NCA
National Crime Agency

UKFIU
UK Financial Intelligence Unit

SARs Reporter Booklet

October 2026

This is a United Kingdom Financial Intelligence Unit (UKFIU) product for reporters of Suspicious Activity Reports (SARs), produced in line with the National Crime Agency's commitment to share perspectives on the SARs regime.








SARs Reporter Booklet Overview

This document is produced by the UKFIU which has national responsibility for receiving, analysing and disseminating financial intelligence submitted through the SARs regime.

This booklet contains a sanitised summary of feedback from law enforcement agencies (LEAs) on their use of SARs.

This booklet is aimed at:

- sharing perspectives on the use of SARs with regime participants
- sharing and encouraging best practice amongst reporters
- providing a feedback mechanism to the UKFIU about the operation of the regime.

More information about the UKFIU, the SARs regime and further guidance notes can be found at the NCA website www.nationalcrimeagency.gov.uk.



Don't forget to also follow us on LinkedIn and X (NCA_UKFIU).

SCAN ME

We would appreciate your feedback on the effectiveness and format of this document. Please email any comments to UKFIU.DigitalMediaPublications@nationalcrimeagency.gov.uk.

Disclaimer

Cases reported on in this document were collated in response to biannual requests from the UKFIU to LEAs to report on the use of SARs intelligence during the course of their investigations. This Reporter Booklet contains examples received in April 2026.

While every effort is made to ensure the accuracy of any information or other material contained in this document, it is provided on the basis that the NCA and its officers, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or other material contained herein.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.

Foreword from **Vince O'Brien**

Welcome to the October 2026 edition of the UKFIU's Reporter Booklet aimed at all SAR reporters.

With this publication we aim to provide a snapshot of some of the excellent examples we receive highlighting the work of law enforcement agencies in utilising SAR intelligence to initiate investigations and informing existing ones.

SARs are a critical intelligence resource for law enforcement – they provide information like phone numbers, addresses, company details, investment activity, bank accounts and details of other assets. They have been instrumental in identifying sex offenders, fraud victims, murder suspects, missing persons, people traffickers, fugitives and terrorist financing.

These Reporter Booklets focus predominantly on sanitised case studies. News relating to the UKFIU/SARs regime features instead in the UKFIU magazine, SARs In Action, available via the NCA website.

Don't forget to also subscribe to the UKFIU podcast – this is available on a number of streaming sites including Spotify, Apple Podcasts, Amazon Music and Audible. In September 2026, a two part series on Op MACHINIZE 2 was released, **Episode 30: Op MACHINIZE 2 part 1 - Building the intelligence picture** and **Episode 31: Op MACHINIZE 2 part 2 - From intelligence to enforcement**.





Vince O'Brien
Head of the UKFIU

UKFIU Assistance

For information or assistance with submitting SARs or SAR Portal enquiries, please visit www.nationalcrimeagency.gov.uk or email UKFIUsars@nca.gov.uk.

When contacting the UKFIU please have available your SAR reference number if applicable. If you wish to make a SAR by post you should address your SAR to: UKFIU, PO Box 8000, London, SE11 5EN. NB: post is slower than SAR Portal and therefore it will take longer for your SAR to be processed. You will not receive an acknowledgement if you use post.

General UKFIU matters may be emailed to UKFIUsars@nca.gov.uk. All Defence Against Money Laundering (DAML) request queries are only dealt with via email. Should you have any queries please email DAML@nca.gov.uk.

Case Studies

A review of case studies provided by LEAs and other end users[1] of SARs demonstrates how they continue to be instrumental in instigating and supporting investigations to tackle a wide range of the highest priority threats identified by the National Strategic Assessment of Serious and Organised Crime (NSA).

Money Laundering

A suspect's business account remained dormant for an extended period, before receiving a large number of high value payments over a short timeframe. The reporter conducted an internal investigation, which revealed that the business had registered with multiple contradictory Standard Industrial Classification (SIC) codes and had no clear rationale to account for receipt of the payments. The reporter held suspicion that the business account was being used for money laundering and decided to close the business account and exit their relationship with the suspect. The reporter submitted a DAML SAR to seek a defence to pay away the business account balance. The UKFIU refused the DAML request and shared intelligence with the relevant law enforcement agency (LEA). Following their investigation, the LEA successfully obtained an account freezing order (AFO) for over £65,000 on the business account which was subsequently forfeited. The DAML SAR stopped further money laundering activity and led to a large benefit of crime being denied to criminals.



A subject was remanded in custody after pleading guilty to drug supply and money laundering offences. Following this, a reporter identified recent activity in an account held by the subject, even though they were in prison. The reporter was unable to establish who was using the subject's account. Due to this suspicious activity, the reporter decided to end their relationship with the subject and sought a DAML to pay away the balance held on the subject's account. The UKFIU refused the DAML SAR and shared the intelligence with the LEA, who had arrested the subject. The LEA used the DAML SAR to support their restraint order application, resulting in over £28,000 being frozen. The resulting DAML provided crucial time for the judicial process to take place, preventing the funds held in the subject's account being dispersed. The subject is undergoing confiscation proceedings, where the frozen funds will be considered as available assets.

[1] A current or potential user of SARs such as an LEA or relevant government body.

Concerns of money laundering were raised by a reporter after identifying suspicious activity on a customer's business account (account). A review of the account revealed a high volume of suspicious payments from a wellness brand business, totalling over £200,000 within a short period of time. Account information held by the reporter was inconsistent, and payments did not match the expected business profile of the industry, raising suspicion that the account was being used to launder the proceeds derived from fraud. The reporter closed the account and submitted a DAML SAR to pay away the account balance. The DAML SAR was refused and fast-tracked to the relevant LEA. The LEA's investigation linked the funds to the supply of unlicensed supplements. Following the LEA's enquiries, an additional DAML SAR was identified for a different account held by the same customer. This DAML SAR was also refused, resulting in two AFOs, which totalled more than £60,000. The timely DAML SAR allowed the LEA to freeze a significant amount of the proceeds of crime, while also identifying and freezing other money laundering routes used by the business, with the intent to pursue forfeiture of the funds.



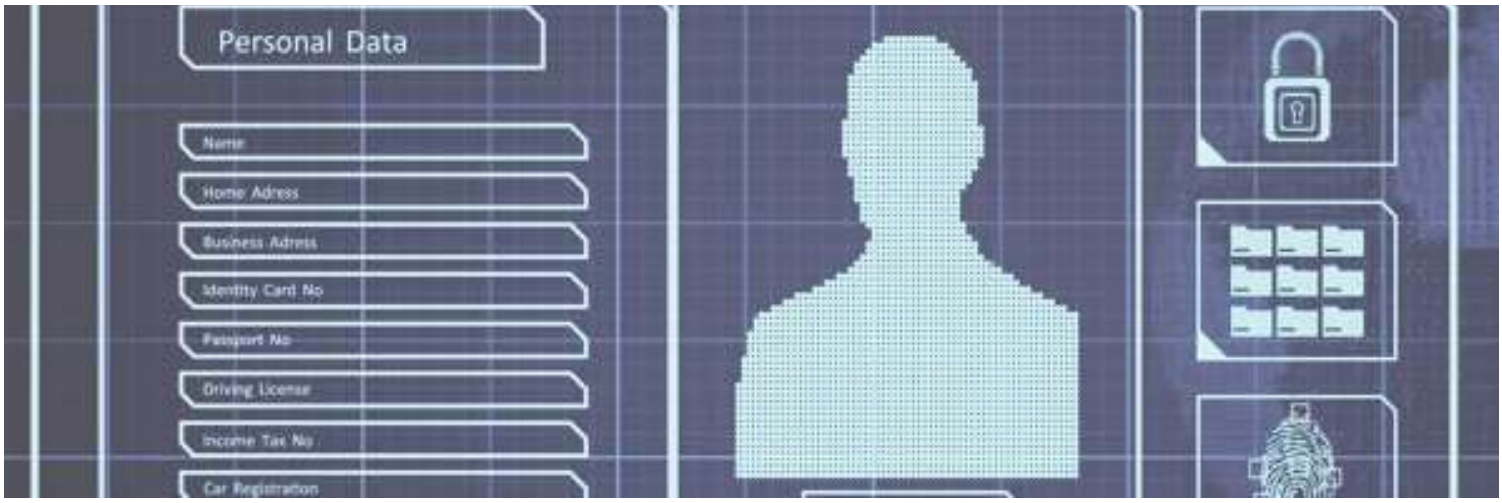




A number of SARs received from multiple reporters provided vital financial intelligence during an ongoing investigation into the unlawful practices of multiple companies involved in waste management. This intelligence enabled the investigating LEA to proceed in requesting further information to open up additional lines of enquiry and evidential opportunities relating to the case. For example, one reporter suspected a customer was laundering funds from tax evasion relating to waste management and decided to submit a SAR. This and other SAR intelligence evidenced further suspected criminality including tax evasion, operating without appropriate licenses, and layering of funds indicative of money laundering. LEA enquiries are still in operation with a view to a Proceeds of Crime Act (PoCA) confiscation investigation.

Fraud

Following a review of their customer's business account, a reporter identified several suspicious deposits. The deposits into the business account were consistently higher than the goods advertised for sale on the business' website and the majority of the payments were received on the same day from the same payment card located overseas. The reporter suspected that the business account was being used for money laundering and wished to end their relationship with their customer, submitting a DAML SAR to the UKFIU to request a defence to return the funds. The UKFIU disseminated the DAML SAR to the relevant LEA who began an investigation to locate the source of the funds. The LEA contacted the customer, who revealed they were an ongoing victim of identity fraud and had no knowledge of the business or business account. With this information, the UKFIU refused the DAML SAR to allow for further investigation. The LEA applied for an AFO leading to the uncontested forfeiture of over £10,000. As a result of this DAML SAR, the customer was safeguarded from further identity fraud harm, while criminal property was withheld from the offender responsible for setting up the fraudulent business account.



A reporter suspected that their customer was complicit in money laundering and layering the proceeds of crime. The customer's account had received a series of payments in excess of £50,000 from a business account that was also under investigation for suspicious activity and failure to provide a legitimate explanation for the funds, despite the reporter's repeated contact attempts. The reporter wanted to end their relationship with the customer and submitted a DAML SAR to return funds to the customer. The DAML was referred to the relevant LEA and subsequently refused to allow further investigation. The LEA discovered the customer was in fact a victim of stolen identity and the account had been fraudulently opened in their name. Using open source intelligence, the LEA discovered the business who had sent payments to the customer was linked to scams and fraudulent activity. The LEA obtained an AFO on the customer's account for over £35,000 which was subsequently forfeited. The LEA was able to use the intelligence to link together a series of additional fraudulent businesses and linked accounts, enabling a further forfeiture of over £45,000 of funds. This SAR intelligence assisted the LEA by discovering further criminality and removing the proceeds of crime from the perpetrators.

As part of an ongoing fraud investigation, an LEA contacted a reporter regarding a subject suspected of involvement in fraudulent activity, prompting the reporter to review the subject's account. The reporter's review identified concerns that a fraudulent ID had been provided by the customer during their Know Your Customer (KYC) checks and activity on the subject's account was indicative of money laundering. The reporter subsequently exited the relationship with the subject and submitted a SAR containing intelligence which identified several accounts linked to the subject and highlighted suspected offences, including money laundering and the use of a forged ID. The UKFIU shared the intelligence with the LEA, enabling the LEA to pursue additional lines of enquiry linked to fraudulent insurance claims. The SAR provided previously unknown information on the subject and methods used to avoid being caught and supported the LEA in obtaining production orders on the subject's account. The production orders assisted in identifying additional accounts used by members of an Organised Crime Group (OCG) connected to the subject. These accounts had fraudulent funds in excess of £68,000 pass through them. The subject was subsequently arrested and remains under investigation.

During their Customer Due Diligence (CDD) checks, a reporter identified concerns in relation to a business account in receipt of a high volume of payments from international accounts, which were then quickly dispersed to multiple third-party accounts. Public searches also raised concerns around one of the main third-parties the business account was sending money too. This led to reporter suspicion that the business account was being used as an intermediary to launder the proceeds of crime. The reporter decided to exit their relationship with the business and submitted a DAML SAR to pay away the account balance. The UKFIU refused the DAML request and shared the intelligence with an LEA, who conducted an investigation. The LEA sought and successfully obtained an AFO for the account balance of over £22,000 which was subsequently forfeited. The DAML SAR provided key lines of enquiry that allowed the LEA to successfully seize criminal assets and prevent further money laundering from the business account.





A key services provider (the reporter) held suspicions that a vulnerable customer's account held the proceeds of crime. The customer's account received a high volume of payments, resulting in a large account balance that did not match the customer's profile. This suspicion was reinforced when the reporter was approached by a victim, whose debit card had been fraudulently used to fund the payments into the customer's account. The reporter sought a DAML due to concerns of accepting payment for services from the customer's account. The UKFIU shared the DAML SAR intelligence with the relevant LEA, who actively engaged with the reporter to understand the customer's vulnerability and ensure that the customer retained access to key services. The LEA launched an investigation to assess which of the funds in the customer's account were legitimate and which were the proceeds of crime. During this investigation, the customer disclaimed the balance of over £8,000 held in the customer's account. The LEA sought and successfully obtained an account freezing order AFO on the proceeds of crime.



A reporter submitted a DAML SAR to exit their relationship with a customer and pay away funds they suspected to be the proceeds of crime. The customer set up a new business account for a newly incorporated business, which then received several high value payments from a public body. More than £150,000 was quickly transferred from the business account to third parties and businesses who then immediately transferred the funds onwards. Further payments of over £150,000 from the public body were blocked by the reporter before reaching the customer's business account. Following enquiries, the public body confirmed that the customer's business was not entitled to the payments. The UKFIU disseminated the DAML SAR to an LEA for further investigation. The LEA's investigation found that the business had been set up by the customer as a shell company to fraudulently claim the funds. The customer was revealed to have previously been associated with an OCG and had a previous conviction for drug related offences. The LEA pursued confiscation measures and £160,000 was forfeited. The investigation into the suspicious activity prevented further public funds from being misappropriated and the forfeited £160,000 was returned to the public body.



A reporter became concerned that a customer was using a website as a front to process fraudulent transactions. Several hundred suspicious payments had been made through the website, with a high percentage of these disputed by cardholders who had not received the purchased goods. The reporter therefore decided to end its relationship with the customer and submitted a DAML SAR to pay away the account balance, which totalled over £7,000. The UKFIU refused the DAML SAR and fast-tracked the intelligence to the relevant LEA. The LEA commenced an investigation into the source of funds and discovered that the website's business address was registered to a PO Box known to be used by perpetrators of economic crime and the director's home address was overseas, increasing suspicion that the website was fraudulently selling goods without intention to supply. The LEA successfully obtained an AFO and the funds held in the customer's account were subsequently forfeited. The DAML SAR provided law enforcement valuable intelligence to investigate, prevent fraud and recover over £7,000.

Money Muling

Following an internal alert, a reporter found that their customer's account was receiving funds from multiple third parties, which were rapidly transferred to an external account, indicating potential money muling activity and a suspected attempt to layer the proceeds of crime. The customer had been making payments to an online dating website, known to be easily utilised by fraudsters intending to commit romance fraud. The reporter submitted a DAML SAR which was subsequently refused. The LEA's investigation found that the customer was known to them as a previous victim of romance fraud and was now being targeted by criminals to launder funds. The LEA obtained an AFO for over £3,000 which was subsequently forfeited following the LEA's investigation. The LEA conducted a welfare check on the customer to educate them and ensure that adequate safeguarding measures were in place. This DAML SAR prevented the customer from continuing to be used as a money mule to launder the proceeds of crime.



A reporter suspected that a customer was being used as a money mule to layer the proceeds of crime through their account. The customer had received a transfer of over £8,000 soon after opening the account which they attempted to move to cryptocurrency accounts, just minutes after receipt. The reporter suspended the account and contacted the customer to make enquiries. The customer explained that an associate had transferred the funds to enable the customer to make a high-value purchase. The reporter suspected that the customer and their associate were unwitting money mules and submitted a DAML SAR to return the funds while closing the account. The DAML request was refused by the UKFIU and the intelligence disseminated to an LEA for further investigation. Upon first contact with the LEA, the customer disclaimed the funds, but due to the customer being considered vulnerable, a safeguarding officer made contact to discuss the case further. It was revealed that the customer had been contacted by an unknown third party who had copies of the customer's personal documents and images. The third party had coerced the customer with specific instructions to relay to the LEA about the source and purpose of the funds. The submission of this DAML SAR led to the safeguarding of a vulnerable customer, who would have endured further financial abuse, and the forfeiture of over £8,000 of criminal property, which would have been moved undetected.







Drugs

A DAML SAR was submitted by a reporter after their customer (the suspect) was flagged as a suspect in a drug supply investigation. The suspect had been arrested whilst in transit and was found to be in possession of drugs and over £10,000 in cash. Upon review of the suspect's account, the reporter held suspicion that the account was being used to launder the proceeds derived from drug related crime and wished to exit their relationship with the suspect. Account activity displayed common indicators associated with drug related crime including: the receipt of rounded payments funded by multiple third parties, payment references alluding to street names of drugs and these payments being the sole source of funds on the account. None of the deposits on the account were indicative of the suspect receiving a legitimate income. This information, combined with the suspect's arrest and an additional previous arrest for possession with the intent to supply drugs, suggested that the funds were the proceeds of crime. The DAML was refused by the UKFIU and SAR intelligence shared with an LEA who pursued asset recovery methods, resulting in the forfeiture of over £10,000 of the seized cash and over £1,000 held in the suspect's account. Criminal investigations are ongoing.



SARs intelligence supported an LEA's investigation into a suspect involved in the supply of Class A drugs. The SARs noted activity of concern on the suspect's account, including suspicious third-party deposits for small rounded amounts, the account regularly acting as an intermediary for quickly transferred deposits and rapid movement of funds indicative of layering. The suspect was listed as unemployed and in receipt of benefit payments, leaving no clear explanation for the account deposits. Through SARs intelligence, the LEA were also able to identify a company suspected to have been set up by the suspect as a front to process fraudulent transactions as payments were made to the company by cards reported as lost, stolen or where the account had been closed. This intelligence assisted the LEA's investigation to demonstrate the suspect had no legitimate income and also enabled the investigating LEA to identify another LEA who had an interest in, and has charged the suspect for similar offences.

A reporter held suspicion that a subject's account was laundering the proceeds of crime derived from the supply of drugs. When the subject opened the account, they stated that the source of funds would be from wages, yet no payments matched this activity. Instead, the account received a high volume of small payments from third party accounts, including references unrelated to the account's expenditure. Many of the payments occurred at irregular times of the day and were in excess of the subject's expected income. The reporter decided to exit the relationship with the subject and submitted a DAML SAR to pay away the account balance. The UKFIU refused the DAML and shared SAR intelligence with the relevant LEA. The LEA launched an investigation and was able to obtain an AFO against the account balance. The subject was unable to give sufficient evidence as to how the funds were accumulated, resulting in the forfeiture of the account balance of over £8,000. The DAML SAR provided actionable intelligence that allowed law enforcement to stop the subject benefitting from the proceeds of crime.



Other

An LEA investigated a subject in a position of trust, who had undermined the integrity of the system in which they were entrusted to serve. The subject was connected to others (suspects) involved in the same behaviour, who were all known to each other. To support the LEA's investigation, the UKFIU shared SARs intelligence held on the suspects. Multiple reporters had submitted SARs due to the suspects' accounts receiving high volume funds from individuals that did not match the expected activity on the suspects' accounts. These funds were then withdrawn or transferred in a short period of time, and in some cases, the suspects could not provide sufficient documentation to demonstrate the origin of funds. As a result of the LEA's investigation, five suspects, including the original subject who held a position of trust, were arrested. These SARs allowed the LEA to identify previously unknown suspects, their account details and arrest them before they caused further harm in the subject's position of trust.



Concerns were raised after activity on a subject's digital wallet and open-source intelligence indicated funds were being used to purchase child sexual abuse material (CSAM), resulting in a SAR being submitted by the reporter. The UKFIU disseminated SAR intelligence to the relevant law LEA, who launched an investigation into the subject. LEA officers attended the subject's address where CSAM images were found. The subject was arrested and interviewed. Safeguarding disclosures were made to the subject's workplace to ensure no access to potentially vulnerable persons. The investigation is ongoing whilst a case against the subject is built. The SAR prevented the subject from further purchases of CSAM and ensured the subject had no access to vulnerable persons.