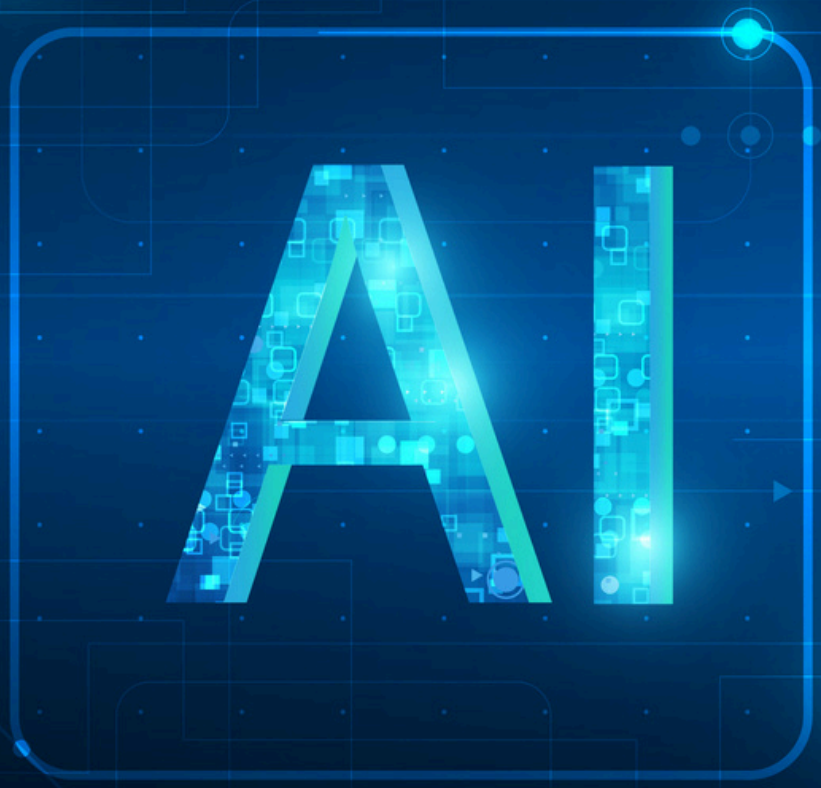
Issue 26

SIA
SARs IN ACTION MAGAZINE

UKFIU
UK Financial Intelligence Unit



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 the 26th issue of the UKFIU's magazine *SARs in Action.*

This issue features multiple articles from the UKFIU and our partners at the NCA's National Assessment Centre (NAC).

The first article highlights how Artificial Intelligence (AI) is playing an increasing role in the fraud crime threat. In this article, the NAC distinguishes the different ways criminals use this technology to prey on potential victims.

This issue also contains updates from the UKFIU, including the latest episode of the UKFIU podcast, which focuses on the legal sector, including discussions on key money laundering threats and risk areas for the sector. Another article discusses the latest glossary codes available on the SAR Portal, which reporters may wish to consider using in future SAR submissions. These glossary codes focus on the threat from terrorism. This article also includes an extensive list of all current glossary codes, a useful point of reference for all in the illicit finance field.

This is followed by an informative piece for financial institutions on crypto asset risk indicators; originating from their engagement with international partners in the Joint Chiefs of Global Tax Enforcement initiative (J5). Another UKFIU article provides a detailed examination on the necessity for reporters to maintain compliance in their SAR submissions, particularly within the DAML and DATF SAR processes. This issue then finishes with an update on advancements made by SARs digital transformation.

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.

Produced by UKFIU

THE THREAT FROM GENERATIVE ARTIFICIAL INTELLIGENCE ENABLED FRAUD

National Assessment Centre (NAC)
National Crime Agency (NCA)

Generative artificial intelligence (GenAI) is highly likely the most significant threat to the fraud landscape from artificial intelligence (AI) technology, according to a report issued by the NCA.

Coming in the forms of large language models (LLMs), voice cloning, and deepfakes, the proliferation of GenAI has widened the accessibility of sophisticated tools that can be easily obtained and misused by fraud offenders.

GenAI is highly likely to enhance the threat from investment fraud, romance fraud, impersonation enabled fraud and phishing attacks. As all cyber enabled frauds involve the use of text, images, audio or video, GenAI is more likely to augment existing high harm frauds than create entirely new ones.

Although AI is not a new phenomenon, national attention has grown over the past few years as platforms such as ChatGPT became almost overnight sensations and rocketed into public attention. GenAI content is challenging to distinguish from human-produced material, which means that fraud victims are unlikely to be aware of when it has been used. This in turn is likely to lead to underreporting.

The scale of GenAI enabled fraud directed against the banking sector is unknown, although it is highly likely identity fraud is a significant vulnerability.

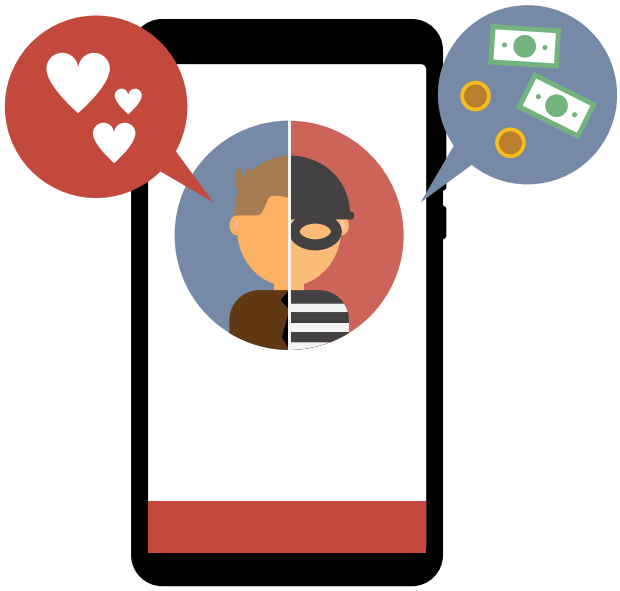
The use of GenAI to enhance offender access to fraudulently obtained bank accounts is also likely to be a vulnerability.

LLMs are of particular use to an offender with minimal experience in defrauding victims, being capable of providing detailed information on how to execute a fraud whilst evading detection. LLMs have the potential to upskill an offender in areas like anonymization technology, enabling them to plan how to more effectively obfuscate their online activity. LLMs also limit the time required to research niche topics, quickly generating background context on unfamiliar locations, events or financial processes that would be useful when planning an investment or romance fraud.

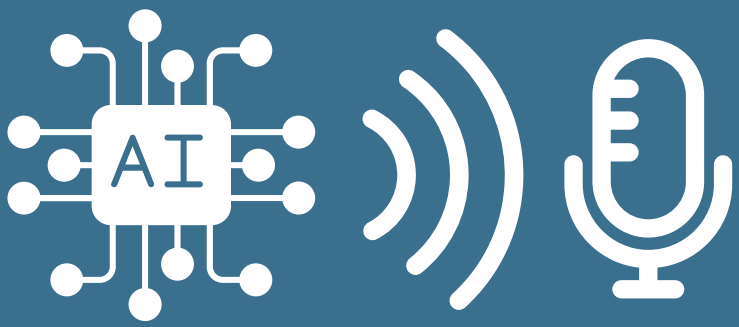
Although LLMs like ChatGPT are generally programmed to reject prompts that can be used by fraud offenders to engage new victims, there are methods used to circumvent these safeguards. Users can rephrase the prompt in specific ways so that the LLM will provide responses that would otherwise trigger its moderation features.

Since 2022, LLMs with few or no moderation features have emerged, often targeted at fraud offenders and cyber criminals. FraudGPT is an LLM sold on a subscription basis, mainly developed to generate malware and phishing emails. However, the authenticity and effectiveness of these services remains unknown.

Deepfake imagery and videos have reportedly been used in romance frauds to deceive the victim into believing the persona they are communicating with is real, improving the chances of forming a genuine emotional connection. 'Face swapping' tools are already being advertised on criminal forums which enable offenders to video call victims using a synthetic appearance. According to one open source report in 2023, a UK based victim lost around £350,000 after believing they were in a two year relationship with the offender who had used deepfake technology during video calls.



Voice cloning can be used in impersonation enabled frauds to deceive the victim that they are speaking with a colleague, friend or family member. Whereas previously such frauds relied mostly on text, the capability to clone the voice of specific targets opens the potential for targeted, high harm attack methods against individual victims as well as businesses.



Testing by industry bodies indicates that some tools can replicate a person's voice with up to 95% accuracy. This highlights its potential use to control money mule accounts which use voice as a form of identity authentication.

Offenders are likely to combine different GenAI tools to enhance the overall legitimacy of the fraud. Deepfake images alongside LLMs are highly likely to become more frequently used in investment fraud to generate bank statements, official documentation or positive reviews to enhance the credibility of a scheme. It is highly likely these methods undermine the capability for potential victims to conduct due diligence on these investment options. Additionally, voice cloning and LLMs are highly likely to be used in payment diversion fraud to generate fake invoices and impersonate key figures in businesses to enhance the legitimacy of the request.

Although it is highly likely that the most significant threat to fraud will be from GenAI methods, broader AI technology – while entailing a number of challenges - has a wide range of applications that present opportunities to organisations involved in detecting and combatting fraud.

Key terms

Term	Definition
Artificial intelligence (AI)	Machine-driven capability to achieve a goal by performing cognitive tasks.
Generative artificial intelligence (GenAI)	AI systems that can create new content. The most popular models, such as ChatGPT, generate text and images from text prompts, but some use other inputs such as images to create audio, video, and images.
Large language model (LLM)	Models trained on large volumes of text-based data, typically from the internet.
Voice cloning	The use of AI technology to create a simulation of a person's voice.
Deepfake	Videos or images that use a form of AI to digitally manipulate existing content, for example by replacing images of faces with someone else's likeness.

UKFIU PODCAST - EPISODE 19: LEGAL SECTOR: CHALLENGES AND OPPORTUNITIES

Digital Media Publications (DMP) Team
UK Financial Intelligence Unit

In January the UKFIU's Digital Media and Publications (DMP) Team had the pleasure of attending the Solicitors Regulation Authority (SRA) offices in Birmingham to record their latest podcast episode. Hosted by UKFIU Reporter Engagement Team (RET) Manager Emma-Jayne Turner, the episode focuses on the legal sector, highlighting key considerations and challenges facing legal professionals when it comes to anti-money laundering (AML) and suspicious activity reporting. Insights were provided by a panel of experts who attended in person and virtually.

Guests included Sara Gwilliam, Money Laundering Reporting Officer (MLRO) at SRA; Colette Best, Director of AML at SRA; Graham MacKenzie, Head of AML at the Law Society of Scotland; Rick Kent, Economic Crime and AML Policy Lead at the Law Society of England and Wales and; Dr Joanne Cracknell, Director of legal services at Willis Towers Watson (WTW).

The legal sector covers everything from large global firms down to sole practitioners, and the guests discussed the key money laundering threats, risk areas, and red flags firms and practitioners should be looking out for.

The number of SAR submissions is low compared to other sectors, accounting for 0.32% of all submissions. What is more significant is the quality of the SARs and the importance of using correct glossary codes and good quality, accurate information. Good quality SARs play a vital role in combatting serious organised crime, and can provide law enforcement with vital intelligence to assist in investigations.

Law firms and practitioners face significant challenges concerning AML compliance and SARs. Key themes from firms facing AML compliance investigations and enforcement action are - inadequate importance of robust controls, procedures and risk assessments, inadequate supervision and training, systems and processes which allow checks to be conducted.

To listen to this and other challenges between legal privilege and the SARs regime, follow the link to the podcast episode. https://spoti.fi/3xRfMHC

NEW TERRORIST FINANCING GLOSSARY CODES - COMING SOON

Reporter Engagement Team (RET)
UK Financial Intelligence Unit

The UKFIU will be adding four new terrorist financing glossary codes to the SAR Portal soon.

The UKFIU recently published an updated list of glossary codes with the April 2024 Reporter Booklet. This updated list announced these four new Terrorist Financing glossary codes, and provided guidance on how to include these codes in relevant SARs prior to them being added to the SAR Portal.

The UKFIU has identified an error in one of the codes published, and the updated codes have now been removed from the April 2024 Reporter Booklet to avoid confusion.

The new Terrorist Financing codes will be available for use on the SAR Portal shortly, and reporters will be notified via the UKFIU's social media channels when these go live. **Reporters using the SAR Portal should not manually type the new glossary codes into their SARs.** Please wait until the codes have been embedded into the glossary code section of the SAR Portal for selection.

The glossary codes currently active on the SAR Portal are set out in the following table. Further guidance on when to apply each code to your SAR is also available on the SAR Portal.

SAR Glossary Codes (as of July 2024)

Vulnerable people	
XXV2XX	Risk to vulnerable adults
XXV3XX	Risk to children
XXOICXX	Organised immigration crime
XXMSHTXX	Modern slavery and human trafficking
XXVICTXX	Returning money to a victim of crime
High risk individuals	
XXD9XX	Bribery and corruption
XXPRFXX	Professional enablers

High risk predicate offences	
XXDRUXX	Illegal supply of drugs
XXFIREXX	Firearms
Money laundering typology	
XXTBMLXX	Trade-based money laundering
XXPROPXX	Purchase and rental of real estate property
XXMLTMXX	Money laundering through markets
XXILTXX	Illegal lotteries
XXVAXX	Virtual assets
Economic predicate offences	
XXTEOSXX	Tax evasion offshore
XXTEUKXX	Tax evasion UK-based
XXF1XX	Proceeds from benefit fraud
XXF2XX	Excise evasion (duty on alcohol, tobacco, fuel etc.)
XXF3XX	Corporate tax evasion (tax evasion by businesses, corporations)
XXF4XX	Personal tax evasion (tax evasion by individuals e.g. income tax)
XXF5XX	VAT fraud
XXF9XX	Frauds against the private sector
National interests	
XXSNEXX	Money laundering linked to sanctioned entities
XXPCPXX	Illegal proliferation of chemical, biological, radiological or nuclear weapons, associated technology or their means of delivery
XXCVDXX	Suspicious activity connected to COVID-19
XXSATXX	Suspected fraudulent use of the HMRC Self-Assessment Tax Refunds system

CASE STUDIES

A Law Enforcement Agency (LEA) launched an operation that utilised SARs intelligence to launch multiple investigations in to **trade based money laundering, VAT re-payment fraud, and investment fraud**. These SARs contained valuable information submitted by multiple reporters for a number of concerns including; high value transfers, credits not reflecting business profiles, links with fraudulent businesses, and adverse media on the subjects.

The LEA was able to identify links with potentials leads, increasing the intelligence the LEA had to pursue a number of subjects and identify Organised Crime Groups (OCGs). These SARs were invaluable as subject criminality was linked to Electronic Money Institution (EMI) accounts, which was not identifiable through other searches.

As a result of the LEA's operation and intelligence from these SARs, **funds in excess of £750,000 were forfeited,** uncontested, denying OCGs the benefits of their criminality.

A reporter had concerns regarding the source of funds in a subject's account. It was believed these funds were the proceeds of crime due to **the subject previously committing fraud**. In order to exit the relationship with the subject, the reporter submitted a DAML SAR to pay away the funds to the subject.

The UKFIU highlighted this intelligence to the relevant LEA. During the LEA's investigation, a victim was identified as the source of the funds. Through LEA, reporter and UKFIU coordination, the reporter was able to **return over £23,000 to the victim**, rather than the subject.

A reporter submitted a SAR after becoming concerned that an elderly subject was a victim of fraud after they could not make contact with the subject following **rapid cash withdrawals and card purchases which did not match their expected spending profile**.

The UKFIU fast-tracked the SAR to an LEA who conducted a safeguarding visit to the subject and found that the subject's family members had fraudulently accessed the subject's account, withdrawing in excess of £80,000.

The LEA provided safeguarding intervention and the subject's family members were arrested. **The subject's funds were recovered in full** by through reporter processes and the LEA's investigation into fraud by abuse of position is ongoing.

A reporter was concerned that a customer (the subject) was using their accounts to launder money. The UKFIU fast-tracked the SAR to an LEA, who had an ongoing money laundering investigation open into the subject and their high-end accessories business.

Further enquiries into the subject's financial accounts revealed **links to drug dealing and drug supply.** The subject refused to be interviewed and disclaimed more than £25,000 found in their accounts. One associate of the subject, who had been arrested in possession of drugs in a previous incident, was financially linked through another SAR. The SAR detailed the associate had been sending regular payments to the subject's business account which further heightened suspicion.

Over £15,000 was forfeited after the associate also disclaimed the funds in the account and refused to offer any explanation for the payments into the subject's account.

JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT INITIATIVE - CRYPTO ASSET RISK INDICATORS FOR FINANCIAL INSTITUTIONS

International
UK Financial Intelligence Unit (UKFIU)

The UKFIU in partnership with HMRC work collectively with international colleagues within the Joint Chiefs of Global Tax Enforcement initiative known as the J5.

The J5, a collaborative partnership among tax authorities and law enforcement comprised of five countries; Australia, Canada, Netherlands, UK and US, has identified several risk indicators that financial institutions should be aware of.

Risk indicators play a pivotal role in enhancing the ability of financial institutions to detect and report money laundering and illicit activities involving crypto assets. To counteract these risks, timely identification allows financial institutions to intervene and to report to the relevant authorities contributing to the overall integrity of the financial system and ensure compliance with anti-money laundering (AML) regulations.

Detecting signs of money laundering and tax evasion requires the gathering, analysis and reporting of financial data. By disseminating the risk indicators to the financial institutions, valuable insights from law enforcement can be relayed to the financial sector and reporting agencies. The J5 Advisory "Crypto Asset Risk Indicators for Financial Institutions" is intended to enhance the abilities of reporting entities to detect and report suspicious activity necessary to disrupt illicit financial flows. While risk indicators may vary and not all are covered, the details in this advisory note are commonly observed.

This advisory is provided for your information only and to assist in the identification and management of risk arising from crypto assets.

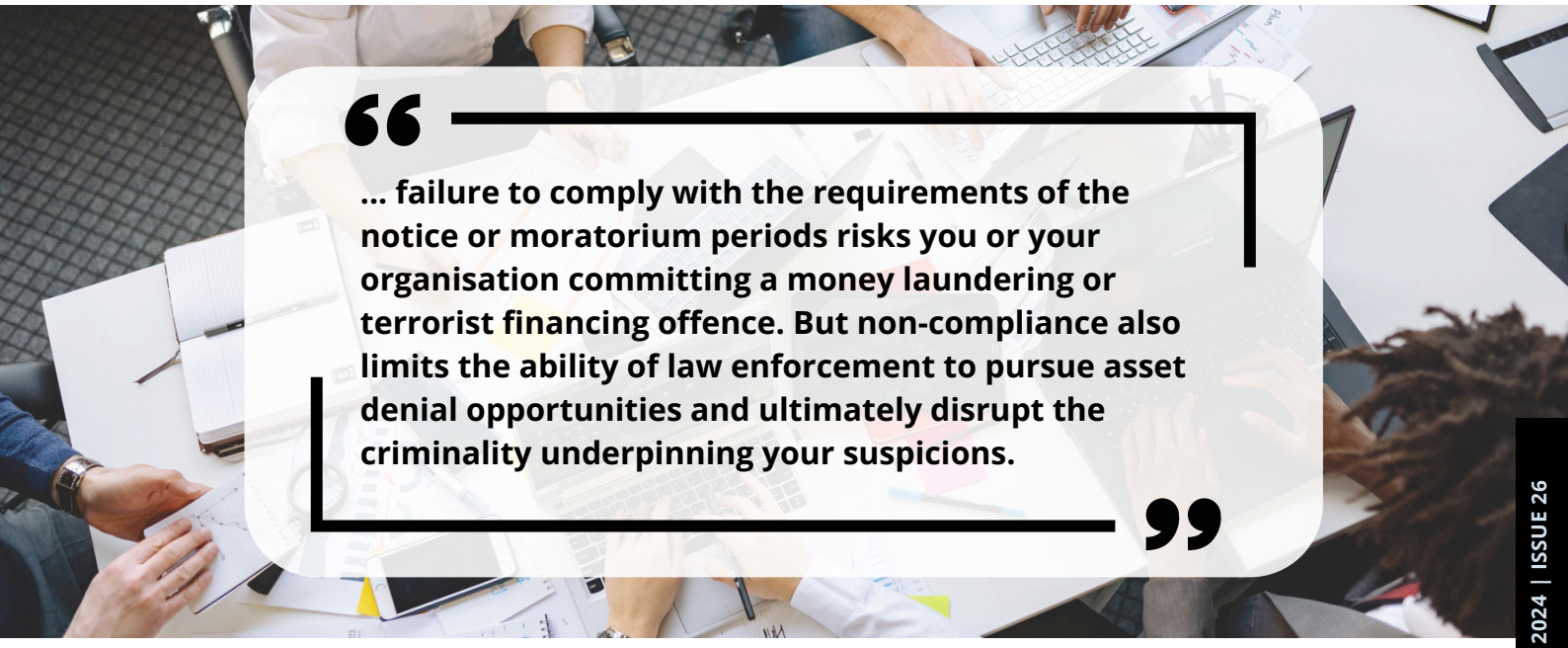
For further details please see the J5 Advisory "Crypto Asset Risk Indicators for Financial Institutions" located via https://bit.ly/4dUPe8B.

ARE YOU AT RISK OF COMMITTING A MONEY LAUNDERING OR TERRORIST FINANCING OFFENCE?

Emma-Jayne Turner
Reporter Engagement Team (RET)
UK Financial Intelligence Unit

A thorough understanding of how the POCA and TACT notice periods work is vital for all reporters to ensure they do not commit a money laundering or terrorist financing offence by proceeding with a prohibited act before a defence is granted.

One of the core functions of the UKFIU is to consider requests for a defence against money laundering (**DAML**) or a defence against terrorist financing (**DATF**), also known as 'consent', 'appropriate consent' or 'prior consent'. In the 2022/2023 financial year, the UKFIU received over 74,000 DAML requests and over 300 DATF requests.[1] The principal money laundering offences are set out in Part 7 of the Proceeds of Crime Act 2002 (**POCA**), and the Terrorism Act 2000 (**TACT**) established several terrorist financing offences. Both pieces of legislation recognise that there may be circumstances where individuals and organisations need to carry out an activity in the course of their business that could result in them committing a principal money laundering or terrorist financing offence, because they know, believe or suspect that the property involved is, or may be, criminal or terrorist property. In these circumstances, reporters can request a defence from the NCA in relation to the intended activity.[2]



> **... failure to comply with the requirements of the notice or moratorium periods risks you or your organisation committing a money laundering or terrorist financing offence. But non-compliance also limits the ability of law enforcement to pursue asset denial opportunities and ultimately disrupt the criminality underpinning your suspicions.**

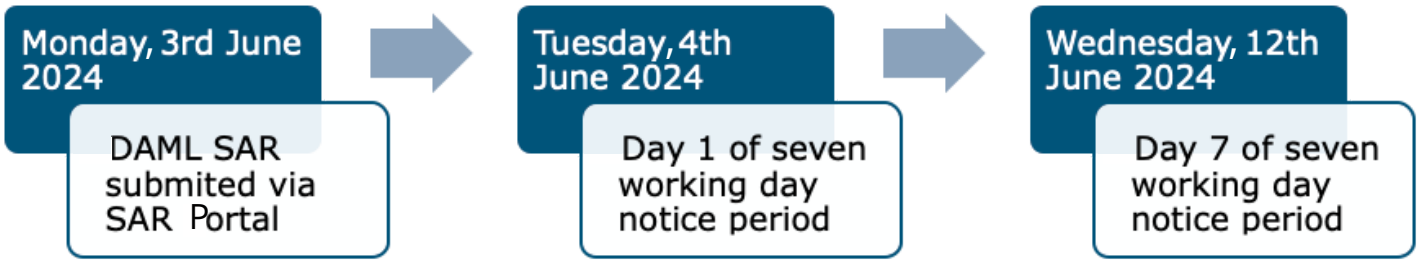
[1] SARs Annual Statistical Report 2023.

[2] POCA includes some exemptions to the requirement to seek a defence against money laundering from the NCA. Reporters should consult their AML supervisor or seek legal advice for more guidance on this.

The 7-working day notice period for DAMLs and DATFs

A key element of both the DAML and DATF request processes is the 7 working day notice period (the **notice period**).[3] This period starts from the first working day after the day the SAR is submitted, and continues for seven full working days, as defined in the relevant legislation.

For example:



During the notice period, the UKFIU will assess the information provided in your defence request and consult with partners as necessary. The UKFIU may contact you for further information or clarification of your request within the notice period; or we may close your request if it does not meet the requirements of an Authorised Disclosure under s338 of POCA.

The UKFIU will consider proportionality and necessity when determining the appropriate response. In applying these tests of proportionality and necessity to DAML requests, the UKFIU will consider the likelihood of law enforcement being able to take positive action against the criminal property (for example, an account freezing order) during the 31-day moratorium period that follows a refusal decision (see below).

You will hear from us during the notice period if:

- we decide to **refuse** your request for a defence; **or**
- we decide to **expressly grant** your request.

In other DAML cases, you may not get any response from the NCA before the end of the notice period.

If your DAML or DATF request is refused, then you do not have a defence to the money laundering or terrorist financing offence you are proposing to undertake and risk committing an offence if you proceed with the activity.

You **do have a defence** to the money laundering or terrorist financing offence you are proposing to undertake if:

- you receive a **granted letter** from the NCA in response to your request; or
- the **notice period expires without any response** from the NCA.

[3] POCA ss335(5), 335(6), 336(7), and 336(9); TACT ss21ZA(3) and 21ZA(4).

The 31-calendar day moratorium period for DAMLs

If your DAML request is refused, the day you receive the refusal marks the start of a 31-calendar day moratorium period (the **moratorium period**). During this moratorium period, law enforcement will work to take positive action against the criminal property. This moratorium period can be extended beyond the initial 31-days by the court.[4]

Throughout the notice period, and any subsequent moratorium period, the UKFIU will routinely engage with law enforcement to ensure any refusal continues to be proportionate and necessary.

As with the initial 7-working day notice period, until you receive a granted letter or until the expiry of the moratorium period, whichever is earlier, you do not have a defence to the money laundering offence you are proposing to undertake and risk committing an offence if you proceed with the activity. If you receive notice that an application has been made to the court to extend the moratorium period, the moratorium period will continue beyond the expiry of the original moratorium period even if the application to extend is not heard by the court until after the expiry date.[5]

There is no moratorium period for refused DATFs, and you do not have a defence unless and until the request is granted by the NCA. DATF decisions are kept under review following refusal.

Why is compliance with the notice and moratorium periods, and refusal decisions, so important?

The obvious answer is that any failure to comply with the requirements of the notice or moratorium periods risks you or your organisation committing a money laundering or terrorist financing offence. But non-compliance also limits the ability of law enforcement to pursue asset denial opportunities and ultimately disrupt the criminality underpinning your suspicions. Ensuring your organisation complies with the requirements of the notice and moratorium periods every time means you are playing a key role in protecting the public against serious and organised crime and terrorism.

[4] POCA s336A.

[5] POCA s336C.

Avoiding the common mistakes that can lead to committing an offence

Reporters must have robust systems and controls in place to ensure the prohibited act is not undertaken either during the notice period or following a refusal. Nominated Officers and MLROs are reminded of their obligations under POCA and TACT to ensure a prohibited act is not undertaken without appropriate or prior consent.

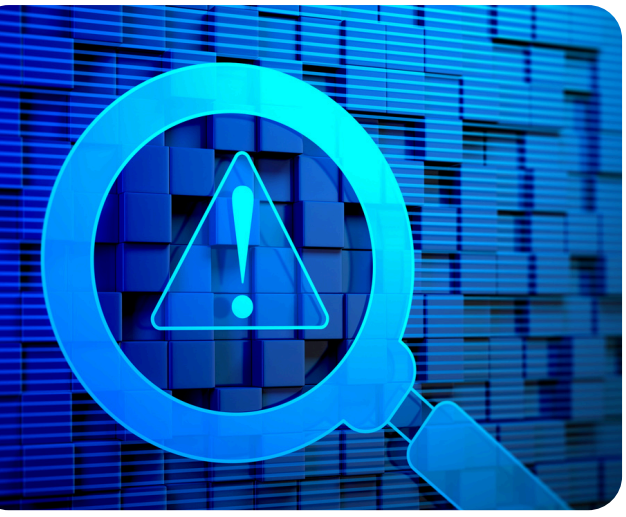
Common failures and mistakes to avoid are:

Not keeping your SAR Portal main contact details up to date

The UKFIU will use the main contact details registered on the SAR Portal to notify reporters of DAML and DATF decisions. It is imperative that all reporters review these details frequently to ensure they are up to date, and this includes both the email address and the contact telephone number.

We recommend reporters use a shared mailbox for the main contact email address, so requests for information and refusals are not missed if an individual member of staff is on leave. If the main contact details used are those of an individual member of staff, reporters must ensure appropriate processes are in place for their emails and voicemail messages to be accessed by other appropriate staff members during any period of absence or leave.

Please note, while the SAR Portal allows organisations to include two alternative contacts, these should not be relied upon for receiving refusals and other requests from the UKFIU.



Human error or systems failure

Reporters must also ensure they have robust processes and training in place for all relevant staff to ensure account restrictions or other mechanisms designed to prevent breaches cannot be overridden or circumvented without proper oversight. Similarly, where automated systems are used to restrict accounts, these should be frequently tested and reviewed to ensure continued compliance.

What to do if you identify a breach

All identified breaches of notice and moratorium periods should be notified to the UKFIU as soon as possible, and we expect reporters to proactively notify their regulator and/or AML supervisor. The UKFIU will also refer notified breaches to the relevant regulator or AML supervisor, and law enforcement may pursue prosecution of those responsible for any resulting money laundering or terrorist financing offence.

The NCA has detailed guidance for reporters on requesting a defence from the NCA under POCA and TACT, which can be accessed from the NCA website.

If you have any questions or need further guidance, please contact the UKFIU Reporter Engagement Team on UKFIUEngagement@nca.gov.uk.

Most POCA SAR submissions are made available to SARs accredited officers within Law Enforcement Agencies (LEAs) within 10 days of submission and any information you provide could be used to support investigations. The NCA UKFIU may also proactively share both the content of SARs and your SAR Portal registration details (including name, phone number and email address) with LEAs where there is a legitimate purpose to do so, such as the detection and prevention of crime. LEAs include police forces and other accredited SAR end users with enforcement capabilities (such as local authorities and other government agencies). LEAs may contact you via your registration details for additional information to support investigations.

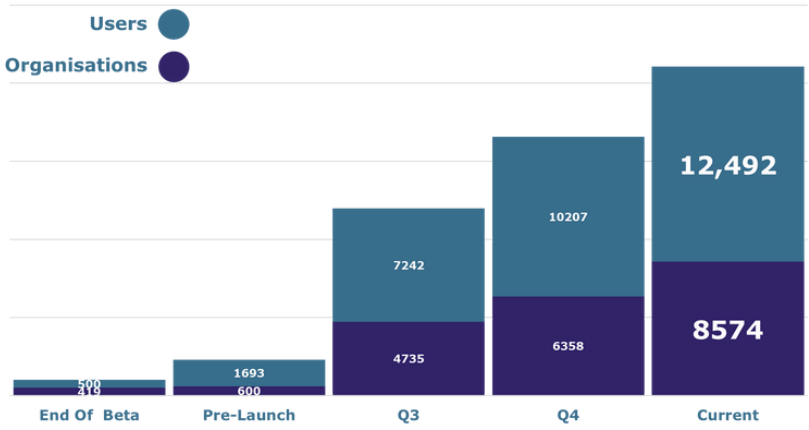
LANDMARK POINT FOR SARs DIGITAL TRANSFORMATION PROGRAMME

SARs Digital Transformation Programme (formerly SARs Reform Programme) National Crime Agency (NCA)

SARs Digital Transformation Programme (the Program) is celebrating a key milestone.

All SARs from regulated sectors are now being submitted through the newly developed SAR Portal or Bulk API platforms. These channels (which have been designed to provide a more structured way of submitting SARs) will enhance the ability of investigators to quickly identify and act on key information.

With the onboarding phase of the Programme complete, legacy online and bulk CSV have been closed off and are no longer available for use.



Since April 2023, when the reporters first began submitting through the new routes, the SAR Portal has grown to have over **12,000** registered users across **8,500** organisations.
The last remaining bulk reporter was recently onboarded and, to date, there have been **200,000** submissions made using this route. Bulk reporters include some of the country's largest financial institutions, and they accounted for 73% of all SARs made in 2023.

> This is a significant milestone for the programme and represent the end of 18-months' work by the SARs Digital Transformation Programme.
>
> Information submitted through the new structure gives us improved means of analysing and exploiting data. It will bring long-term benefits for reporters, government and law enforcement agencies – so we can better protect the public from serious, organised crime.
>
> The completion of this crucial phase allows us to move into the next stage of the programme.
>
> **Programme Director, Martin Sidaway**

The work of the Programme is now focussed on developing the SARs Digital Service (SDS), which will employ latest technology to aid officers in developing and utilising the data, to help protect the public.

The team has also ended its monthly newsletter drop to reporters, closing on a thank you to all who have helped make the migration to the new platforms a success.

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 19

AVAILABLE HERE

THE UKFIU PODCAST

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

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

Updates can also be found on our LinkedIn page and on X (formerly Twitter) at NCA_UKFIU.