Issue 37

SIA
SARs IN ACTION
MAGAZINE

UKFIU
UK Financial Intelligence Unit

SPOTTING THE ENABLERS
Understand the threat and how to report it

BRIBERY AND CORRUPTION
Strengthening the UK's response

UKFIU IMPERSONATION WARNING
Protect yourself from fraud

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 37 of the UKFIU's magazine, SARs in Action.

This issue brings together a range of threats with insights and practical guidance to support SAR Regime stakeholders in identifying and combatting financial crime. We begin by looking at recent reports of UKFIU impersonations, highlighting what to do if you receive suspicious communciations claiming to be from the UKFIU or NCA. We then explore the growing use of artificial intelligence (AI) to bypass customer due diligence checks.

Taking a look at bribery and corruption in the UK, we examine the current threat landscape and the ongoing efforts to tackle it, a subject featured in the latest episode of the UKFIU podcast. From there, we showcase the work of the NECC Asset Tracing Team which led the UK's contribution to Europol's Project A.S.S.E.T, a cross-border, multi-agency collaboration that has successfully identified a significant number of criminal assets, demonstrating the impact of cross-border cooperation.

We then outline the work undertaken by the UKFIU and Banking SARs Group to review the position of regulated entities when their customers have fallen victim to fraud and publish a guide from the Reporter Engagement Team and NECC Money Laundering Threat Team on professional enablers, who they are, indicators to watch out for and the information that can strengthen SAR submissions.

In addition, HMRC provide insight into the Enterprise Investment Scheme and the key risks SAR reporters should consider when asessing whether supicious activity may be present.

Finally, the Reporter Engagement Team explains what happens after a Defence Against Money Laundering (DAML) request is submitted, offering insight into the process and how these requests are handled.

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.

Impersonation Fraud

UK Financial Intelligence Unit

WARNING: UKFIU impersonations

We have recently been made aware that some members of the public have received letters or emails claiming to be from the UK Financial Intelligence Unit (UKFIU). These communications have asked the recipient to provide personal information in order for a transaction to proceed or to ensure compliance with anti-money laundering regulations.

The UKFIU does not communicate with members of the public in this way, and these communications are fraudulent attempts to obtain personal information.

Communications from the NCA will always come from an email address ending with @nca.gov.uk or @nationalcrimeagency.gov.uk. All communications and acknowledgements from the NCA SAR Portal are sent by the Notifications Service Gov UK. No other email address domains are used for official communications.

NCA GUIDANCE

The following guidance is available on the NCA website and applies to all communications from the NCA, including from the UKFIU:

- In the event an NCA officer needs to speak with you they will identify themselves clearly.
- An NCA officer will only ever contact you for investigative purposes in person, by telephone, or by email - we will never contact you by text message or instant messaging such as WhatsApp.

CONTACT IN PERSON

An NCA officer will identify themselves by showing you their NCA warrant card. This is proof of their identity and authority.

CONTACT VIA EMAIL

Official alerts on issues such as compromised accounts may be sent by email. However official NCA emails will NEVER:

- Ask for remote access to your computer
- Ask you to click on a hyperlink in order to participate in an investigation
- Send you unsolicited emails with attached files, especially zip or macro enabled Microsoft Office files.
- Ask you for any login credentials or passwords.

IDENTIFICATION BY TELEPHONE

If you're contacted by telephone it can be more difficult to verify an NCA officer's identity.

There are a number of things however that an NCA officer would **NEVER DO**

- Ask you for your bank details or pin
- Ask you to transfer funds to another account
- Ask you to hand over cash or bank cards to a courier
- Ask you to pay a fine or a fee to them or a third party over the phone or online
- Ask you to "assist" in an investigation by doing any of the above
- State that you are committing a crime by not complying
- Communicate in an abusive, threatening or coercive manner.

We strongly recommend that after hanging up you wait for five minutes before calling the Police or Report Fraud. There have been cases of fraudsters keeping the line open after a victim had hung up. Leaving several minutes between calls will ensure that the call has closed.

Stay SAFE

Suspect anything or anyone you don't know - no matter what or who they claim to be

Ask questions. Whatever a fraudster tries, you have the power to stay in control

Find out for certain who you are dealing with. Challenge anything that seems suspect

End a situation if you feel uncomfortable. If you feel threatened call your local Police on **101** or **999**.

If you're in any doubt as to the identity of an NCA officer, please complete the Officer Verification form on the NCA website.

If you have any further concerns about a communication you have received from the UKFIU, please contact **UKFIUEngagement@nca.gov.uk**.

Bribery and Corruption in the UK: The Current Landscape and Fight Against It

Scott Griffin, Illicit Finance, National Economic Crime Centre

Bribery and corruption in the UK may not be as visible as in some parts of the world, but they remain persistent threats to public trust, economic fairness, and the integrity of institutions.

While the UK consistently ranks as one of the least corrupt countries globally,[1] recent scandals from procurement controversies to political lobbying concerns have highlighted that no system is immune. As a result, the UK has strengthened its legal framework, enforcement mechanisms, and public sector safeguards to address both traditional and emerging forms of corruption.

At the heart of the UK's anti-corruption regime is the Bribery Act 2010, widely regarded as one of the toughest pieces of anti-bribery legislation in the world. The Act criminalises offering, receiving, or requesting a bribe, and crucially introduces a corporate offence of failing to prevent bribery. This means companies can be held liable even if senior management were unaware of wrongdoing - an approach designed to force organisations to build robust compliance cultures rather than rely on reactive enforcement.

The Serious Fraud Office (SFO), the City of London Police (CoLP) and the NCA play central roles in investigating and prosecuting corruption. The SFO has used tools such as Deferred Prosecution Agreements to hold companies accountable while encouraging cooperation and internal reform. CoLP have created the Domestic Corruption Unit (DCU). The DCU is tasked with identifying, investigating, and disrupting domestic bribery, fraud and corruption. Meanwhile, the NCA's International Corruption Unit (ICU) targets overseas bribery involving UK nationals or companies, recognising that corruption often crosses borders.[2]

---

[1] https://www.transparency.org/en/countries/united-kingdom

[2] To learn more about cases involving the DCU and ICU, click here to read articles from SARs in Action issue 34.

In the public sector, transparency has become a key weapon. The UK maintains open registers of ministerial interests, political donations, and public procurement contracts. Although these systems are not perfect, and critics[3] argue they fail to capture the full scope of potential undue influence, they provide a level of scrutiny that helps deter misconduct. The creation of the Register of Overseas Entities in 2022 also aims to expose the real owners of UK property, reducing opportunities for corrupt individuals to launder illicit wealth through real estate.

Whistleblowing protections have also expanded, though campaigners argue they still fall short. The Public Interest Disclosure Act 1998 offers legal safeguards for individuals who report wrongdoing, and many organisations now operate confidential reporting channels. However, high profile cases have shown that whistleblowers often face retaliation or career damage, prompting calls for an independent 'Office of the Whistleblower' to strengthen oversight.

Political integrity remains a contentious area. Allegations of "cash for access," lobbying scandals, and concerns about the revolving door between government and private industry have fuelled public scepticism. In response, the UK has tightened lobbying rules, strengthened the Ministerial Code, and increased oversight by bodies such as the Advisory Committee on Business Appointments (ACOBA). Looking ahead, the UK faces new challenges: digital fraud, opaque financial networks, and the use of cryptocurrencies for illicit payments. The government's Economic Crime Plan 2 (2023–2026) sets out a coordinated strategy to tackle these threats, including enhanced data sharing, tougher corporate liability rules, and increased investment in enforcement agencies.

While corruption in the UK may be less overt than in some countries, it is far from absent. The combination of strong legislation, growing transparency, and evolving enforcement tools shows that the UK is taking the issue seriously, but continued vigilance, political will, and cultural change remain essential to maintaining public trust.

The UK's ongoing work and collaboration against this threat has been discussed in the recently released UKFIU podcast – Episode 29: Inside the Fight Against Bribery and Corruption – Special Edition. Listen to learn about the fight against bribery and corruption, with the NCA and partners exploring in detail their remits and contributions to this critical work.

[3] https://www.transparency.org.uk/news/promise-vs-practice-why-britains-new-ministerial-gift-register-misses-mark

The Use of AI to Bypass Customer Due Diligence Checks

NECC Illicit Finance - Crypto-assets and Tech Enablers Team

Amber Alert

In April 2026, the Joint Money Laundering Intelligence Taskforce (JMLIT) published a second edition Amber Alert[1] (0801-NECC) covering the use of Artificial Intellience (AI) to bypass customer due diligence (CDD) checks.[2]

This Alert was a follow up to the first edition, published in October 2024 (0752-NECC)[3], and is based on the findings of a public-private partnership cell, which sought appropriate data from members to answer key questions on this threat.

The Alert used data from members to estimate the overall scale of the threat on the UK financial sector, and confirmed the threat as a current one not a theoretical one.

AI has been used to manipulate identity documents and create deepfakes, allowing criminals to impersonate real individuals or create synthetic personas, masking the criminal's identity and providing evolving challenges to CDD processes. Accounts, created using AI manipulated images or video, have facilitated different frauds and laundered proceeds from drug trafficking and other crimes.

If you or your institution identifies activity which may be linked to the detail in this report, and there is a suspicion of money laundering or terrorist financing, you may wish to make a Suspicious Activity Report (SAR). If you decide to make a report in this way, you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference 0801-NECC for this Alert within the relevant field on the NCA SAR Portal.

---

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

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

[3] This Alert has been shared with the JMLIT+ membership and is not publicly available.

NECC Asset Tracing Team lead UK response to Europol Project A.S.S.E.T

National Economic Crime Centre

Europol, in collaboration with law enforcement from 31 countries and leading private sector partners, has concluded its third and most successful operational week of Project A.S.S.E.T. (Asset Search and Seize Enforcement Taskforce). This initiative has become a crucial component in the global fight against serious and organised crime and the seizure of criminal assets.

From 19 to 22 May 2026, Europol's headquarters in The Hague hosted over 40 law enforcement agencies, including Asset Recovery Offices (AROs), Financial Intelligence Units (FIUs), and specialised units focusing on money laundering and organised crime. The operation was supported by Eurojust, INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC), and key private sector partners from the financial services and cryptocurrency industries.

The European Public Prosecutor's Office (EPPO) and AMLA (Anti-Money Laundering Authority) also participated in the event. UK representatives from the NECC and HMRC were present at Europol HQ during the course of the sprint to build relationships, and manage/co-ordinate engagement and intelligence exchange with overseas partners.

The UK response, led by specialists in the NECC Asset Tracing Team, brought together a multi-agency response with significant input from the NCA (including the UKFIU), HMRC, Companies House, Financial Conduct Authority (FCA), Land Registry and members of the financial services sector through the Joint Money Laundering Intelligence Taskforce (JMLIT).

Over a two-week period, over 36,000 asset tracing checks were completed, delivering a high quality, collaborative capability at pace. UK assets and leads identified on behalf of overseas partners include properties, bank accounts, companies, card details, addresses and tax details with an estimated value of £5 million.

Jess Sommerlad, Head of NECC Illicit Finance said:

> "The NECC continues to fully support Project A.S.S.E.T. by leading and co-ordinating the UK's multi-agency response. Tracing and recovering criminal assets to disrupt serious organised crime is of vital importance and this initiative has again shown the significant benefit of joint-working with partners both domestically and internationally."

The operational week yielded significant results, demonstrating the impact of cross-border cooperation and innovative investigative asset tracing techniques. Combining the efforts and expertise of both law enforcement and private sector partners, it led to the identification and tracing of a significant number of criminal assets:

- **884 Bank Accounts**
- **80 Companies**
- **55 Crypto Wallets**
- **74 Vehicles & 1 Vessel**
- **44 Items of real estate**
- **2 Suspected criminals were located and one arrested**

The exact value of identified assets will be determined through follow up investigations and analysis of findings by partners, but can already be estimated in the millions.

Jürgen Ebner, Acting Executive Director of Europol said:

> "Project A.S.S.E.T. has become an important operational platform in the fight against organised crime and criminal finances. During my visit to the taskforce at Europol Headquarters, I witnessed first-hand the extraordinary commitment and professionalism of investigators and partners working side by side across borders. Their efforts demonstrate how international cooperation and financial intelligence can strike directly at the financial foundations of organised crime."

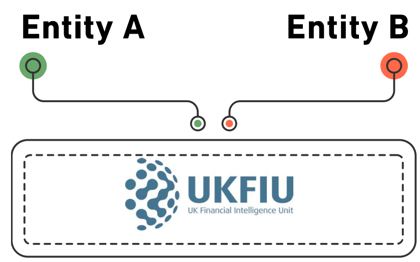
UKFIU Guidance Note: Fraud Victims and SARs

UKFIU Reporter Engagement Team

The UKFIU has been working with the NECC, FCA, and members of the Banking SARs Working Group on a range of initiatives designed to improve efficiency of the SARs regime and support Systems Prioritisation objectives. One of these recent initiatives was a review of the position relating to the submission of a SAR where a regulated entity's customer has been the victim of fraud.

Currently, when a customer becomes a victim of fraud, the victim's financial institution (Entity A) notifies the perpetrator's financial institution (Entity B) of the fraudulent transaction. In many cases, both financial institutions then submit separate SARs to the UKFIU about the same incident.

Following detailed analysis, it has been agreed that **the perpetrator's financial institution (Entity B) is better placed to submit a more informed and useful SAR to the UKFIU**, as they hold key information about the account receiving the funds.



The Proposal

If the victim's financial institution (Entity A) has notified the perpetrator's financial institution (Entity B) about the fraudulent transaction, then Entity A may – based on its own risk appetite – choose not to submit a SAR in relation to the fraud victim. The perpetrator's financial institution (Entity B) would then provide the primary SAR, containing fuller and more actionable intelligence.

This approach helps both financial institutions and the UKFIU focus their time and resources on high-risk, high-value intelligence, rather than producing duplicative reports with limited system benefit. A similar approach has already helped improve efficiency through the recent raising of the DAML threshold.

Regulatory and Governance Support

The NCA and FCA have reviewed this proposal and confirmed that they support this approach.

The System Prioritisation Governance Group (SPGG) – co-chaired by the NCA and FCA and attended by Home Office and HM Treasury – has also formally ratified this position.

Next Steps for Regulated Entities

It is now for individual entities to consider the proposal and decide, in line with their own risk appetite and reporting obligations, whether to implement any operational changes to reduce duplicative fraud victim SARs.

Professional Enablers

UKFIU Reporter Engagement Team and
NECC Money Laundering Threat Leadership

Professional enablers pose a significant risk to the integrity of the UK's legitimate economy and reputation as a global centre for finance and investment. The NCA's National Assessment Centre (NAC) and partners have produced numerous assessments highlighting the role of professional enablers at the heart of serious and organised crime impacting the UK. Their specialist skills, knowledge and expertise are exploited by criminals to launder the proceeds of crime. Professional enablers can also be used to facilitate all other forms of crime including corruption, modern slavery & human trafficking, organised immigration crime, drugs trafficking and child exploitation.

Without professional enablers, criminal and corrupt actors would not be able to launder their criminal proceeds or progress other criminal activities to the scale and complexity that they currently do.

Definition

The government's definition for a professional enabler was published in the UK's Economic Crime Plan 2 following significant consultation across the public and private sectors. This definition guides the UK response to professional enablers.

A Professional Enabler is an individual or organisation that is providing professional services that enables criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations.

The definition covers a spectrum of intent from those who are complicit in facilitating criminal needs, to those who are negligent or reckless in facilitating crime or otherwise failing to comply with regulatory obligations, as well as those who are turning a blind eye to the possibility they are facilitating criminal activity.

'Professional service' includes but is not limited to:

- Legal professions
- Accountants and bookkeepers
- Bank officials (including relationship managers)
- Investment advisors and wealth managers
- Payment service providers
- Estate agents and letting agents
- Trust and company service providers
- Family offices
- Art and auction houses
- Company services including nominee directors/shareholders

This list is not exhaustive but the term professional enabler does not include other types of enablers of crime, such as technological enablers (e.g. cryptocurrency) or logistical enablers (e.g. haulage companies).

How should the definition be interpreted?

A professional service provider can fall within the definition of a professional enabler if they provide services that facilitates criminal activity and they were intent or negligent in doing so. The sliding scale of intent from complicity to negligence illustrates the professional enablers observed across a number of law enforcement and regulatory operations:

Any individual or firm falling within the definition of a professional enabler is vulnerable to both criminal prosecution and regulatory/supervisory enforcement action which will significantly hinder, and in some cases stop their ability to operate in the UK. It is vital that all professional service providers have an in-depth understanding of who their customers are, and for what purpose their services are being used, and the associated risks. They must take steps to prevent their services from being exploited by criminal and corrupt actors. A lack of knowledge around the exact criminal activity the professional enabler is facilitating does not mean a professional service provider falls outside of the definition.

In contrast, the definition for a professional enabler does not include legitimate professional service providers who take a thorough risk-based approach, implement robust controls and procedures to detect and deter criminal activity, and do not accept business having identified that their services could be exploited to facilitate criminal activity.

Response

The threat from professional enablers is complex and driving serious and organised crime in the UK and overseas. Professional enablers play a critical role in the efforts of organised crime groups (OCGs) and corrupt elites to conceal the origin and destination of the proceeds of crime, and they often play a direct role in the criminal activity impacting our local communities.

The NCA has made firm commitments to tackle professional enablers of serious and organised crime and will be using its unique capabilities to tackle the highest harm enablers and disrupt their activity. This is underpinned by work being conducted by the National Economic Crime Centre (NECC) and the wider system. The NECC and partners established the UK's Cross-System Strategy[1] to Tackle Professional Enablers, which ran from 2024 until April 2026. This strategy galvanised the system response to the threat by bringing together UK government, regulators, the private sector and international partners to implement the strategy, focusing on:

1. Enhancing threat understanding
2. Improve information and intelligence sharing
3. Coordinating the system response
4. Protecting financial and professional services
5. Delivering disruptive action against professional enablers
6. Driving an international response

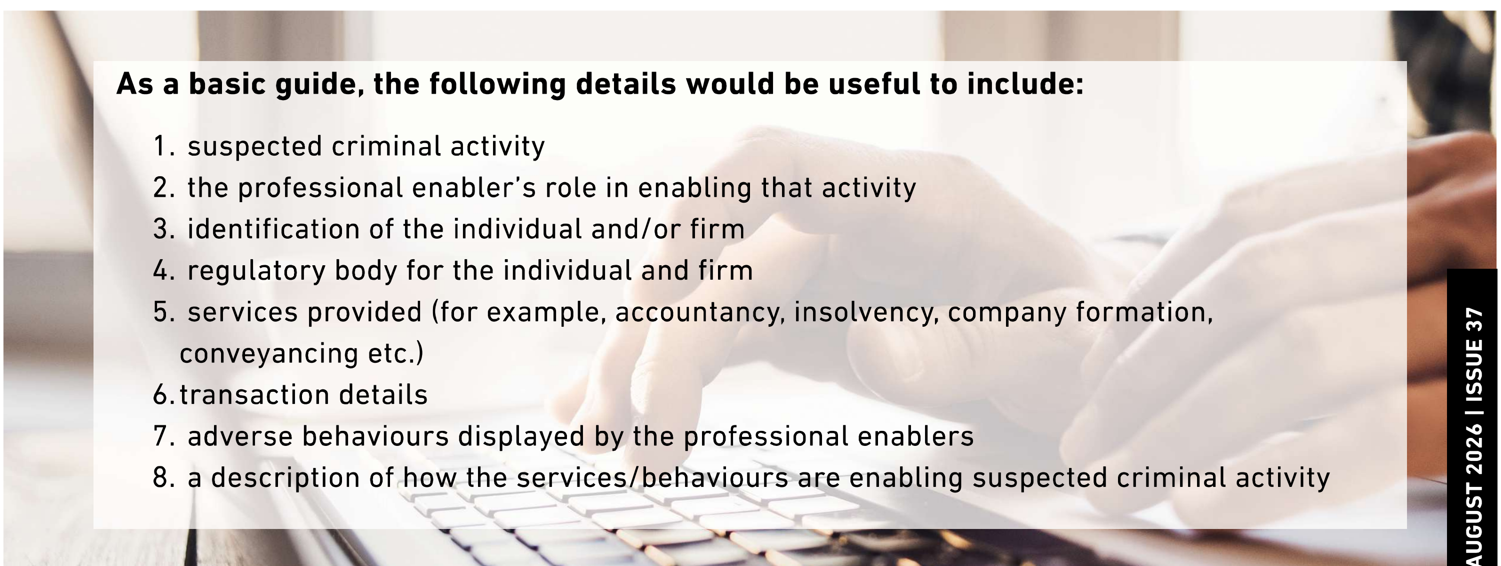
The strategy established the building blocks for a more robust response to those who seek to abuse their position as a professional or financial service provider to facilitate criminal activities. The NECC and partners will continue to drive this response over the coming years, building on the success of the strategy and developing an extended action plan to take this work forward.

What can SAR Reporters do?

SARs are a vital intelligence source which provide tactical leads to improve threat understanding and inform the law enforcement response.

The use of the glossary code **XXPRFXX** enables law enforcement to identify SARs related to professional enablers for further development and investigation, as well as informing the UK's understanding of the threat.

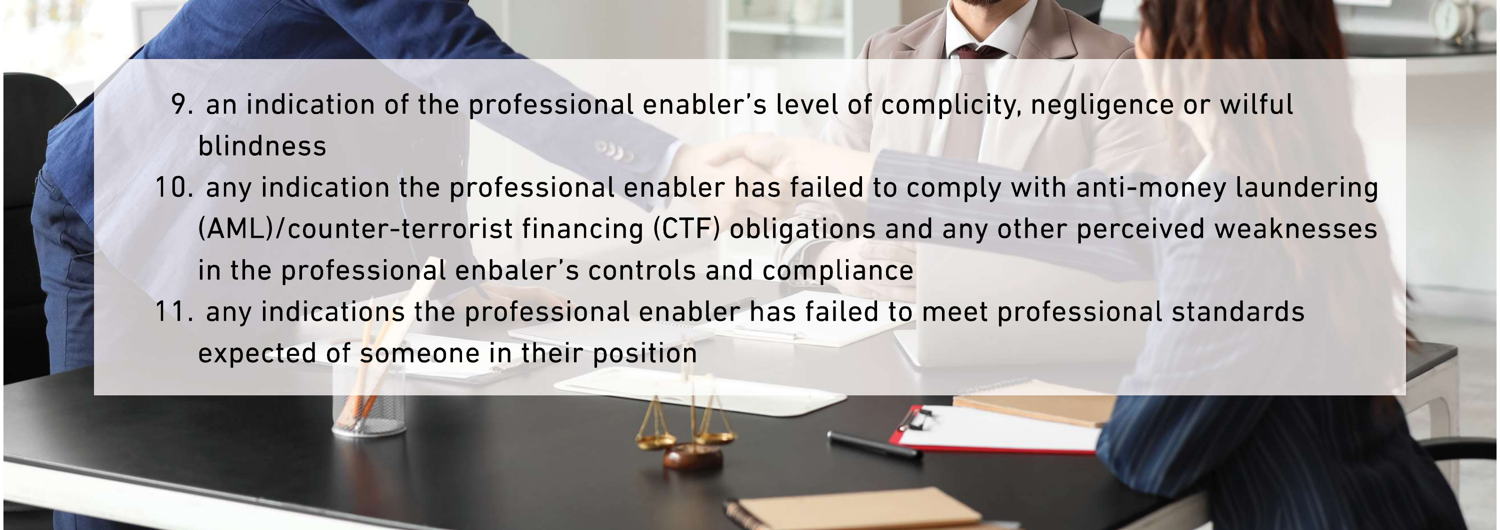
If you believe criminal activity is being facilitated by a professional enabler (whether through complicity, negligence or turning a blind eye), this should be referenced within SARs.



As a basic guide, the following details would be useful to include:

1. suspected criminal activity
2. the professional enabler's role in enabling that activity
3. identification of the individual and/or firm
4. regulatory body for the individual and firm
5. services provided (for example, accountancy, insolvency, company formation, conveyancing etc.)
6. transaction details
7. adverse behaviours displayed by the professional enablers
8. a description of how the services/behaviours are enabling suspected criminal activity

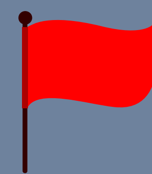
[1] This is covered in SARs in Action Issue 27 Special Edition - Professional Enablers



9. an indication of the professional enabler's level of complicity, negligence or wilful blindness
10. any indication the professional enabler has failed to comply with anti-money laundering (AML)/counter-terrorist financing (CTF) obligations and any other perceived weaknesses in the professional enbaler's controls and compliance
11. any indications the professional enabler has failed to meet professional standards expected of someone in their position

Indicators of professional enabler activity can include:

- provision of services to individuals or companies related to adverse media reporting or displaying red flags of money laundering
- activities/services aimed at obscuring the identification of the underlying client
- failures in identifying or responding to red flags of money laundering or other criminal activity
- failures to apply proper scrutiny to customer due diligence, source of funds and source of wealth information/documentation
- misuse of personal, corporate or client accounts, for example to move suspected proceeds of crime
- evasive or obstructive responses to reasonable enquiries made by a bank to support customer due diligence
- client or transactional links to high risk entities or jurisdictions
- incorporating and/or managing corporate entities and structures believed to be obscuring beneficial ownership
- acting as a nominee for an unreasonable number of companies/trusts
- creating false or misleading accounts or other documentation
- providing documentation that contradicts transactional activity or statements made by the professional
- prolific incorporation of companies where the company formation agent does not appear to have conducted proper customer due diligence
- incorporation of shelf companies
- setting up complex corporate structures and/or servicing transactions that do not have a sound economic or business rationale
- clients and/or transactional activity falling outside of expectations at client onboarding
- significant funds received and/or expenditure on luxury items identified in personal bank accounts



The NECC and UKFIU has been working with SAR reporters to enhance the quality of intelligence reported in SARs and exploit this vital intelligence source as part of the system response to the threat. The UKFIU strives to assist in disrupting those responsible for enabling and laundering the proceeds of crime belonging to people committing a range of offences. The UKFIU has engaged directly with relevant sectors to further highlight the importance of the SARs received concerning professional enablers and, importantly, why it is crucial to ensure that the correct glossary codes and relevant details are included. Partnership working with all of our stakeholders remains as important as ever as we continue to enhance the response to this threat"

Emma-Jayne Turner, Engagement Manager, UKFIU

What can law enforcement do?

Professional enablers play a pivotal role in the criminal activities of criminals and corrupt actors operating in the UK and overseas. The NCA will tackle those enabling the activities of the highest harm OCGs but local policing must also take a robust approach to the professional enablers operating in their area.

As a part of the NECC's coordination of the system response, it is driving the Pursue response across the NCA, policing and wider law enforcement. The NECC would like to know about the professional enablers operating across the UK particularly where driving the serious and organised crime threat.

There are a range of disruption opportunities available to law enforcement as well as regulators which can bolster the UK's response. The NECC can offer advice and a crucial link into the regulatory bodies to further operational activity targeted against professional enablers.

Please contact the NECC Money Laundering Threat Leadership team on:

NECC.MLB&C@nca.gov.uk

Enterprise Investment Scheme Fraud

HMRC Venture Capital Reliefs Team

The Enterprise Investment Scheme (EIS) promotes UK economic growth by encouraging private investment in high-risk, early-stage companies through tax reliefs (30% income tax relief as an example), with HMRC responsible for administering and ensuring compliance.

HM Revenue & Customs

While most activity is genuine, some arrangements may involve misuse resembling tax evasion, money laundering, or investment fraud.

For financial institutions (FIs) and reporting entities, understanding how EIS operates—and how it can be exploited is essential, with key risk indicators helping support effective, consistent reporting.

Understanding EIS Investment Flows

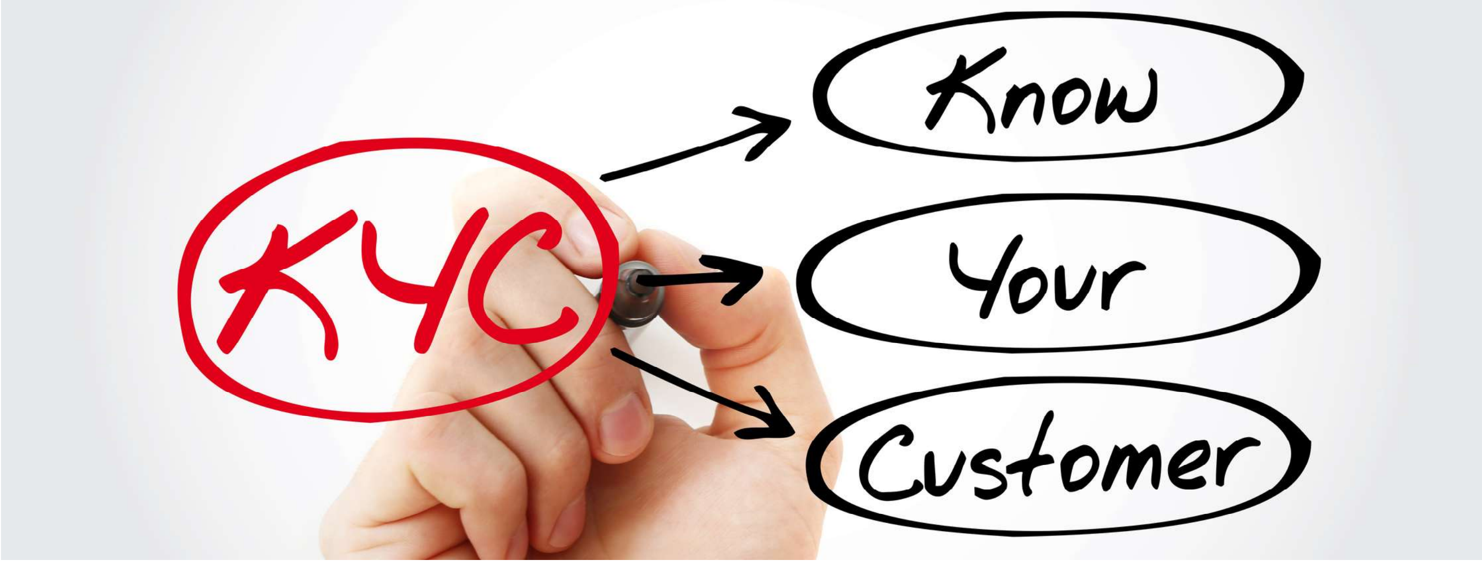
Many EIS investments are straightforward, but some involve intermediaries (e.g. fund managers, promoters or special purpose vehicles), which can obscure activity without being inherently suspicious.

FIs can identify potential EIS activity through indicators such as payment references (e.g. "EIS", "SEIS" (Seed Enterprise Investment Scheme), links to known EIS funds or nominees, or customer behaviour consistent with tax-efficient investing, helping guide further analysis.

Knowing Your Customer

In some instances identified by HMRC, fraudsters have targeted individuals who are not sophisticated or high-net-worth investors, promoting EIS as a way to extract funds. These schemes often emphasise income tax relief and claim to be "HMRC approved" to appear legitimate.

FIs may also encounter individuals or companies acting as "introducers" who collect investor funds to pass to EIS/SEIS firms or receive large commissions from them.



FIs should conduct enhanced checks where customers make large transfers to early-stage or low-activity companies, especially if they appear vulnerable, act beyond their means, or invest significant savings.

If you believe you have been the victim of fraud, please report it to Report Fraud.

The Importance of Suspicious Activity Reports (SARs)

SARs are key to protecting EIS integrity, safeguarding investors, and tackling financial crime. HMRC reviews all SARs flagging EIS risks, and FIs should consider EIS in cases of suspected investment fraud. When unsure, referencing EIS in a SAR allows HMRC to quickly assess whether action is needed.

Summary

EIS is a key tool for supporting UK innovation and growth, but its complexity and generous reliefs can make it susceptible to misuse. Financial institutions play a vital role by recognising risk indicators and submitting clear, well-evidenced SARs to help protect both the financial system and the integrity of the scheme.

This article was produced by the Tax Crime and Evasion Public Private Threat Group, a part of the Joint Money Laundering Intelligence Taskforce (JMLIT+) model.

jmlit
Joint Money Laundering Intelligence Taskforce
Tackling financial crime together

EIS Misuse Indicators

EIS risks fall into two areas: those relating to the investor and those linked to the EIS company. Financial institutions may have visibility over one or both sides of the transaction.

Risks Associated with the EIS Company

A SAR decision should focus on business legitimacy.

Indicators of EIS misuse when reviewing an EIS company include:

- no clear or credible investment rationale
- limited evidence of genuine operations despite significant funding
- high spending inconsistent with stated purpose, especially on consultancy or marketing
- high commissions (over 20%) paid to third parties for fundraising
- funds routed through multiple intermediaries (layering)
- artificial or circular transactions to generate losses or recycle funds
- funds transferred (directly or indirectly) to connected parties soon after investment
- complex or opaque ownership structures
- involvement of overseas entities, particularly in low-transparency jurisdictions

Risks Associated with the EIS Investors

Investors must hold their investment for three years to retain EIS benefits, so any returns within this period - unless due to a company sale - are unusual.

Indicators of EIS misuse from an individual perspective include:

- inconsistent behaviour, especially where vulnerable individuals invest significant savings or act beyond their means
- large investments by individuals who are not sophisticated investors
- limited or inconsistent information on the source of funds
- vague or contradictory explanations (e.g. unclear if for genuine investment or tax avoidance/money laundering)
- unusual pre-investment receipts, particularly from higher-risk jurisdictions or showing signs of financial crime
- circular arrangements where investors receive funds back from the company or linked parties

Ask the UKFIU: What Happens After a Defence Request Has Been Submitted?

UKFIU Reporter Engagement Team

Dear UKFIU,

I've submitted a defence request and I'm not quite sure what happens next. Does the notice period start straight away? Can we continue working the case in the meantime? And what exactly is the UKFIU doing with the request while it's under review?

Once a request for a defence against money laundering (DAML)[1] or a defence against terrorist financing (DATF)[2] is submitted, it enters what is known as the statutory 'notice period'.

The notice period begins on the first working day after the SAR is submitted and lasts for seven full working days, as set out in the relevant legislation. During this period, the future specified activity (prohibited act) must not be carried out, as doing so may risk committing an offence.

That said, the notice period does not prevent you from taking other action on the case. You may still continue with actions such as reviewing the file, conducting searches, or writing correspondence etc, but please be mindful of 'tipping off' offences when completing such tasks.

During the notice period, the UKFIU will assess the information provided in the defence request and consult with partners where necessary. Each case is triaged for factors such as:

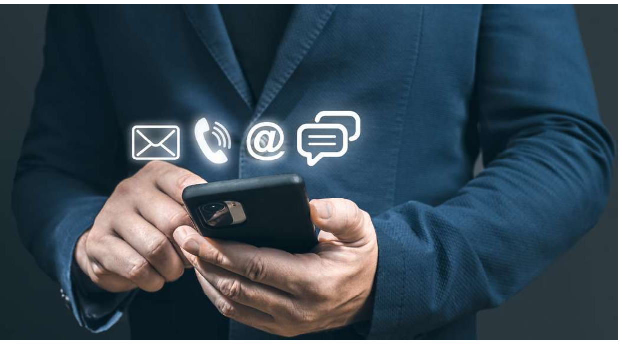
- priority
- risk
- existing law enforcement interest
- asset recovery opportunities

[1] DAMLs are defence requests submitted under the Proceeds of Crime Act 2002 (POCA).

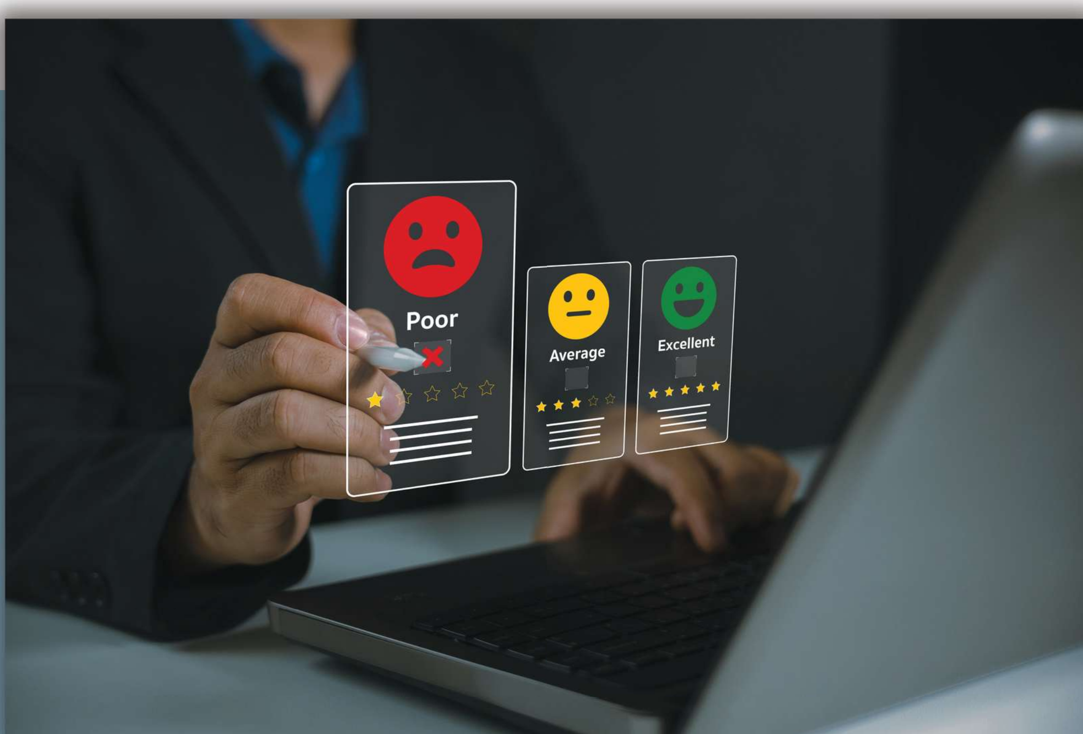
[2] DATFs are defence requests submitted under the Terrorism Act 2000 (TACT).

This helps determine how the case will be progressed. The UKFIU will also consider proportionality and necessity when deciding the appropriate response.

In some cases, the UKFIU may contact you within the notice period to request further information or clarification. Equally, a request may be closed if it does not meet the requirements of POCA or TACT.



Where further information is requested, it is important that reporters respond in writing and within the timeframe given. If no response is received, or the response provided does not contain enough detail to allow an informed decision to be made, the case may be closed.



Where your case is closed and you still require a defence, you will need to resubmit your request, ensuring you include the information that was missing from the initial request, for it to be considered again. The statutory notice period for a decision will restart when the new request is submitted.

It is also worth bearing in mind that poor quality SARs may be referred to the relevant anti-money laundering supervisor for their attention and any appropriate action.

SIA

SARs IN ACTION

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

Episode 29

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.