The NECC has been identifying TCSPs who represent the highest risk to the UK and tasking supervisory bodies with monitoring and action.

Themes identified in reporting suspicious activity

These differ to the risks highlighted in the National Risk Assessment. The main themes of reporting in TCSP SARs were:

- ▶ AML compliance issues where the subjects have accessed TCSP services but are failing to comply with continued due diligence requirements
- ▶ supplying false documentation
- ▶ law enforcement interest
- ▶ identity fraud

Small themes included credit card fraud, adverse media and concerns of tax or sanctions evasion.

UKFIU analysis identified that over 60% of 'main' entities did not include an address, resulting in the SARs not being allocated to law enforcement (copied only to HMRC) but remaining searchable on intelligence systems.

HOW POLICE SCOTLAND USE SARs

Detective Sergeant Greig McOustra
Serious and Organised Crime Financial Intelligence Unit
Police Scotland

Police Scotland's Serious and Organised Crime Financial Intelligence Unit is based at the Scottish Crime Campus just outside Glasgow. It consists of a dedicated team of financial investigators and intelligence officers.



Scottish Crime Campus

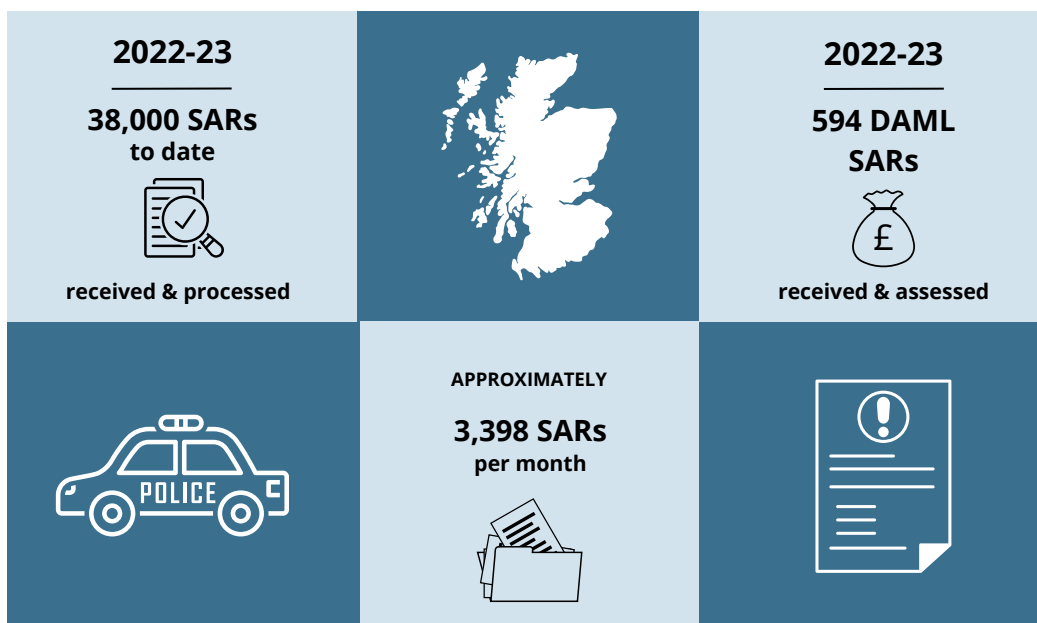
The team reviews all SARs, Defence Against Money Laundering (DAML) SARs and fast-tracked SARs allocated to them by the UKFIU.

The assessment of SARs relating to vulnerable people is prioritised and the intelligence on the SAR is used, with information available on local and national databases, to build a picture and make an informed assessment of the possible financial exploitation. This could include romance frauds, abuse of position or human trafficking. These assessments are used to create intelligence packages which are passed to local officers to enable a visit to the potential victim, investigate any reported criminality and to put in place any required protective measures.

The intelligence received from SARs is incredibly useful. In the majority of cases the potential victims are either previously unknown to police or they are documented in relation to other vulnerabilities not just financial exploitation. Through our engagement with local officers and other partners we have been able to safeguard vulnerable people and bring the individuals who have been exploiting them to justice.

We also have responsibility to assess and allocate all DAML SARs for Police Scotland including the administration regarding the recommendations for granting/refusing consent, as well as liaising with the UKFIU in respect of Moratorium updates in the year 2022/23. We received and assessed 594 DAML SARs which resulted in a number of restraints, account freezing orders and S107 of Proceeds of Crime Act 2002 seizures (variations of confiscation orders).

As well as dealing with fast-tracked and DAML SARs, the team read, assess, research and analyse all SARs allocated to Police Scotland. In 2022/23 to date, this has been just over 38,000 SARs, which equates to an average of 3,398 SARs per month.



By reading every SAR the team can **assess the intelligence and identify emerging or changing crime trends and profiles**. SARs which are suitable for further investigation and those of an enhanced intelligence value to different business areas are also assessed.

The information provided in SARs, such as customers' personal information, transaction information or the actual summary of the disclosure, is invaluable during criminal investigations and this information is not readily available to investigators who are not trained financial investigators. It is anticipated that through the new SAR Researcher Programme, SARs will be utilised more and provide a highly useful source of intelligence for the wider organisation.

Our work is focused towards Police Scotland's priorities of protecting vulnerable people, tackling digital and cybercrimes and supporting operational policing, fulfilling our purpose of improving the safety and wellbeing of people, places and communities in Scotland.

CASE STUDIES

1 A reporter submitted a DAML SAR following concerns of money laundering due to high value transactions made by a customer. The UKFIU refused the DAML request, allowing the relevant law enforcement agency (LEA) to investigate the customer, revealing that the customer was charging for VAT services but not making the returns. This allowed the LEA to seek an account freezing order (AFO), which was granted and resulted in over £400,000 being forfeited.

2 A DAML SAR was submitted after a disqualified director (the subject) was found to be operating a limited company, whilst also likely engaging in tax evasion and money laundering. The UKFIU refused the DAML request and information was disseminated to the relevant LEA. The investigation found that the subject had significantly under declared their tax liabilities. An AFO was obtained leading to a successful forfeiture of almost £300,000.

3 A reporter submitted a DAML SAR to return funds to a suspect after the suspect received high value cryptocurrency payments following a long period of no activity on the suspect's account. The UKFIU fast-tracked the DAML SAR, refusing the request. This intelligence was shared with the relevant LEA whose investigation resulted in obtaining an AFO in excess of £1m on multiple accounts held by the suspect. Enquiries are ongoing.

4 A DAML SAR was submitted due to concerns that an individual was using their business account for illicit activities including money laundering and tax evasion. The reporter's checks also identified transactions from the business account to a number of high risk businesses in several countries. The UKFIU refused the DAML request, and intelligence was disseminated to the relevant LEA whose enquiries determined that the individual had declared no income, resulting in the LEA successfully obtaining an AFO for over £5m. Enquiries are ongoing.

TAX EVASION

THE UK ART MARKET SECTOR

The UKFIU regularly conducts strategic and statistical analysis of SARs to review and analyse issues, themes and trends in more depth. As part of this remit, the UKFIU recently looked at the UK art market sector.

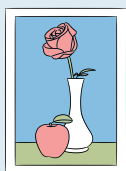
It was announced in July 2019 that as part of the implementation of the EU's 5th Anti-Money Laundering Directive, businesses carrying out art market activity in the UK would be required to register with HMRC from January 2020, carry out customer due diligence and report SARs. These businesses are referred to hereafter as art market participants (AMPs).

From the date AMPs were brought under scope, AMPs were initially given 12 months to register with HMRC, up to January 2021; this was extended for a further six months due to COVID-19, up to June 2021.

What is an AMP?

The term AMPs refers to businesses trading in or storing works of art at a value of EUR 10,000 or more.

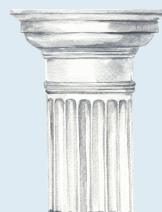
The term works of art is defined, following the Money Laundering Regulations (MLRs), as the objects specified under the VAT Act 1994, Section 21 6 to 6B:



a painting, drawing, collage, decorative plaque (or similar)



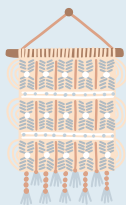
a sculpture cast



an original sculpture or statuary



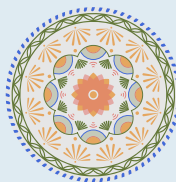
an original engraving, lithograph, or other print



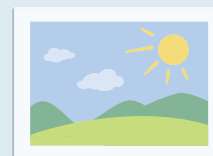
a tapestry or other hanging



a ceramic



an enamel on copper



a photograph

This does not include non-fungible tokens or antiquities in general.

As defined by the MLRs, AMPs are distinct from high value dealers (HVDs). AMPs may include auction houses, which may fall under the definition of an AMP, an HVD, both, or under neither inasmuch only as they are either carrying out activity falling under each definition in the MLRs.

HM Treasury's National Risk Assessment of Money Laundering and Terrorist Financing 2020 (NRA 2020), issued 17 December 2020, assessed AMPs as High Risk for money laundering and Low Risk for terrorist financing. The NRA 2020 cited risks/vulnerabilities as the 'ability to conceal the beneficial owners and the final destination of art, as well as the wide-ranging values involved, the size of the market and the international nature of the market'. When the NRA was published, it was too early to assess the effectiveness of new regulation for AMPs to mitigate these factors, leading AMPs to be categorised as High Risk.



Analysis by the UKFIU



Themes identified by the UKFIU within art market SARs were varied and included (in order of prevalence):

- ▶ general money laundering
- ▶ bribery and corruption
- ▶ tax evasion
- ▶ professional enabling activity
- ▶ Politically Exposed Persons
- ▶ stolen or looted art and sanctions evasion



Transactional volumes of money laundered via art sales or of the art sales themselves are difficult to establish accurately through SAR reporting. In many cases reporters will only know the value of funds they see to or from an AMP's accounts, particularly for reporting on the art market by banks.

The UKFIU has assessed that it is highly likely that opportunities to report suspicious financial activity within the art market are being missed by AMPs themselves. It is also likely that reporting by AMPs will increase, as their understanding of their new obligations under the MLRs increases.

THE FINANCIAL CRIME INFORMATION NETWORK


FIN-NET Secretariat

FIN-NET

Financial Crime
Information Network

Did you know that there is an information sharing network in the UK that provides **rapid access to information about financial crime** held by over 100 organisations including law enforcement, financial and specialist regulators, and anti-money laundering/counter-terrorist financing (AML/CTF) supervisors?

FIN-NET brings together a unique range of organisations representing different sectors, all with a remit around financial crime. Using the FIN-NET referral network is a simple way to request assistance from organisations that you may not otherwise be able to easily reach. With a FIN-NET Single Point of Contact (SPOC) in each organisation we can help you make contact when urgent advice or information is needed.



If you work for UK law enforcement, you are automatically eligible to use FIN-NET. You may also be able to use FIN-NET if you are a regulator or professional body supervisor.

“

Operating for over 30 years with a proven track record, FIN-NET helps its members share confidential information about fraud, money laundering, terrorist financing, bribery and corruption and serious regulatory breaches.

”

Using FIN-NET can help you reach a unique group of organisations including:



all UK law enforcement



financial regulators, including the Financial Conduct Authority and equivalent financial regulators in some overseas jurisdictions and crown dependencies



AML/CTF supervisors across the accountancy and legal sectors



public bodies, including government departments and specialist regulators.

By completing one simple form you can ask FIN-NET members if they have any information relevant to your investigation. You can also use FIN-NET to alert members to a particular individual or organised crime group operating across the UK or share a new modus operandi that you are seeing.

Here's how using FIN-NET can supplement information you have received through a SAR or help your investigations:

- ▶ Deconfliction – who else is investigating your subject of interest?
- ▶ Receiving new intelligence to support your case
- ▶ Corroboration of existing intelligence
- ▶ Identification of previously unknown victims
- ▶ Making use of alternative powers (for example, what started as a police investigation may, by working with the regulator or AML supervisor, lead to a disruption or conclusion using that organisations specialist powers).
- ▶ A SPOC in each membership organisation allows rapid access to specialist knowledge (for example assistance with newly emerging modus operandi (MO)).




For more information about FIN-NET, whether your organisation is a member, how to submit a referral, or to arrange a training session about using FIN-NET for your team, contact us at ffinsec@fca.org.uk

BRIBERY AND CORRUPTION RISKS TO UK INDEPENDENT SCHOOLS

An Alert on bribery and corruption risks to UK independent schools is available on the [NCA website](#), issued by the Joint Money Laundering Intelligence Taskforce (JMLIT).¹

Issued with the support of the Home Office, the Independent Schools Council, the Independent Schools Bursars Association and the Office of Financial Sanctions Implementation, the purpose of the Alert is to review the methods through which the proceeds of bribery and corruption may be placed into the independent school sector, including through the circumvention of financial sanctions regulations and to highlight red flags which may help identify this type of activity.

The Alert is primarily aimed at assisting:

-  banks that provide financial services to the UK independent school sector and seek to ensure their products and services are not used to launder the proceeds of crime
-  other supporting professions providing audit, legal and accountancy services, which may be best placed to identify activities of concern and proceeds of corruption; and
-  the independent school sector.

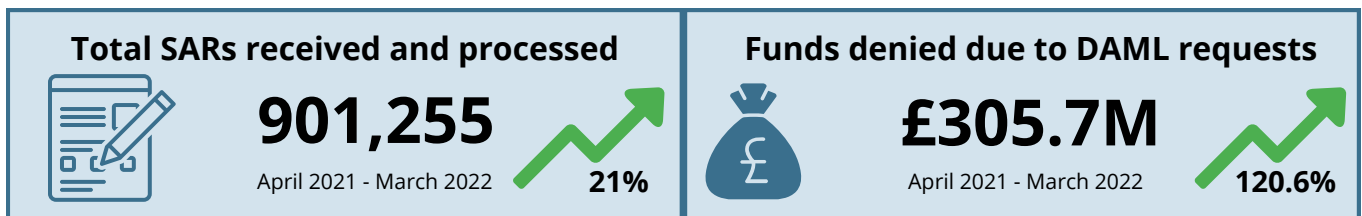
If you identify activity, which may be indicative of the activity detailed in the Alert, and your business falls under the regulated sector, you may wish to make a SAR. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help analysis if you include the **SAR glossary code XXJMLXX** within the text and the **reference 0581-NECC for this Alert**.

¹ The independent schools sector includes all UK fee-charging schools including state boarding schools.

SARs ANNUAL REPORT 2022

The 2022 SARs Annual Report, which features statistics covering the years 2020-21 and 2021-22, has now been published by the UKFIU on the NCA's website.

The latest report shows:



The financial and predicate crimes intelligence provided by SARs has proved to be invaluable as criminals sought to take advantage of the pandemic to advance their illicit enterprises. More recently, as a result of Russia's invasion of Ukraine, SARs have provided increasingly important information on money laundering linked to sanctioned individuals and their associated entities.

In 2022, the NCA set up the new **Combatting Kleptocracy Cell (CKC)**, with a remit that includes the investigation of criminal sanctions evasion and high end money laundering.

SARs are an important component of the information coming into the cell, and the UKFIU – which receives, processes and assesses SARs on behalf of the NCA – now has a dedicated team to work as part of the CKC.

Under the SARs Reform Project the UKFIU has undertaken a significant transformation since the last report with new methods of working and new teams. This has included an **uplift in staff to over 150 and measures are in place to reach the target of 201** by the end of the next financial year, driving increased analysis and engagement within the SARs regime.

Vince O'Brien, Head of the UKFIU, said: "SARs are vital to the fight against money laundering, illicit finance and wider criminality. Major improvements to the UKFIU through the SARs Reform Project, including the establishment of dedicated analytical teams to support specific operational requirements such as those of the Combatting Kleptocracy Cell, and further enhancements rolling out over the next 24 months, will ensure we maximise the intelligence value derived from SARs, driving greater impact on economic and other crime, and helping to keep the UK public and businesses safe."

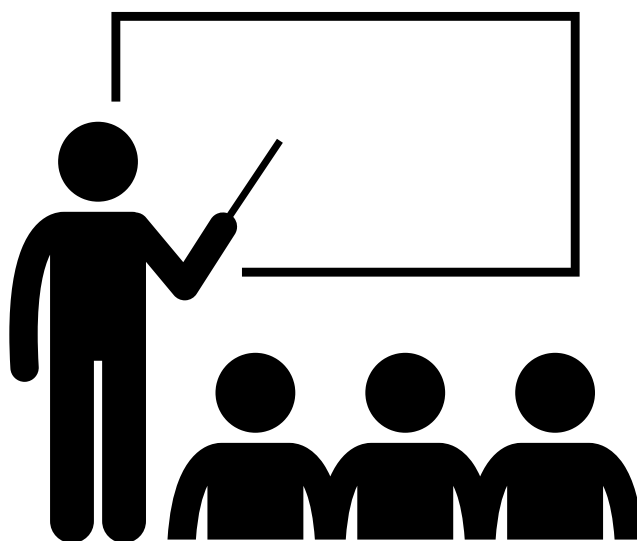
The report can be found on the NCA website [here](#).



MODERN SLAVERY ILLICIT FINANCE EVENT

In January the UKFIU SARs Exploitation Team (SET) delivered a presentation at a Continuous Professional Development (CPD) event in Bristol with a focus on illicit finances within Modern Slavery and Human Trafficking (MSHT). The event was hosted by the NCA's MSHT Unit, the South West Regional Organised Crime Unit and the National Police Chiefs' Council's Modern Slavery and Organised Immigration Crime Unit.

A number of points were covered that illustrated the value of SARs in identifying MSHT links through the use of Arena.



The event was well attended and highlighted the value of SARs in all forms of investigation. Following the presentation, the SET received requests from multiple LEAs requesting bespoke Arena training packages. As a result, Arena has seen an uptick in users, indicating greater LEA exploitation of SARs intelligence.

If you wish to receive the Arena training presentation, please contact the team at: SARsExploitationTeam@nca.gov.uk



THRESHOLD CHANGE

From the 5th January 2023 the £250 threshold amount, specified in section 339A of the Proceeds of Crime Act 2022 (POCA), increased to £1,000. The threshold amount is the value of criminal property below which a bank or similar firm (a deposit-taking body, electronic money or payment institution) can carry out a transaction, in operating an account for a customer, without committing one of the main money laundering offences in sections 327 to 329 of POCA..

- The Statutory Instrument increasing the threshold can be found at: The Proceeds of Crime (Money Laundering) (Threshold Amount) Order 2022 (legislation.gov.uk)
- Further guidance on the current threshold, and submitting better quality SARs more generally, can be found on the [NCA website](#).

Deposit taking institutions with concerns that an account may contain the proceeds of crime/used for laundering money may still have to process regular 'lifestyle' payments to/from that account. Legislation permits discretion in relation to such payments, up to a threshold of £250 per transaction. If frequent transactions are over this threshold, the reporter can apply to the NCA for a threshold variation under POCA and seek permission to impose a higher threshold for regular transactions.

SAR CONFIDENTIALITY BREACH LINE

The UKFIU has recently updated its dedicated helpline for reporting sectors to raise concerns about the inappropriate use of SARs by end users (individuals with authority to view or submit SARs) or breaches of SAR confidentiality.

This dedicated helpline number for the SAR Confidentiality Breach Line is 0207 238 1860 and is a 24 hour line.

This will allow the user to advise the UKFIU as soon as there is an awareness of a potential breach of confidentiality of a SAR, irrespective of whether the breach is unplanned or is compelled by the direction of a court.

Here are a few examples of inappropriate use of SARs by end users and breaches of SAR confidentiality, where the user should contact the UKFIU SAR Confidentiality Breach Line:

- ▶ a SAR has been revealed (inadvertently or otherwise)
- ▶ a SAR is in the process of being challenged by a defence team at court
- ▶ a SAR is subject to protracted debate between prosecution and defence during any investigation
- ▶ if any concerns are raised by any member of the reporting sector
- ▶ there is any other issue that causes the user concern over SAR confidentiality.

Please only contact the UKFIU SAR Confidentiality Breach Line for this purpose and not for general UKFIU and SAR queries.

If you do require assistance with general UKFIU and SAR queries please contact the dedicated number or email provided in the table below.

If you require further information on the SAR Confidentiality Breach Line please contact the UKFIU Disclosure Team (email provided below).

General UKFIU and SAR enquiries	0207 238 8282 or UKFIUSARs@nca.gov.uk
SAR Confidentiality Breach Line	0207 238 1860 (24 hour line available from Monday to Sunday) or UKFIU.DisclosureTeam@nca.gov.uk

Day in the Life Fiona - Operational Support

How I got here

In my role I oversee all the teams in the Operational Support function of the UKFIU. This is my 14th year in the agency and my first in the UKFIU.

I wasn't sure what I wanted to do after leaving university and applied to lots of different organisations. I picked the NCA as I wanted to be in London and thought it sounded like something a bit different!

What's kept me here is the varied and interesting nature of the work we do, the friendly and supportive teams I have worked on and the enjoyable work-life balance.

“ I have the privilege of helping to shape how the UK will tackle crimes ”

I've loved the different opportunities I've been able to take advantage of: working as an intelligence officer; on an international desk with opportunities for travel; in a victim identification unit; within operational teams; delivering training to national and international law enforcement agencies and the industry partnerships team.

When the opportunity came up to join the senior management team at the UKFIU I was excited to take on a leadership role and get exposure to a whole new crime type again.

In recent years, my focus has been much more on business strategy and the corporate side of the NCA. I now focus on delivering outcomes that have a long-term impact on how the agency fundamentally operates and tackles different crime threats.



My role and how I protect the public

My Operational Support teams enable the UKFIU to deliver priority activities, covering a range of areas from business support to how we report performance as a unit, handle our risk management, developing policies and processes to help the UKFIU do what it does to the best of its capability.

We regularly engage with teams across the NCA, wider government, LEAs and the private sector. We are constantly thinking about what we need to do for the future to protect the public, staying abreast of legislative changes and developing those bigger picture, long-term solutions.

If my teams didn't do what they do, the UKFIU could not effectively operate and the public would be less safe.

On a great day

For me a great day is one where I get to engage with lots of passionate people to collaborate on work with real meaning – whether that be my own teams, wider UKFIU teams, the rest of the NCA or partners. That is always interesting. The human element of any job is important to me and this really is a supportive environment to work in.

Work that is focused on the future of the UKFIU is always exciting as my teams and I have the privilege of helping to shape how the UK will tackle crimes such as money laundering and terrorist finance for years to come.



On a typical day

I can't say there is one typical day in this job. In any one day I may be doing a number of activities from: working with the team to prepare a Director General briefing; meeting with key stakeholders on how to future-proof the UKFIU; reviewing our risk register and making sure we have the right mitigations in place; arranging visits for our Home Office partners to collaborate on how SAR data can be exploited to support wider government activity; or reviewing and updating our policies on things such as whistleblowing or how we train our people.

To find out more about working at the UKFIU please see the [NCA website](#).

Missed an issue?

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



“

We'd love to hear what you think of the publication, what topics you'd like us to consider and we're always open for possible articles and collaborations. Please send any feedback to ukfiufeedback@nca.gov.uk

”



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



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

