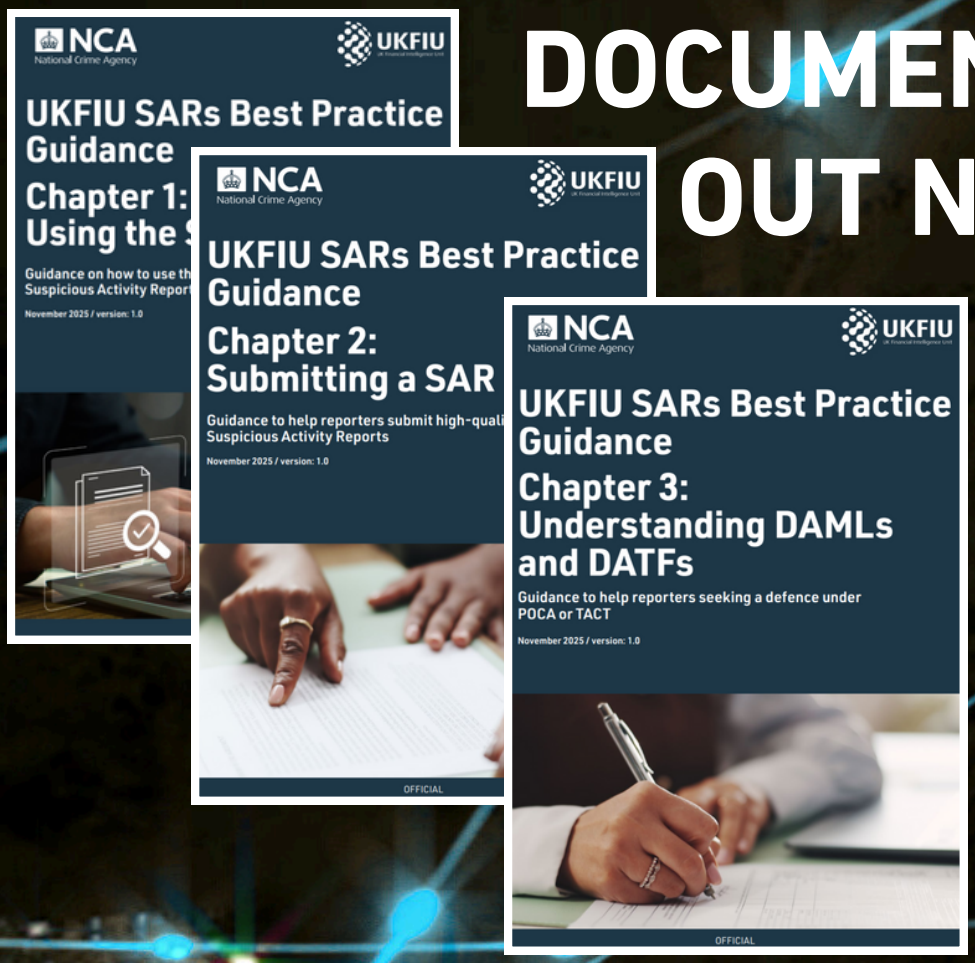
Issue 34

SIA
SARs IN ACTION MAGAZINE

UKFIU
UK Financial Intelligence Unit

NEW GUIDANCE DOCUMENTS OUT NOW



TACKLING BRIBERY AND CORRUPTION ACROSS THE UK

Coordinating the national policing response to domestic bribery and corruption

CHILD SEXUAL ABUSE MATERIAL in SARs

UKFIU analysis of CSAM SARs

THE EGMONT GROUP

30 years of partnership

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

NCA
National Crime Agency

Message from the Head of the UKFIU

Vince O'Brien
Deputy Director

Hello and welcome to Issue 34 of the UKFIU's magazine, SARs in Action.

We open with the release of updated UKFIU guidance documents. These are vital reading for all SAR reporters, and replace previous guidance documents issued by the UKFIU.

Following on from this, we focus on the issue of Child Sexual Abuse (CSA) and the analysis that has been completed by the UKFIU and partners to better understand and report this horrendous crime. We have also included articles on the growing threat of Financially Motivated Sexual Extortion (FMSE) and the threat of fraud by Organised Crime Groups against the Student Finance System.

In support of International Anti-Corruption Day (9 December 2025), we hear from the City of London Police on how they lead and coordinate the national policing response to bribery and corruption, and the NCA's International Corruption Unit, who continue to combat those aiming to exploit the system for their personal gain.

We also take a look at insights resulting from EMMA 10, a Europol led intensification that targets money muling. Then a look at Egmont, a key organisation the UKFIU engages with regularly to maximize the impact of the SAR regime globally, facilitating the UKFIU's ability to support the UK and international law enforcement.

In this issue, the SARs IT Programme Team provide an update on the SARs Digital Service (SDS), a key component in updating the the IT of the SARs regime.

Finally, to conclude this issue, we include case studies demonstrating the positive outcome of 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

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 UKFIU guidance

New SARs Best Practice Guidance

The UKFIU has published a brand-new suite of Suspicious Activity Reports (SARs) Best Practice guidance documents, which has replaced all previous UKFIU guidance documents and will be vital reading for all UK SAR reporters.

We ask that you **delete all previous versions of the guidance** from your internal systems and platforms to avoid any confusion.

The new guidance comprises of three chapters, covering the following topics:

- Chapter 1: Using the SAR Portal
- Chapter 2: Submitting a Good Quality SAR
- Chapter 3: Understanding DAMLs and DATFs

The guidance can be accessed, by scanning this QR code:

Or using this link: https://bit.ly/4oRYGyu

Reporters are also reminded of the importance of keeping SAR Portal contact details up to date. The SAR Portal allows users to update personal and organisational contact information via the 'Account Settings' section, in the top right-hand corner of the SAR Portal home page.

SARs Best Practice Videos

The UKFIU has also produced six SARs Best Practice videos aimed at supporting reporters to submit high-quality SARs.

The videos are available on YouTube, and the playlist can be accessed by scanning this QR code:

Or via this link: http://bit.ly/4lBm3tR

Follow the UKFIU on LinkedIn and/or X to stay up to date with new UKFIU guidance products and other important information.

Keep an eye on our social media channels for updates.

Combatting the Live-streamed Sexual Abuse of Children

SARs Enquiry and Action Team,
UK Financial Intelligence Unit (UKFIU)

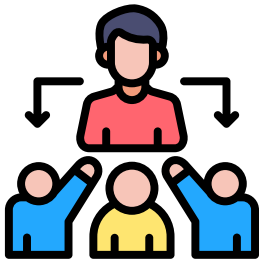
WARNING: This article contains references to child sexual abuse

Live-streaming Sexual Abuse of Children

A recent report published by the Financial Action Task Force (FATF)[1] defines the Live-streamed Sexual Abuse of Children (LSAC)[2] as:

> 'the broadcasting of sexual abuse of children for financial gain. Specifically, the real time transmission or sharing of any material depicting a child in sexual activity, either alone or with other persons, that consumers pay to watch remotely'

It is a cyber-enabled crime that covers a range of offences, including sexual exploitation and human trafficking. The FATF report notes that LSAC (also known as CSA live-streaming) involves individuals in different roles including those of facilitator, abuser and consumer.



Facilitators will arrange the sexual abuse of a child victim, including forcing them to engage in sexual activity in front of a webcam or camera device. The facilitator and abuser, who are often the same person, arrange and conduct the abuse in exchange for a financial payment from the consumer. The consumer is typically in a different location from where the abuse is taking place, and may direct the nature of the offending remotely.

[1] Financial Action Task Force (FATF) is the global Money Laundering and Terrorist Financing watchdog. The inter-government body sets international standards that aim to prevent these illegal activities and the harm they cause to society

[2] Financial Action Taskforce (FATF), Detecting, Disrupting and Investigating Online Child Sexual Exploitation

Scale and Threat

The overall threat from online child sexual abuse (CSA) is increasing in scale, severity and complexity. Advances in technology, such as end-to-end encryption and generative artificial intelligence, provides greater capability and opportunity for offenders as well as increased challenges for law enforcement and governments across the world. Annual detections and reporting of CSA offences are rising, and, according to the Crime Survey for England and Wales,[3] 7.5% of the adult population in England and Wales had been sexually abused before the age of 16.

The live-streaming of CSA in exchange for financial payment is a major threat. The 2024 National Strategic Assessment (NSA) from the National Crime Agency (NCA) estimates that there are between 710,000 and 840,000 UK-based adults who pose varying degrees of risk to children. As well, the UK is one of the highest global consumers of LSAC from the Philippines.

LSAC offenders rely on platforms using end-to-end encryption, which helps them avoid detection, and makes identifying the offending and gathering evidence much harder for law enforcement. The global nature of the crime also means that international cooperation and collaboration is crucial in safeguarding victims and gathering evidence to prosecute offenders.

Detecting Financial Transactions

The FATF provide a number of general indicators of transactions linked to LSAC, which financial institutions should consider. These include:

1. Transactions from developed countries to high-risk jurisdictions for child sexual exploitation.
2. Payments being made to receivers in another jurisdiction, with whom the remitter has no apparent legitimate connection.
3. Transactions made late at night or early in the morning (signalling that the consumer may be in a different time zone).
4. Transaction references may refer to social media profiles, or describe the transaction as being for medical or subsistence costs or refer to relationships between the remitter and receiver.

[3] Office for National Statistics (ONS), Child sexual abuse in England and Wales: year ending March 2019

Particularly relevant to UK financial institutions are the indicators of transactions being conducted by consumers of live-streamed content. These include:

Purchases on dating or adult service sites linked to high-risk countries/webcam/live-streaming, or online gaming platforms, including those providing adult entertainment.

Purchases of video capture software.

Transactions linked to individuals charged with child sexual exploitation-related offences or who are the subject of adverse media involving child sexual exploitation-related offences.

While one of these indicators, and others in the FATF report, may not on their own signify potential cases of CSA live-streaming, combinations of indicators and other relevant factors may point to this type of offending.

Reporting LSAC

There are a number of ways financial and other institutions can report suspected offenders, or victims, of CSA livestreaming (or other suspected sexual abuse or exploitation of children).

- If a child is in immediate danger, call 999. If there is no immediate danger, you can make a report through 101 or anonymously through CrimeStoppers. You can also make a report to the National Society for the Prevention of Cruelty to Children (NSPCC).
- Child Exploitation and Online Protection command (CEOP) within the NCA accepts online reports from both adults and young people who are worried about online sexual abuse or the way someone has been communicating with a child online.
- The National Centre for Missing and Exploited Children (NCMEC) has a Cyber Tipline for reporting child sexual exploitation and can take referrals from individuals and organisations globally.

If you are in the UK regulated sector and you hold money laundering suspicions related to CSA live-streaming, you should consider your obligations to report your suspicions to the UKFIU.

SARs are solely for reporting knowledge or suspicion of money laundering under the Proceeds of Crime Act 2002 (POCA), or belief or suspicion relating to terrorist financing under the Terrorism Act 2000 (TACT). The SAR regime is not a route to report crime, including any predicate offences to the suspected money laundering.

To learn more about the LSAC threat and the system response to it, check out Episode 26 of the UKFIU podcast: "Combatting CSA live-streaming".

In this episode, panellists from the National Crime Agency (NCA) and Natwest Group discuss actions taken by law enforcement and reporters to combat this crime, potential indicators, and how to report if you have suspicions of CSA or money laundering linked to CSA.

Child Sexual Abuse Material in Suspicious Activity Reports

Strategic and Statistical Analysis (SSA),
UK Financial Intelligence Unit (UKFIU)

WARNING: This article contains references to child sexual abuse

The UK Financial Intelligence Unit (UKFIU) performed an analysis of Suspicious Activity Reports (SARs) submitted between July 2019 and March 2025 to review the reporting for elements linked to the monetisation of Child Sexual Abuse Material (CSAM).[1] The analysis concentrated on material which includes imagery and non-live videos, while excluding both the use of sexualised material for extortion and live-streamed sexual abuse of children. The UKFIU utilised a keyword search methodology to identify CSAM-related SARs.

SARs relating to CSAM have increased consistently year on year since financial year (FY) 2020-2021.

5,500

In FY 2024-2025 over 300% more CSAM-related SARs were received than in FY 2020-2021. This amounts to 5,500 CSAM-related SARs reported between July 2019 and March 2025.

Proportionally, this is 0.12% or approximately one in every 800 SARs received.

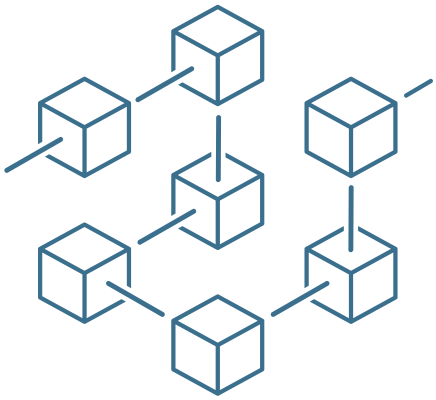
For context, CSAM-related SARs (as defined by our analysis) are highly likely to be the majority (70%) of CSA related SARs submitted to the UKFIU. Using a keyword search methodology, we identified **8,110 SARs related to CSA (in any form) were submitted between July 2019 and March 2025**.

A dip sample of CSAM-related SARs identified that it is likely that only a small minority of CSAM-related SARs contained a suspicion of money laundering (9%) and even fewer reported the production and monetisation of CSAM as the predicate offence crime for money laundering (4%).

Most (85% of) CSAM SARs submitted to the UKFIU do not contain a suspicion of money laundering and are likely to be a report only of the purchase of CSAM. Purchases of CSAM reported in SARs most commonly use virtual assets to send a payment to a virtual asset wallet without a geographical or person attribution known to the reporter.

[1] The definition of CSAM covers any material depicting a child in sexual activity.

Virtual assets are likely to be present in most CSAM SARs (70%) and the crypto-currency most commonly used in these is Bitcoin. The most common red flag for a reporter's suspicion was a transaction that utilised a virtual assets wallet that had previously been flagged as CSAM associated, such as a darknet market. A significant portion of relevant SARs were also submitted due to a reporter's awareness of existing law enforcement interest in the customer.



A significant proportion of CSAM SARs (40%) are only connected to the UK by the use of an account registered with a business who reports SARs in the UK, in these SARs the customer is often based overseas. It is highly likely that this reflects the international customer base of Virtual Asset Service Providers (VASP) who report under the UK regime. SARs with an overseas nexus did not specify if the information had also been reported to international law enforcement in the relevant jurisdiction in which the customer resides.

This analysis has highlighted the need for collaborative work between UK law enforcement and the regulated sector. In particular, work to mitigate the trend identified by this analysis for the inappropriate use of SAR reporting to report crime. Also, by identifying and improving the use of appropriate reporting routes for purchases of CSAM, without the loss of valid intelligence to UK law enforcement. We will seek to do this in partnership with the UKFIU Reporter Engagement Team.

SARs Digital Service update

SARs IT Programme Team,
National Crime Agency

The new SARs Digital Service (SDS) has begun onboarding users from the UKFIU's partner agencies.

In September, an initial test group of accredited users from all our partners were invited to access the service for the first time and provide feedback. Comments from these early adopters have been very positive, with testers reporting that they liked the speed and layout of results when running searches. Users have also been suggesting areas for enhancement and these are being considered by the development team.

Over the coming months, the invitation to access the SDS will be extended to all accredited users, with the aim of having everyone on board by January 2026. Legacy systems for all work on SARs will remain the primary tools for UKFIU and partner users, as more functionality is added to the SDS. Both old and new systems will continue to run in parallel for an extended period.

The SARs IT programme team can be contacted via your dedicated SPOC.

Tackling bribery and corruption across the UK

Domestic Corruption Unit,
City of London Police

The Domestic Corruption Unit (DCU), part of the City of London Police, leads and coordinates the national policing response to domestic bribery and corruption. Acting as the UK's central hub for corruption referrals, the DCU ensures a consistent, intelligence-led approach to identifying, investigating and preventing corruption that undermines public confidence and facilitates wider criminality.

Corruption may occur at lower volumes than fraud, but its impact is disproportionately high, eroding trust in institutions, distorting fair competition and enabling organised crime. The DCU was established to ensure that these high-harm threats receive the prioritisation, expertise and coordination they demand.

The DCU receives and assesses referrals from across UK policing and partner agencies, triaging cases to understand threat levels, inform prioritisation and guide national investment. It focuses on high harm threats, with particular emphasis on national-level corruption and the professional enablers who facilitate it.

Where appropriate, the DCU adopts and leads investigations directly. In other cases, it strategically places investigations with local or regional partners, providing operational guidance, access to covert and proactive capabilities, and additional resource to enhance outcomes. Working closely with the Crown Prosecution Service's specialist team, the unit ensures cases are progressed effectively to achieve maximum criminal justice impact.

Beyond enforcement, the DCU plays a central role in prevention and system-level reform. By analysing intelligence from referrals and investigations, it identifies recurring vulnerabilities and high-risk sectors, using this evidence to drive policy, training and long-term change. The DCU contributes to national consultations and works alongside the Home Office, National Crime Agency, National Economic Crime Centre (within the NCA), and other agencies such as the Serious Fraud Office to shape a more consistent, capability-driven response to corruption.

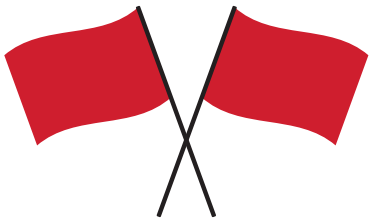
The DCU also supports upskilling across policing and partners, sharing expertise, guidance and learning to improve investigative quality and raise awareness of corruption typologies. Through this collaborative approach, the DCU strengthens the UK's collective ability to deter and disrupt corruption at every level.

Case Study: Operation CHANDRILA

Recent referrals have highlighted local government as a sector vulnerable to corruption risk, particularly within housing services. Operation Chandrila is a live DCU-led investigation into alleged large-scale housing fraud and bribery within a London local authority.

The DCU's involvement has provided strategic investigative support, coordination with regional partners, and intelligence development to identify systemic weaknesses. The learning from this case is now being shared nationally to prevent repeat harm across other authorities.

Red-Flag Indicators



The DCU has identified several recurring red flags and system weaknesses, that are relevant to law enforcement, regulators and the regulated sector:

- Concentration of decision-making power, where one individual controls multiple approval or verification stages.
- Missing, falsified or duplicate documentation in procurement or allocation records.
- Payments routed through personal or unrelated third-party accounts.
- Procurement and local government functions with discretionary control over high-value assets or public funds.
- Referrals or intelligence from whistleblowers, often the earliest indicator of corruption risk.

These patterns mirror many fraud and money laundering typologies, underscoring the need for robust internal controls and cross-sector vigilance.

The DCU plays a vital role in strengthening the UK's system-wide resilience against bribery and corruption. By combining strategic intelligence, specialist capability and cross-sector collaboration, the DCU ensures the national response is coordinated, proactive and informed by real-world threat insight.

Partnership remains key. The DCU encourages continued engagement from the regulated sector financial institutions, professional service providers and local authorities alike, to share intelligence, report suspicions and strengthen governance frameworks.

Together, through collaboration and vigilance, we can better protect public integrity, safeguard national interests and ensure that corruption has no place in the UK's institutions.

Madagascar bribery arrest

International Corruption Unit,
National Crime Agency

A former Chief of Staff to the President of Madagascar was jailed after being found guilty of bribery following an investigation by the National Crime Agency (NCA).

The subject, from Madagascar, and the associate, a French national, were charged by the NCA's International Corruption Unit (ICU) after requesting substantial payment in exchange for their help securing exclusive mining deals with the government of Madagascar.

The pair attempted to solicit a bribe from Gemfields, a UK-based company specialising in the responsible mining of gemstones.

Gemfields reported concerns about corruption to the NCA, who launched an investigation using covert tactics including surveillance and audio recording.

At a meeting in London in June 2023 to discuss the draft "Business Consulting Services" contract written by the associate, the pair requested 250,000 Swiss Francs as payment for organising a meeting with the President of Madagascar and ensuring that the contract was signed. This was in addition to a "success fee" of a 5% equity stake in the collaboration, worth millions, and a further 5,000 Swiss Francs. This was later bumped up to 10,000 by the subject, as a 'goodwill payment' to progress the project.

Following introductions, the subject and the associate discussed a "buffer zone" or "firewall" to distance bribery payments from Gemfields. They clearly understood the request for money and shares to be solicitation of a bribe.

The subject described their role within the Madagascan government and showed no concern around demands being made, stating:

"there is my work in terms of supporting the government and the country in terms of development [...] **But there is also my work of, you know, earning my life**".

During their Evidence-in-Chief at trial, the subject blamed incriminating comments on their struggling with the English language. The subject had studied at universities in both Nottingham and Canada, and spoke and understood an excellent standard of English. They conducted the trial without requiring an interpreter.

Another of the subject's defences was that they remained a passive voice throughout key discussions. In contradiction, they were recorded emphasising their power within government: "I'm very honest, but also very humble, the value of my words is what the boss is listening to." Their "boss" was the President of Madagascar.

In a phone call during July 2023, the subject made a clarification regarding the goodwill payment of 10,000 Swiss Francs: "May I just tell you because I believe there is a misunderstanding but it's important that we keep transparency, and direct conversation between us, because what I read in the contract was 10 for both of us, and what I was saying when I met you was 10 per capita. For [the associate], and myself."

During a final meeting in August 2023, the subject's status was emphasised by the associate who stated the President "won't sign if [the subject] doesn't say sign".

NCA officers arrested the pair that same day.

The associate pleaded guilty in September 2023, the subject was found guilty by a jury at Southwark Crown Court in February 2024. In May 2024, the pair received a combined sentence of five years and nine months years in jail.

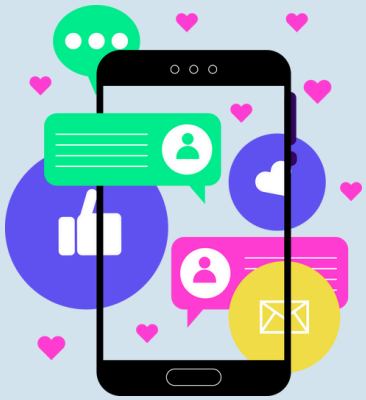
Insights from EMMA 10:
A Europol-led intensification to deliver coordinated action against money muling

National Assessment Centre and National Economic Crime Centre, National Crime Agency

EMMA 10 was a Europol-led intensification which ran from September to November 2024.[1] The main goal was to deliver coordinated action against money muling in all participating European countries at the same time.

The National Crime Agency partnered with law enforcement to operate an intensification which was aligned to the Europol initiative, aimed at disrupting mule activity by targeting the mule facilitators, recruiters and prolific money mules.

Findings from this work have highlighted a continued reliance upon social media by those recruiting money mules and facilitating laundering activity, due to the level of anonymity this provides. Word of mouth and extended interpersonal networks were also found to be used but to a lesser extent.



It is highly likely that young people are particularly vulnerable to online money mule recruitment due to their high use levels of social media platforms and desire to earn easy money.

Most money mules identified were active participants in the laundering activity, however their awareness levels and understanding of the consequences of this differed. For example, some mules expressed concern about trusting others with their account information rather than on the prospect of enabling fraud or money laundering.

Financial gain was identified as the most common incentive for individuals to participate in money mule activity, with coercion and threats of violence reported to a lesser extent.

The growth in the number of financial technology (FinTech) institutions and their popularity amongst young people is also acting as an enabler for money mule networks. Opening such accounts can often be quicker and simpler than with traditional banks. Some FinTechs offer the ability to send funds without knowing someone's full account details and/or offer in-app messaging or broadcast services. Additionally, the speed that payments can be made across the wider faster payment system allows funds to move through a network of mule accounts often before it can be identified and stopped.

Please refer to the National Strategic Assessment 2025 for more details on money mules and the wider illicit finance threat impacting the UK.

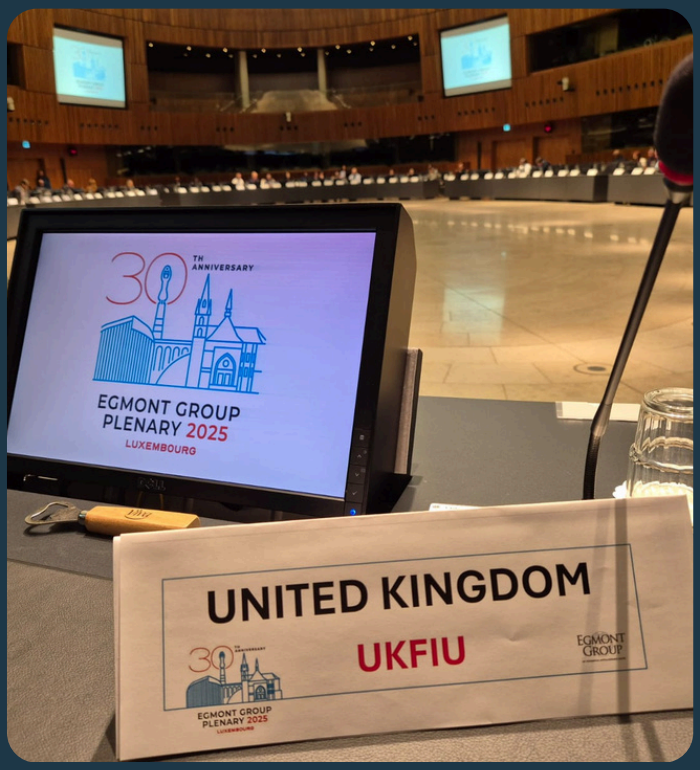
[1] During September to November 2024, 14 Regional Organised Crime Units (ROCUs), two Police Forces, and National Trading Standards took part. This marked the tenth year of the intensification.

The Egmont Group 30 years of partnership

UKFIU International Team
National Crime Agency

The UKFIU was one of the founding members of the Egmont Group, created to foster international co-operation against economic crime. The Egmont Group has grown from modest origins to a membership of over 180 jurisdictional Financial Intelligence Units (FIUs) from across the globe, with a permanent Secretariat to support its work. It is firmly established now as a key part of the global response to money laundering, the financing of terrorism, and as the primary route for data-sharing between FIUs.

The Egmont Group marked its 30th anniversary in July 2025, when representatives from across the world convened in Luxembourg for Plenary Week, the focal point of the year for the organisation.



The UKFIU's delegation joined discussions on issues ranging from alignment between the Egmont Group's procedures and Financial Action Task Force's (FATF) [1] Recommendations to the shape of a comprehensive training programme which will benefit FIUs worldwide. As current Chair of the CARIN [2] initiative, the UKFIU took part in a panel discussion focused on the role of FIUs in tracing and recovering the proceeds of crime and also learned from the experience of others. One of the highlights of the week was a series of presentations from counterparts describing operational successes they had achieved through creative investigative methods and innovative IT packages in their FIUs. Another was the opportunity to hear from experts from the United Nations about the relevance of financial analysis in their response to human trafficking.

[1] The Financial Action Task Force (FATF) is the global money Laundering and terrorist financing watchdog that sets international standards aimed to prevent these illegal activities and hard they cause to societies.

[2] Camden Asset Recovery Inter-agency Network (CARIN) is an informal network of international law enforcement and judicial practitioners working in the field of asset tracing, freezing, seizure and confiscation.

As well as sharing insights, Plenary Week is a moment for making key decisions affecting the Egmont Group. This year's event saw the election of a new Vice-Chair and the appointment of other nominees to the Egmont Committee, the body which guides the Group's direction. By the time the conference closed, amendments had been approved to the processes governing co-operation between FIUs, and agreement reached on the admission of new members. These changes will ensure that FIUs remain robust in their response to financial crime, and collaboration between them keeps pace with the evolving threat.

Above all, the Plenary Week is an opportunity for staff from FIUs to establish and renew contacts, and to discover interests held in common with counterparts. The process was helped this year by a reception and a first-class series of cultural and social events. Like professionals in other fields, financial intelligence officers from different jurisdictions need little prompting before they start to exchange ideas and spot opportunities to work together on something new. The marks of a successful Plenary Week are a clutch of new business cards and a series of fresh projects for the FIUs to pursue as the annual cycle of work resumes.

To reflect the importance of the conference, our hosts arranged for HRH Crown Prince (now Grand Duke) Guillaume, the Ministers of Finance and Justice and the Mayor of Luxembourg to join events and meetings throughout the week. As another indication of the crucial part the event plays in cementing relationships between FIUs, this year's event had the largest number of attendees in the Egmont Group's history. The Egmont Group itself continues to grow, in the ambition and the volume of work it undertakes as well as the size of its membership. Its most recent annual report, covering the full range of activity it takes on, is available to download on the Egmont Group's website here.

The UKFIU is proud to play a full role in the life of the Egmont Group, through the appointment of its Head, Vince O'Brien (right) to serve as Vice-Chair of a Working Group, the secondment of a staff member to the Secretariat and its contribution to research and policy projects.

With thanks paid to our hosts for a highly successful event, the UKFIU is firmly focused on completing the work initiated in Luxembourg. We look forward to reviewing progress and to further productive exchanges over the coming months, and to the 2026 Plenary in Azerbaijan.

The growing threat of Financially Motivated Sexual Extortion

National Economic Crime Centre (NECC)
National Crime Agency

WARNING: This article contains references to child sexual abuse

NECC
NATIONAL ECONOMIC CRIME CENTRE

In June 2025, the Joint Money Laundering Intelligence Taskforce (JMLIT) issued an Amber Alert (0771-NECC) with information and guidance on how to detect Financially Motivated Sexual Extortion (FMSE). The Amber Alert was commissioned by National Economic Crime Centre (NECC) and shared with NECC Public Private Partnership members in response to the emerging threat of FMSE.[1]

FMSE, often referred to as sextortion, is a type of online blackmail where someone is coerced into paying money or meeting another financial demand after an offender has threatened to release intimate, naked or sexual photos, or videos of them. This can be by threatening to share them online, or to third parties such as friends, family or colleagues. When perpetrated against someone under 18 years old, this is a form of child sexual abuse.

Although there has been an increase in FMSE reporting both in the UK and internationally, it is still assessed as an underreported offence. It is dependent on instilled feelings of embarrassment, guilt and shame in victims, which inhibits reporting.

Research highlights that FMSE can have severe psychological consequences. In some cases, it has led to suicide and self-harm.

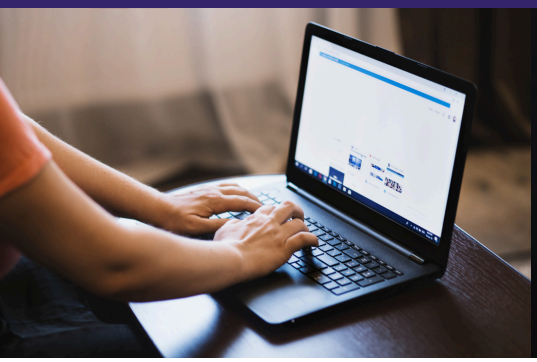
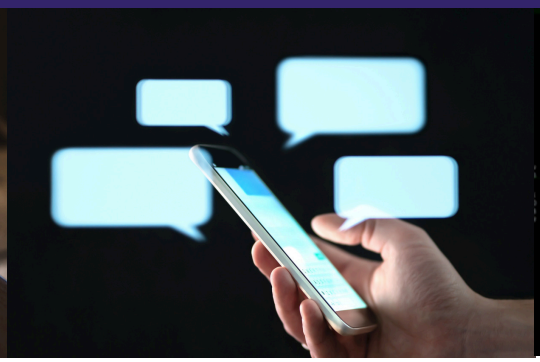
[1] This Amber Alert has been shared with NECC Public Private Partnership members and is not publicly available.

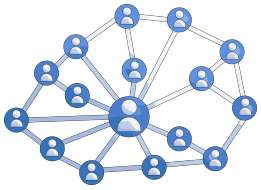
Children, primarily 14-17 year olds, and young adults between 18-30, have reported being forced into paying money or meeting other financial demands, such as purchasing pre-paid gift cards, after an offender has threatened to release sexual or indecent images of them. The increase in reports has primarily stemmed from the following ways:

- Financial blackmail using sexual or indecent images that have been sent by the victim to somebody with whom they have had online contact.
- Financial blackmail using images that have been stolen from the victim, acquired through hacking.
- Financial blackmail through fabricated images using altering technology or artificial intelligence.

FMSE typically takes place over a short period of time. The offence escalates quickly and demands are often made within the first few hours of contact. Despite the speed of FMSE, there tends to be a structure to the offending, with the key elements of the methodology seen in a high proportion of cases. The below steps are typical but not essential;

1. The victim receives a friend request on social media, messaging platform, online gaming, or connects on a dating website.
2. Direct contact is made with the victim, eliciting sexual content. In some cases, contact is moved to a preferred, often end-to-end encrypted platform, such as WhatsApp or Telegram. The offender obtains sexual or indecent images from the victim.
3. The victim is threatened with release of the sexual content to friends/family or social media/online unless financial demands are met.
4. In some cases, the content is publicised by the offender, regardless of whether payment is made. Offenders may make further threats to obtain additional payments.

It is likely that organised offenders engage in the blackmail of both children and adults. Whilst other forms of online blackmail and fraud are often more lucrative, the speed and relative simplicity of FMSE drives offenders to engage in this crime type, which offers typically small gains, but against a larger number of victims.

This type of offending is financially driven and distinct from offending in which indecent images of children or sexualised images of adults are obtained for sexual motivation. An FMSE offender's main motivation is to use the images for blackmail with the intent to make profit. Anyone can be a potential target, however young males aged 14-17 and male adults aged 18-30 are particularly at risk.

The Amber Alert provides potential indicators of FMSE to help financial institutions detect instances and direct them to the correct channels for reporting.

The threat of fraud by Organised Crime Groups against the Student Finance System

JMLIT+ Cell

The Fraud Public Private Threat Group commissioned a time-limited cell to examine the threat of fraud by Organised Crime Groups (OCGs) against the Student Finance System.

The cell first met in June 2023, bringing together partners from across the public sector and UK financial institutions. They offered insight into a rapidly emerging intelligence picture indicating that there are a range of community-based enablers and actors, which are likely operating with a view to facilitating related criminality. Engagement has been strong from all involved, with cross partner analysis, the sharing of bulk data information and potential avenues of investigation; and the sharing of contacts and colleagues, cementing future activity.

The cell has developed an Amber Alert,[1] based on in depth correlation and analysis of student finance and banking data, made achievable by innovative data sharing practices between the public and private sectors, an unprecedented level of trust and collaboration between member organisations. The analysis and finding of the cell are now supporting a wider range of significant government activity already underway to address related threats, whilst the Alert's publication of a range of Red Flag Indicators will be invaluable to banks in their management of customer risk.

If you identify activity which may be indicative of the activity detailed, and there are proceeds of crime, you may wish to make a Suspicious Activity Report (SAR). It will help our analysis if you would include XXJMLXX within the text and the reference 0770-NECC for this alert within the relevant field on the NCA SAR Portal.

[1] The Amber Alert has been shared with relevant stakeholders and is not publicly available.

UKFIU
UK Financial Intelligence Unit

SARs Case Studies

A reporter submitted a DAML SAR after becoming suspicious that the subject, who was in receipt of benefit payments with no record of employment, had received a series of large unexplained payments from external accounts. The UKFIU fast-tracked the DAML SAR to the relevant LEA which commenced a money laundering investigation. **The LEA identified several linked accounts with a very large amount of funds received from overseas.** The LEA obtained an initial Account Freezing Order as a result of the DAML SAR for over £49,000, made multiple arrests and seized a large number of luxury goods and other assets linked to the subject. It is now suspected that the funds are the proceeds of a fraudulent investment scheme targeting victims across multiple countries. Additional DAML SARs from other reporters have led to further AFOs. **The total amount restrained is now over £1.9m (far exceeding the value of the initial DAML SAR).** Enquiries are ongoing.

Multiple DAML SARs led to an LEA launching an investigation into tax fraud and money laundering. A reporter identified multiple linked business accounts in receipt of large credits that were rapidly dispersed to third parties in the UK and to overseas businesses. These transactions did not fit the business profiles of their respective accounts, raising suspicion that the credits were the proceeds of crime. T**he LEA's investigation uncovered evidence that the linked business accounts were involved in tax fraud and the laundering of the proceeds of crime. The LEA obtained AFOs and forfeitures against these linked business accounts, resulting in over £300,000 being forfeited.**

A reporter submitted a DAML due to suspicions that a subject's account was exhibiting money mule activity. There were large credits deposited into the account and limited business activity, upon review the reporter deemed that the activity appeared illegitimate. **Checks were conducted by the LEA and it became clear that the business was part of a large-scale VAT fraud scheme,** the UKFIU provided a refusal decision to allow for further investigation. An AFO was later obtained, and following a detailed investigation, the **LEA successfully obtained a forfeiture order in excess of £450,000,** with funds returned to the public purse.

SIA

SARs IN ACTION

UKFIU
UK Financial Intelligence Unit

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

Episode 26

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 at NCA_UKFIU.