NCA
National Crime Agency

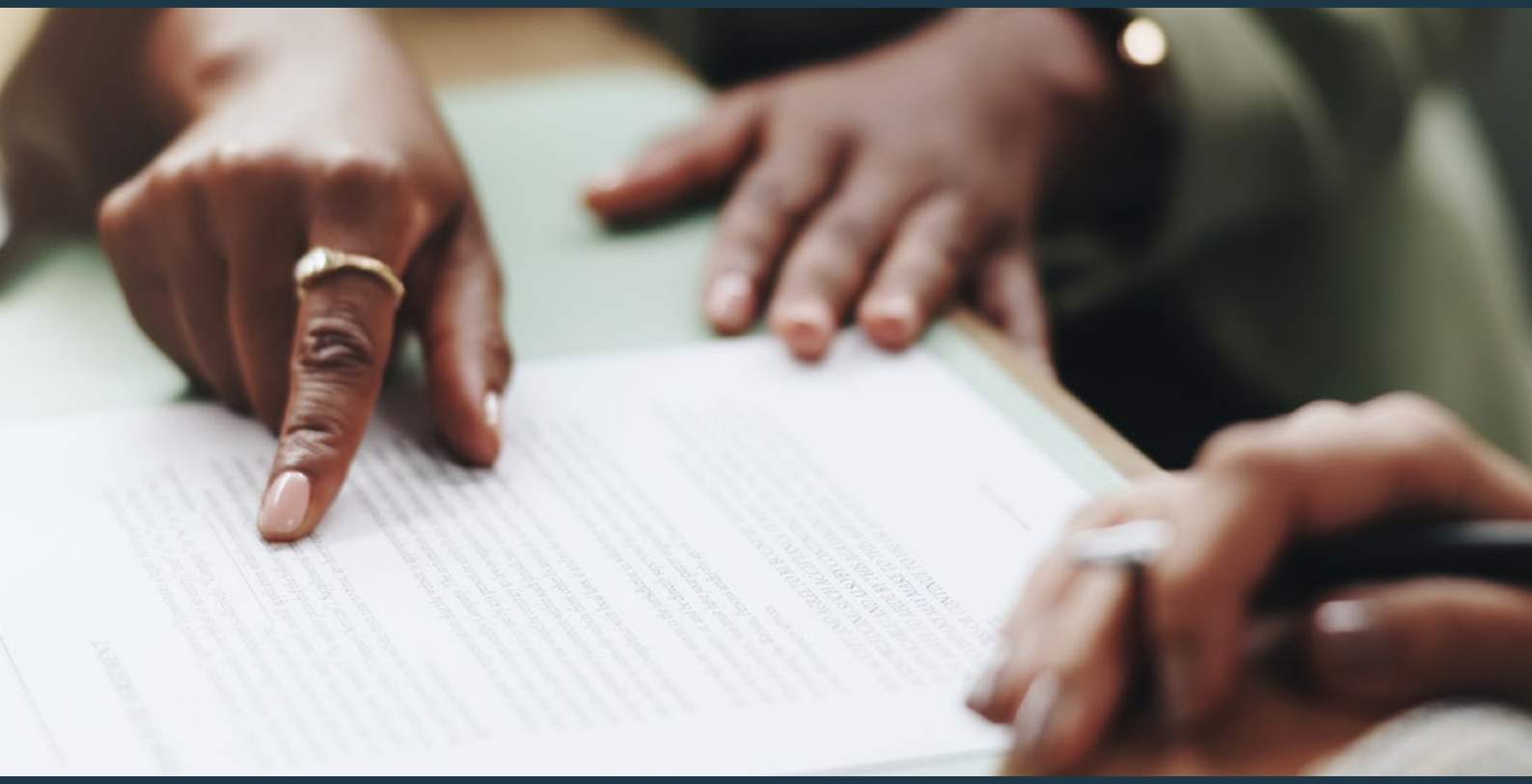
UKFIU
UK Financial Intelligence Unit

UKFIU SARs Best Practice Guidance

Chapter 2: Submitting a SAR

Guidance to help reporters submit high-quality Suspicious Activity Reports

November 2025 / version: 1.0



UKFIU
UK Financial Intelligence Unit

Contents

NCA
National Crime Agency

General Guidance and Information

The information within this guidance should not be taken as legal advice. Some references to legislation and regulations have been paraphrased, and all reporters are expected to seek their own legal advice on the application of the law to their business and their obligations to report.

The UK Financial Intelligence Unit (UKFIU) is an independent and autonomous unit located within the National Crime Agency (NCA). UKFIU officers are designated by the Director General (DG) of the NCA to receive SARs. While legislation and other guidance documents may refer to the NCA as the body authorised to receive SARs, this guidance will refer to the UKFIU, as the UKFIU is the only unit within the NCA authorised to receive these disclosures.

Please ensure you are familiar with Part 7 of POCA and Part 3 of TACT, as well as any sector-specific guidance issued by your AML supervisor, regulator, professional body or trade association. You may also wish to seek independent legal advice in respect of your obligations.

A note about crime reporting

SARs are solely for reporting knowledge or suspicion of money laundering under the Proceeds of Crime Act 2002 (POCA), or belief or suspicion relating to terrorist financing under the Terrorism Act 2000 (TACT). The SAR regime is not a route to report crime, including any predicate offences to the suspected money laundering. See Appendix for further information about the appropriate channels for reporting a crime or other information that does not satisfy the criteria for a SAR.

SARs are not crime reports, and submitting a SAR does not replace the need to make a crime report to the police or report the matter to another relevant government department or organisation (for example, HMRC or DWP). SARs are not for reporting concerns about vulnerable people or matters relating to immediate risks to others. Please ensure you have reported these to the police or other emergency services, using 101 or 999 as appropriate, before submitting your SAR.

If you have reported the matter to the police, emergency services or another organisation, ensure you detail this in your SAR and include any crime or report reference numbers you have been provided. If your SAR includes reference to a vulnerable person, outline all safeguarding steps you have taken. Failure to do so may result in the UKFIU or law enforcement contacting you to confirm what safeguarding steps you have taken.

See FAQs in **'Chapter 3: Understanding DAMLs and DATFs'** for further information regarding a threat of harm received followng submission of a DAML/DATF request.

The UK Suspicious Activity Reporting regime

Illicit finance and money laundering underpin and enable most forms of organised crime. This activity allows criminals and terrorists to further their operations and conceal their assets, which impacts the national security of the United Kingdom. This is where the SAR regime comes in.

Suspicious activity reports, or SARs, can be submitted by any organisation or individual who knows or suspects that another organisation or individual is engaged in money laundering or terrorist financing.

SARs are submitted to the UKFIU, which is part of the NCA. The UKFIU has sole national responsibility for receiving, analysing and disseminating SARs in the United Kingdom.

Submitting a SAR provides law enforcement with valuable information about potential criminality. It may also provide you and your organisation with a defence to a principal money laundering or terrorist financing offence. By submitting a valid SAR to the UKFIU, you will be complying with your legal obligations to report suspicious activity under the Proceeds of Crime Act 2002 (POCA) or Terrorism Act 2000 (TACT).

Organisations and individuals falling within the regulated sector have a legal obligation to submit SARs, and there are specific requirements relating to the minimum information SARs should contain.

Failure to submit a SAR when there is a legal obligation to do so could result in both individuals and organisations being prosecuted for criminal offences and/or facing action from their regulator. The offences of failing to disclose come under sections 330-331 of POCA and sections 19 and 21A of TACT, and the penalties for conviction on indictment are up to five years' imprisonment, a fine, or both.

The principal money laundering offences

- Concealing, disguising, converting, transferring, or removing criminal property from England and Wales, or from Scotland, or from Northern Ireland
- Arranging or facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquiring, using or possessing criminal property

The elements of each offence are defined in sections 327 to 329 of POCA.

Reporters must be also mindful of the offences of 'tipping off' (sections 333A of POCA and 21D of TACT) and prejudicing an investigation (sections 342 of POCA and 39 of TACT).

The terrorist financing offences

- Fund-raising for the purposes of terrorism
- Use and possession of money or other property for the purposes of terrorism
- Making money or other property available for the purposes of terrorism
- Insurers making payments in connection with terrorist demands
- Facilitating the retention or control of terrorist property, by or on behalf of another person

These offences are defined in sections 15 to 18 of TACT.

Defence requests

The UKFIU can provide a reporter with a defence against the principal money laundering or terrorist financing offences for a specified future activity or activities. The relevant power is contained in section 335 of POCA (seeking 'appropriate consent') and section 21ZA of TACT (seeking 'prior consent').

Should you wish to avail yourself of a defence, see **'Chapter 3: Understanding DAMLs and DATFs'** for further information.

What is meant by the term 'criminal property'?

Under POCA, property is 'criminal property' if it constitutes (or represents) a person's benefit from criminal conduct and the alleged offender knows or suspects that it constitutes or represents such a benefit.[1] Criminal conduct is conduct which constitutes an offence in any part of the UK, or would constitute an offence in the UK if it occurred there.[2] Criminal property may also be referred to as the 'proceeds of crime'.

It is important to understand the legal concept of fungibility, which may result in a small amount of criminal property tainting the whole of an asset. The Economic Crime and Corporate Transparency Act 2023 introduced exemptions relating to mixed-property transactions.[3] Reporters should seek legal or regulatory advice on the application of the concept of fungibility and the mixed property transaction exemption to their business.

[1]POCA, section 340(3).
[2]POCA, section 340(2).
[3]POCA, sections 327(2F), 328(8) and 329(2F).

What is meant by the term 'terrorist property'?

Under section 14 of TACT, 'terrorist property' is defined as:

a. money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation),

b. proceeds of the commission of acts of terrorism, and

c. proceeds of acts carried out for the purposes of terrorism.

'Terrorism' is also defined in TACT.[4]

When should I submit a SAR?

Both POCA[5] and TACT[6] require reporters in the regulated sector to submit a SAR as soon as practicable after developing the knowledge or suspicion. You must decide whether to submit the SAR under either POCA or TACT, depending on the nature of your suspicion and on a case-by-case basis. If you hold both a money laundering and a terrorist financing suspicion, you will need to submit two separate SARs, one detailing your money laundering suspicion and one detailing your terrorist financing suspicion. You should include reference in both SARs to the fact that you have submitted (or will be submitting) a separate SAR under the other legislation, but each SAR should contain a full description of your suspicion and not just refer the UKFIU to the other SAR.

If you are unsure how the SAR regime applies to you or your organisation, talk to your regulator, supervisor, professional body or trade association, or seek legal advice.

What constitutes 'suspicion'? What is the threshold for suspicion, and when do I hit that threshold to submit a SAR?

The UKFIU is unable to provide any advice on when a reporter should submit a SAR, beyond what POCA, TACT and the Money Laundering Regulations say.

Suspicion is not currently defined in legislation; however, some reporters reflect upon the Court of Appeal case *R v Da Silva* [2006] EWCA Crim 1654 in which the judge defined suspicion as:[7]

" ... a possibility, which is more than fanciful, that the relevant facts exist", noting that

"... a vague feeling of unease would not suffice ...".

It is always a matter for the reporter to decide at what point the 'threshold' is crossed and a disclosure to the UKFIU should be made. It is not for the UKFIU to comment on what circumstances should or should not be deemed suspicious - red flags for suspicious activity should have been discussed during your firm's AML training. More tailored advice or industry specific guidance may be available from your sector's trade body and/or AML supervisor.

[4] TACT, section 1.
[5] POCA, section 330
[6] TACT, section 21A
[7] *R v Da Silva* [2006] EWCA Crim 1654 [16].

What is the process once a SAR is submitted?

The UKFIU currently receives over 850,000 SARs every year. SARs are stored on a secure central database, which currently holds over 4.7 million reports.

With the exception of SARs in certain sensitive categories, SARs are made available to accredited officers in UK law enforcement agencies and remain on the searchable database for six years.

The UKFIU typically operates with very high caseloads and cannot provide progress updates or specific feedback on individual SARs.

Value of SARs

The UKFIU's work with SARs plays a critical role in alerting law enforcement to potential instances of money laundering and terrorist financing. SARs assist with the disruption of criminality and help law enforcement to direct resources by revealing new subjects of interest and emerging methodologies. SARs are a vital source of intelligence, not only for the investigation of economic crime but relevant to a wide range of criminal investigations.

Submitting a SAR

Top Tips:

- Complete all relevant sections of the SAR Portal and ensure data is inputted into the correct fields. Even if a field is shown as optional, if you hold the requested information, please include it. This helps the UKFIU and law enforcement to accurately identify and trace the subject of your disclosure.
- The SAR Portal limits the number of characters that can be used in the free text fields. When setting out the reason for your suspicion, focus on the information most relevant to explaining your suspicion of money laundering or terrorist financing. Remember, you do not need to provide all of the information law enforcement may need to prove an offence has been committed. If law enforcement decides to investigate, they can request further information from you through the proper channels.

Missing, inaccurate, or complex information:

- Limits analysis opportunities and identification of trends or patterns of criminality
- Reduces the overall effectiveness and usefulness of the SAR to law enforcement
- Makes it difficult to accurately and quickly identify subjects
- Could lead to law enforcement having to contact you to clarify or request missing information, which takes up time and resources

While the UKFIU appreciates it is more time-consuming, it is important that details are completed within the appropriate SAR Portal fields and not just written in the '**reason for suspicion**' field. Failure to do this may result in your SAR not appearing in relevant searches and information relevant to law enforcement investigations may be missed.

For security reasons, you are not able to upload attachments with your SAR – all the information relevant to the main party and your suspicion should be contained within one SAR. If there is further information or documents you think might be of interest to law enforcement, please state this within the SAR and include details of how the information can be requested. However, the SAR itself must contain all information relevant to your suspicion.

Useful SAR contacts

Reporter Engagement Team

If you require support in submitting SARs, have a question about SARs best practice, or have a question about anything in this guidance, please contact UKFIUEngagement@nca.gov.uk.

Defence Against Money Laundering (DAML)

All contact with the DAML Team is via email: DAML@nca.gov.uk

All contact regarding live DAML requests (that is, those within the 7 working day notice period) or DAMLs within the moratorium period must be directed to the DAML inbox. Do not send requests to individual case officers, even if you have their details. This could result in your request not being picked up.

You may make direct contact with the DAML Team in the following scenarios:

- To update information on a live DAML (such as updating the future specified activity value).
- To make the DAML team aware of a threat to life or threat of harm related to a live DAML, but only after reporting the threat to the appropriate law enforcement agency or emergency services (see **'Chapter 3: Understanding DAMLs and DATFs'** for further information).
- To withdraw a live DAML if a defence is no longer required. An explanation should also be given as to why the reporter wishes for the DAML to be withdrawn.

Terrorist Finance Team

All queries related to disclosures concerning terrorist financing can be sent to: UKFIUTFT@nca.gov.uk

In particular, all contact regarding live DATF requests (that is, within the 7 working day notice period) or TACT SARs must be directed to the TFT inbox. Do not send requests or queries to individual case officers, even if you have their details. This could result in your request not being picked up.

You may make direct contact with the Terrorist Financing Team in the following scenarios:

- To update information on a live DATF (such as updating the future specified activity value).
- To make the TF Team aware of a threat to life or threat of harm related to a live DATF, but only after reporting the threat to the appropriate law enforcement agency or emergency service (see **'Chapter 3: Understanding DAMLs and DATFs'** for further information).
- To withdraw a DATF if a defence is no longer required. An explanation should also be given as to why the reporter wishes for the DATF to be withdrawn.

SAR Technical Support

If you need technical support for the SAR Portal or the SARs Bulk Reporter API, please contact UKFIUSARs@nca.gov.uk.

Disclosing SARs and reporting SAR breaches

Queries regarding any disclosure of SARs (including as part of a Data Subject Access Request or court proceedings), or any breach of SARs confidentiality, must be directed to UKFIU.InfoManagement@nca.gov.uk.

Completing a SAR on the SAR Portal

Section 1: Background information

Privacy settings on SARs

You will be asked if you want to make the SAR private or accessible to anyone within your organisation with a SAR Portal login. If you make it private, then no other individual in your organisation can view, edit or submit the report.

Main party or associated party of a previous SAR

If the main party or associated party of your SAR has been the main party or associated party of a previous SAR submitted by your organisation within the last 6 years, ensure you include the SAR reference numbers (URNs) for those SARs in the relevant field. You can add up to 19 previous URNs on the SAR Portal. Do not include any internal reference numbers in this field, it must be the UKFIU issued SAR URN.

Failing to include the URNs of relevant previous SARs risks the connection between SARs being missed.

Known law enforcement interest

Please indicate if there is a known law enforcement (LEA) interest linked to your disclosure. Noting LEA interest in SARs helps the UKFIU to coordinate dissemination of the SAR and facilitate opportunities for early intervention and disruption.

LEA interest could relate to current or previous investigations into the main party, associated party, or the specific set of circumstances.

You may become aware of law enforcement interest relevant to your SAR because:

- the NCA or other LEA has made direct contact with your organisation in the form of a pre-order enquiry or court/production order;
- while conducting due diligence you identified publicly available court documentation or media articles relevant to the subject or your suspicion; or
- there has been an appeal for public assistance, or you have received an alert seeking information on the subject.

If there is a known LEA interest, please ensure you:

a. check the relevant box in the SAR Portal;

   AND

b. include details of the relevant force and any reference numbers in the '**Reason for Suspicion**' field of the SAR Portal.

If the relevant LEA is overseas, list the country and agency name in the '**Reason for Suspicion**'.

If the LEA (whether domestic or international) has made a direct enquiry with your organisation, please note if you have responded to them directly and when.

You must not name individual law enforcement officers in any SAR, unless they are the main party or associated party of the money laundering or terrorist financing suspicion. See further details in the Reason for Suspicion section of this guidance.

Court orders and law enforcement enquiries

If you have received notice of a court order or a production order in respect of a particular individual or entity, this may act as a catalyst for you to review your organisation's relationship with that individual or entity.

If, following such a review, you determine that there is an obligation to submit a SAR, or to seek a DAML or DATF, then your submission should clearly outline your suspicions in the context of your relationship with the subject. Suspicion should not be inherited, and receipt of a court order or production order on its own should not be the sole basis on which your suspicion is founded.

Legislation

Ensure you correctly select the legislation under which the SAR is being made (i.e. POCA or TACT). POCA and TACT SARs are dealt with by different teams within both the UKFIU and wider law enforcement. Submitting a SAR under the wrong legislation creates additional work for the officers and may prevent or delay the information you've submitted getting to the correct teams.

It is particularly important to select the correct legislation when seeking a DAML or DATF, as the defence afforded to you is based on the legislation you have submitted the request under. Defence requests submitted under POCA will only be considered for a defence against the principal money laundering offences in POCA. If you mistakenly seek a defence for a terrorism offence under POCA, you may not receive the appropriate defence for the prohibited act you are seeking to undertake, or the UKFIU response may be delayed while we seek clarification from you.

Sections 2 and 3: The main party and associated parties

SARs should contain all available identifying information about the main party and any associated parties. For those in the regulated sector, this includes all available customer due diligence (CDD) or enhanced due diligence (EDD) information you hold on the subjects.

Many of the subject identifier fields in this section are optional, as the amount of information you hold may depend on the sector you are in and the nature of your relationship with the subject. Please ensure you complete all of the fields you have information for, regardless of whether they are mandatory or optional.

Section 2: Main party

You will be asked if the main party is a **person** or a **legal entity**. The subsequent questions will change depending on the option you select.

If you select that the main party is a **person**, you will be asked if you hold the following information:

- Name (forename, middle name, surname, and any former names)
- Date of Birth
- Gender
- Nationality (up to three)
- Address (up to ten)
- Telephone number (up to ten)
- Occupation (up to ten)
- Employer (up to ten)

You will also be asked if the main party is a **politically exposed person**, and whether they are a **suspect** or a **victim**.

Please include as many of these details as you know about the main party. Understanding a subject's employment status, gender, nationality, occupation, etc, helps law enforcement to correctly identify the individual and is also useful in building a picture of the subject and understanding the suspicious activity.

If you select that the main party is a **legal entity**, you will be asked if you hold the following information:

- Entity name
- Address (up to ten)
- Company registration number
- Date of establishment
- Country of establishment
- Type of business
- VAT registration number

Please include as many of these details as you know about the main party.

Main party account details

You will be asked if you know the main party's account details. You can add up to 50 main party accounts. These accounts may be:

- A UK bank or building society account
- An international bank account
- A crypto-currency account
- Another type of account

Once selected, for each of the account types, a series of further questions will appear. Please complete as many of these fields as possible for each account.

Additional information about the main party

If the main party is an **individual**, you will be asked if you hold any of the following additional information about them:

- Passport number and country of issue (up to three)
- National insurance number (up to five)
- Identity card information (up to three)
- Driving licence information (up to ten)
- Birth or gender reassignment certificate information (up to two)
- Vehicle details (up to ten)
- Email address (up to ten)
- Utility accounts (up to ten)
- Gaming account ID
- Any other information (up to ten)

If the main subject is a **legal entity**, you will be asked if you hold any of the following additional information about the entity:

- Telephone number (up to ten)
- Email address (up to ten)
- Tax reference number
- Vehicle details (up to ten)
- Their supervisory body and their registration ID
- IP addresses (up to ten)
- Web addresses (up to ten)
- Any other information (up to ten)

Please provide as much of the requested additional information as possible.

Section 3: Associated party

You will then be asked if there is a person or a legal entity associated with your suspicion. These are known as 'associated parties' or 'associated subjects'. An associated party is a person or entity linked to the main subject/party in some direct way, and who is suspected of being involved in the same suspicious activity.

If you indicate that there are associated parties relevant to your SAR, you will be asked for all the same information for these parties as you were asked for the main party (see above).

It is appreciated that you may not always have the full details concerning all of the associated parties involved, especially where you are reporting on subjects who are not known to you directly. However, include as much detail about all associated persons or entities as you have available to you. This will help the UKFIU and law enforcement identify any other SARs where the associated parties may be mentioned.

Specific fields – apply to both the main party and any associated parties

Date of birth (DOB)

Where the subject is an individual, include their full date of birth in the format DD/MM/YYYY. If you only know a partial DOB you will be unable to include this in the SAR Portal field. However, ensure you include this in the '**Reason for suspicion**' field including as much information as you have. This information is vital for correctly identifying individual subjects.

Addresses

Include the subject's full address and postcode. Specify the type of address using the drop down, i.e. home, accommodation, trading, registered, etc. You will also need to indicate whether the address is current, previous or unknown. The UKFIU's systems use the postcode of the main subject to allocate SARs to the appropriate LEAs.

For UK addresses, use the postcode format SW1A 1NT. For international addresses, please ensure the country field is populated. Provide as much information as possible. If an overseas address is in a non-Roman alphabet, please provide an English translation of the address. SARs with non-Roman characters or symbols may be rejected by the SAR Portal's firewall and your SAR will not be received.

Financial information

If known, provide the relevant account details of all subjects related to your suspicion. Use the standard format: sort code account code e.g. 012345 12345678 or full IBAN. If the account is a virtual IBAN, cross-border account, or multi-currency account, confirm the jurisdiction where the master account is located, particularly if the account is not held in the UK. This helps the UKFIU and law enforcement to identify the correct channels for requesting further information about the account.

If you select yes to international payments, detail in the reason for suspicion the countries where payments have been sent to or received from and clarify how this forms part of your suspicion.

Section 4: Glossary codes and alerts

Glossary codes are primarily used by the UKFIU and law enforcement to quickly identify SARs relating to specific threat areas that may require immediate attention, together with areas of current interest. Glossary codes can also be used to aid the UKFIU in identifying and analysing emerging trends and patterns to share with the wider UK Law Enforcement community and reporters for their information.

Important:

Selecting a specific glossary code **does not** mean you are reporting that predicate crime in addition to your money laundering suspicion. It is simply an indication for law enforcement of the predicate offence(s) related to your suspicion. SARs are not crime reports, and submitting a SAR does not remove the requirement to make a crime report to the police or report the matter to another relevant government department or organisation. See Appendix.

SARs are also not for reporting concerns about vulnerable people or matters relating to immediate risks to others. Please ensure you have reported these to the police or other emergency services, using 101 or 999 as appropriate, before submitting your SAR.

You can use **multiple glossary codes** in your SAR, provided it is clear in your reason for suspicion why you think they apply. It is also possible that there is no code relevant to your suspicion. Further guidance on when to apply each code to your SAR is available on the SAR Portal. The SAR Portal glossary codes list will be updated from time to time, as new codes are added and others become obsolete. Please check the complete list (via the SAR Portal) each time you submit a SAR to ensure you have selected all relevant glossary codes.

Reporters should not be manually typing glossary codes into SARs.[8] If you have a query about a glossary code that is no longer appearing in the list, please contact UKFIUEngagement@nca.gov.uk for more information.

If you do select a glossary code within the SAR Portal, you should be able to explain within the reason for suspicion field why the glossary code was selected.

You can find definitions of all the glossary codes on the SAR Portal.

NCA Alerts

The NCA Alerts process is a recognised and established way the NCA communicates with the UK's private sector. These are written communications that warn of a specific risk/threat/problem. All Alerts contain a keyword and/or an alert code. If you submit a SAR as a result of the information contained in an NCA Alert (including JMLIT Alerts), check the relevant box and provide the alert code in the field that appears e.g. 0123-23Aa.

[8] In some circumstances, reporters may be asked to manually type a specific code into the reason for suspicion field. This is generally only for time-limited codes or codes relevant to a limited group of reporters. If you are unsure whether you should be doing this, please contact UKFIUEngagement@nca.gov.uk.

SAR glossary codes are different to NCA Alert codes. NCA Alerts are warnings produced by the NCA for the general public or businesses in specific sectors. They can be used to inform a range of businesses, financial institutions and industry about serious organised crime and its effects but can simultaneously be related to money laundering.

Including relevant NCA alert codes in your SAR allows law enforcement, including the NCA, to identify SARs that might provide information relevant to existing investigations or operations.

STORs and CIFAS reports

If you have also submitted a STOR to HMRC in relation to the suspicious activity outlined in your SAR, include the application number in the relevant field.

If you have also submitted a CIFAS report in relation to the suspicious activity outlined in your SAR, include the case number in the relevant field.

Including details of related STORs or CIFAS reports in your SAR allows the relevant law enforcement agencies to identify SARs relevant to reports in their system.

Section 5: Reason for suspicion (including criminal property and threshold variation)

The next section of the SAR Portal will ask if you are seeking a threshold variation.

Threshold variations can only be requested by deposit-taking bodies, electronic money institutions and payment institutions, as those terms are defined in POCA.

Part 7 of POCA provides deposit-taking bodies, electronic money institutions and payment institutions with a threshold amount under which they can operate an account where there is a suspicion of money laundering or criminal property without seeking a defence to money laundering from the UKFIU. As at the date of publication of this guidance, the threshold amount is set at £3,000.[9]

Section 339A of POCA allows deposit-taking bodies, electronic money institutions and payment institutions to request a "threshold variation" to amend the threshold amount.

- A threshold variation request cannot include a request for a DAML or a DATF.
- There is no statutory deadline for responding to threshold variation requests. If you also wish to request a defence, then this request should be submitted as a separate SAR.

Note:

You can only request a threshold variation if:

- you are submitting your SAR under POCA;
- your SAR does not also contain a DAML or DATF request; and
- you are a deposit-taking body, electronic money institution or payment institution, as those terms are defined in POCA.

If the above do not apply to your submission, skip this question by selecting **'No'** and then clicking **Save and continue**.

Reason for suspicion

The suspicion element of your SAR is the rationale behind why a SAR is being submitted and therefore should explicitly detail why you are suspicious of money laundering/terrorist financing, and how you have arrived at that suspicion.

A clear and concise reason for suspicion is essential in all SARs, along with a clear description of the suspected criminal or terrorist property. Suspicion is also a very important factor when seeking a DAML or DATF.

Summary of suspicion

The SAR Portal will ask you to provide a brief summary to highlight the key elements of your suspicion. Briefly summarise your suspicion in one or two sentences.

[9] POCA, Section 339A

How to write the reason for suspicion

The '**Reason for suspicion**' field in the SAR Portal is limited to 8,000 characters. Ensure your SAR is concise and includes all the information relevant to your suspicion within this character limit. It is not necessary to include excessive information; keep this section brief with the key information relevant to your suspicion. Reporters should not submit multiple SARs for the same subject/ suspicion in order to circumvent the character limit. Reporters should be able to include all relevant information in one SAR submission.

What to include in the reason for suspicion

Who is involved?

How are they involved?

If you have indicated that there are associated parties, expand on the link/association between them and the main party in the reason for suspicion field. Subjects referenced in the reason for suspicion that are part of your suspicion should also be listed as associated parties in the relevant fields, with as much information about them as possible.

If the beneficiary/remitter of a suspicious transaction is believed to be complicit in the suspicious activity, then consider providing their details as an associated party.

How did the circumstances arise?

When did the circumstances arise?

When are the circumstances planned to happen?

Why are you suspicious or **what** is your knowledge based on?

If you are suspicious because the activity deviates from the normal activity for that customer/ business sector, briefly explain how the activity differs.

If you have undertaken open-source searches and these have added to or enhanced your suspicion, include a brief summary of what those searches were and what they found. Include the title, date and publication name of any relevant article. Do not just include a link to the article.

Details regarding the suspected **criminal property or terrorist property** – see criminal property/terrorist property.

Consider locations. If you are suspicious of a payment activity, it can be helpful to list the town/city where the activity took place. This can be useful for identifying trends and hotspots. Please also indicate if any element of the transaction/activity took place outside of the UK, and if so where.

Summarise relevant suspicious transaction information, but you must also ensure suspicious transactions have been inputted into the '**Suspicious Transaction**' fields of the SAR Portal - see Section 6: Suspicious transactions.

If the suspicious activity does not involve a financial transaction, please explain the suspicious activity that has occurred/will occur.

UK nexus

While the money laundering and terrorist financing offences can have extra-territorial effect, SARs should have a clear UK link or 'nexus' if being reported to the UKFIU. This UK link may be through the main subject or an associated party, the involvement of a UK-based entity, or because the criminal or terrorist property is located in the UK. This is not an exhaustive list and reporters must satisfy themselves that there is a UK nexus to their suspicion and ensure this is clearly described in the SAR.

Criminal property / terrorist property

In all SARs, it is essential that the reporter describes the suspected criminal or terrorist property. If you are seeking either a DAML or a DATF, there are specific fields for including information about the criminal or terrorist property.

If you are submitting a SAR (and not seeking a defence), you will need to include the description of the criminal or terrorist property in the reason for suspicion field.

When articulating the criminal/terrorist property, you should include:

What is the criminal/terrorist property?

What is the value of the property, including currency? This can be an estimate if the exact value is not known. If you have estimated the value, make this clear in your description of the property. If the property is cryptocurrency, enter the converted value of the cryptocurrency in GBP as well as the value in the relevant cryptocurrency.

Where is the criminal/terrorist property? For example, a casino in London, a property in Hampshire etc. If the location is not known, include an explanation of why you are unable to identify its location.

Why is it suspected to be criminal property?

It is best practice to include the destination of any fund movements detailed in the SAR. If this information is included, law enforcement can track those funds more easily.

Further best practice for writing your reason for suspicion

- The explicit rationale behind the reason for suspicion and the context of why the SAR is being submitted should be clearly communicated in simple English.
- Structure your reason for suspicion in a logical format including all relevant information.
- Provide a chronological sequence of events.
- Keep the content clear, concise and simple.
- Do not assume the end user of the SAR will have a detailed understanding of your sector or business. Avoid jargon, define any acronyms used, and explain complex or sector-specific products, services or activities.
- Do not write the SAR in capital letters – this makes it very difficult to read.

- If including a large amount of information/text, break it up into manageable and readable paragraphs.
- If you hold additional information you think would be relevant to law enforcement, list what additional information you hold within the reason for suspicion field.
- If you have selected any of the glossary codes, the reason for suspicion should make it clear why the glossary code has been selected. For example, if you have selected 'Benefit Fraud XXF1XX', the reason for suspicion should articulate clearly why you suspect the main party has engaged in benefit fraud.
- Include a description of your intended next steps e.g. exiting the relationship, monitoring the customer, continuing the relationship etc.

Suspicion should not be inherited

The suspicion of money laundering remains with the reporter. If you have received information from law enforcement about your client/customer, which leads you to review your relationship with that individual/company and you reach the conclusion that you have your own, independent suspicion of money laundering, then you should consider you obligations to submit a SAR. Reporters need to be able to articulate their own suspicion within the SAR. See Court orders and law enforcement enquiries.

Known law enforcement interest

If you have indicated in the earlier section of your SAR that there is known law enforcement interest, include details of the relevant force and any reference numbers in this section. If the relevant LEA is overseas, include the country and agency name. If the LEA (whether domestic or international) has made a direct enquiry of your organisation, note if you have responded to them directly and when.

You must not name individual law enforcement officers in any SAR, unless they are the main party or associated party of the money laundering or terrorist financing suspicion. See Known law enforcement interest.

Main party source of salary

If you are aware of the main party's source of salary, include this information within the reason for suspicion field.

Providing details of the main party's occupation/salary assists with:

- Making judgments about the origin of funds
- Identifying if the activity is inconsistent with the customer's profile or expected behaviour
- Identifying whether the main party is using professional knowledge to facilitate money laundering, including identifying whether there are opportunities to engage with regulators and supervisors

Section 6: Suspicious transactions

You will be asked if the circumstances you are reporting involve suspicious transactions. Only add transactions you know, suspect or believe to be related to the money laundering or terrorist financing. While it is not necessary to include reams of transactional data in your SAR, you must ensure that the transactions relevant to your suspicion are included in the suspicious transactions fields, and not only detailed in the reason for suspicion field. While your reason for suspicion should make it clear why you consider these transactions to be suspicious, failing to provide details of the suspicious transactions in the correct fields will limit the usefulness of your SAR to law enforcement.

If there are multiple suspicious transactions, you can add subsequent transactions after adding the initial one in the SAR Portal.

Main party account details

You will be asked again if you know the account details of the main party used in the suspicious transaction. If you completed this information under the '**Main Party**' field, you will be able to select the account details you have already completed. If the details are not the same, or you did not complete this section earlier in the SAR Portal, you will need to add the account details here.

You will be asked for the following details, depending on the type of account:

- UK bank or building society account
  - » Account holder
  - » Name of financial institution
  - » Account number
  - » Sort code 6 digits, separated with dashes, e.g. 12-34-56
  - » Customer reference number (optional)
  - » Roll number (optional)

Virtual IBANs

If either account used in the transaction is a virtual IBAN, cross-border account, or multi-currency account, ensure you include the jurisdiction where the master account is held in the additional information field, particularly if the account is not held in the UK. This helps the UKFIU and law enforcement to identify the correct channels for requesting further information about the transaction and account.

- International bank account
  - » Account holder
  - » Name of financial institution
  - » International Bank Account Number (IBAN) - IBAN should contain the two-letter country code, followed by the two-digit checking number, and then contain the account number comprising 11 to 30 digits or capital letters, e.g. AA0001234567890
  - » Bank Identification Code (optional) - BIC should be 8 to 11 characters, comprising only digits and capital letters, e.g. HBUKGB4B
- Crypto-currency account
  - » Wallet address
  - » Crypto-currency name
- Other account
  - » Enter other account reference

Details about the transaction

You will then be asked further details about the suspicious transactions.

The SAR Portal will ask you:

- If the main party of this suspicious transaction sent funds or received funds
- The type of transaction
- The currency used in the suspicious transaction and the amount
- The date (mandatory) and time (optional) of the transaction

Counter party to the transaction

You will be asked if you know the counter party to the transaction. This is the counter party that is connected to the suspicious transactions.

You can select from the information already added (main party / associated party), add someone else, or select that you do not know.

If you select '**someone else**', you will then be asked subsequent questions regarding the counter party (whether a person or a legal entity). You will be asked to complete the same fields described under 'Main party account details' for the counter party.

When the transaction is related to buying or selling real estate property

You will be asked if the transaction is related to buying or selling real estate property. For example, buying or selling of a house or commercial premises.

If your transaction is not related to buying or selling real estate property, select **'No'**.

If you select **'Yes'**, you will be asked the following details:

- Property Amount
- Currency
- Building number or name
- Street
- District (optional)
- City/Town (optional)
- County (optional)
- Postcode
- Country

You can add up to 19 more addresses. To add further addresses, select **'Add another address'**.

Location (address) of the transaction

The SAR Portal will ask you if you know the location (address) of this transaction. You can select '**Yes**' or '**No**'.

This is the address that the transaction is connected to. For example, if a payment is made from subject 1's account to subject 2's account. The address of this transaction would be the address that subject 1's account details are registered to.

If you do know the location (address) of this transaction, you will be asked the following subsequent questions:

- Building number or name
- Street
- District (optional)
- Town or City (optional)
- County (optional)
- Postcode
- Country

Financial details known to you

The SAR Portal will ask for the financial details known to you. You can select from the following options:

- Do you know the **payment card number** that was used in this transaction?
  - » If you select this option, you will then be asked for the payment card number.
- Do you know if this transaction was associated with **financial security trading**?
  - » If you select this option, you will then be asked to enter the International Securities Identification Number (ISIN) for the security traded and the name of the exchange.

If you do not know this information, continue without selecting an option.

IP addresses or IMEI / MEID info relevant to the transaction

You will then be asked to select if you have the following information. If you do not hold this information, continue without selecting an option. If you select one/both options, you will be asked further details on this:

- Do you know of an **IP address** used by the main party for the transaction?
  - » Enter the IPV4 address
  - » Enter the IPV6 address
- Date and time stamp for this IP address. Time information is optional.
- Do you know the **International Mobile Equipment Identifier (IMEI)** or **Mobile Equipment ID (MEID)** that was used for this transaction?
  - » IMEI or MEID number
  - » Service provider (optional)
  - » Operating system (optional)

Additional transaction information

You will then be asked if you have any additional information about this specific transaction that is relevant. You can add free text (200 characters) into this field.

Additional transaction information may include:

- If any part of the transaction took place outside of the UK, include further information about the relevant jurisdiction.
- If either account used in the transaction is a virtual IBAN, cross-border account, or multi-currency account, include the jurisdiction where the master account is held, particularly if the account is not held in the UK.
- If the transaction involved cryptocurrency, include the transaction hash if known.

Add another transaction

You will need to add the transactional information for relevant suspicious transactions. You can add additional transactions by selecting **'Yes'**, when asked **'Do you want to add another transaction?'**

The SAR Portal will allow you to add up to 50 transactions.

Section 7: Defence Against Money Laundering (DAML) or Defence Against Terrorist Financing (DATF)

The UKFIU can provide a reporter with a defence against the money laundering or terrorist financing offences, for a specified future activity or activities. The relevant power is contained in s335 of POCA (seeking 'appropriate consent') and s21ZA of TACT (seeking 'prior consent').

Should you wish to avail yourself of a defence, see **'Chapter 3: Understanding DAMLs and DATFs'** for further information; this provides information on the process.

If you need to request a DAML or a DATF, ensure you answer **'Yes'** to the question **'Do you wish to request a defence against money laundering (DAML)?'** or **'Do you wish to request a defence against terrorist financing (DATF)?'** The SAR Portal will then guide you through a series of questions / fields that need to be completed in order to submit your request.

If you do not select **'Yes'** to this question, but instead attempt to seek a defence by writing the request into the reason for suspicion field, your request will not be considered and you will not be afforded a defence to any money laundering or terrorist financing offences you commit as a result.

You may wish to consult your AML supervisor or trade body if you require any further guidance about your obligations to prevent money laundering and terrorist financing.

Should you wish to avail yourself of a defence, see **'Chapter 3: Understanding DAMLs and DATFs'** for further information.

Sections 8 and 9: Further information / report summary

Further information

You will be asked if you have any further information to support the suspicion that you have not included in the report. If you select '**yes**' here, please ensure you have listed what additional information you hold within the reason for suspicion field.

Review and submission

Before submitting, check that the content of your SAR is accurate and understandable.

You will not be able to access your SAR in the SAR Portal once submitted. You may be required to retain a copy of your SAR submission for audit or AML supervision purposes.[10]

To do this, select the **'print this page'** button at the bottom of the page (before you submit) and choose to either print or save as PDF. This copy of the SAR will only be accurate as at the point the SAR content was printed or saved. If you subsequently make further changes to your SAR prior to submission, you will need to print or save it again to ensure the copy in your records is an accurate reflection of what was submitted. The UKFIU cannot access draft SARs and printed/saved copies made prior to submission cannot be accepted as proof/confirmation of the final SAR submission by the UKFIU.

Please note: If you are saving/printing copies of SARs, you must ensure they are saved and stored securely. When storing SARs, reporters should consider their obligations under sections 333A and 342 of POCA, sections 21D and 39 of TACT, and the requirements of UK data protection legislation.

Important – Once you submit your SAR, you will no longer be able to view, save or print a copy of your submission and the UKFIU are unable to provide you with a copy.

[10] Under the MLRs, supervisory authorities have the power to request copies of SARs submitted by their supervised populations.

Frequently Asked Questions

Prior to submitting a SAR

Q1. Should I submit a SAR to report a crime or potential vulnerable person?

No. The SAR database constitutes an extremely useful intelligence tool for law enforcement on suspicions of money laundering and terrorist financing and the information it holds may be used by law enforcement to investigate other crimes. However, SARs are not crime reports and it is not possible to assure reporters that a particular SAR will be reviewed by law enforcement or lead to a positive outcome.

See A note about crime reporting and Appendix for more information about the appropriate channels for reporting a crime or other information that does not satisfy the criteria for a SAR. If you have information on serious and organised crime that you would like to provide to the NCA, but which does not meet the criteria for a SAR, you can use the NCA's public reporting tool available on the NCA website.

Q2. Will the information contained in the SAR I submit be held securely?

Yes. Once a SAR is received by the UKFIU it is held on a secure database that can only be accessed by UKFIU officers. After a period of 7-10 days, most SARs are made available to law enforcement officers and other end users, who are accredited to view SARs and have received training on SARs confidentiality. Refer to Home Office Circular 022/2015 on the confidentiality and sensitivity of SARs for further details and guidance.

In the unlikely event you are made aware that SARs confidentiality may have been breached, you should contact the UKFIU immediately - UKFIU.InfoManagement@nca.gov.uk.

Q3. How long is a draft SAR available on the SAR Portal?

Draft SARs are automatically saved every time you click the '**save and continue**' button as you navigate through the screens. Draft SARs will be deleted after 31 days of no activity

Q4. Can we add attachments or upload supporting documents to our SAR submission?

No. For security reasons, the SAR Portal does not allow you to attach or upload documents. If you would like to share further information with law enforcement or government departments, please mention in the reason for suspicion section that you 'hold further information, which is available upon request', together with details of how that information can be requested

Q5. Can I ask my client or customer further questions to satisfy any initial concerns and determine whether I should submit a SAR?

You can (and, in some cases, may be required to under the MLRs) make further enquiries of your client or customer to properly assess whether you are suspicious and whether you need to submit a SAR. However, when talking with your client or customer, you must be mindful of the offences of 'tipping off' (sections 333A of POCA and 21D of TACT) and prejudicing an investigation (sections 342 of POCA and 39 of TACT).

Q6. My SAR is particularly sensitive and I think access should be restricted, should I still use the SAR Portal or should I email the SAR to the UKFIU?

The SAR Portal is the most secure and efficient way to submit SARs to the UKFIU. It will ensure the information in your SAR is transmitted securely and only accessible by officers designated or accredited to do so. Provided you complete all of the relevant fields in the SAR Portal as accurately as possible, it will also ensure your SAR includes all the relevant information law enforcement might need to investigate your suspicions further.

You should never email SARs to the UKFIU. Due to the sensitive and confidential nature of SARs, it is really important that they are submitted through the correct channels. Once submitted via the SAR Portal, SARs are initially only available to designated UKFIU officers. The UKFIU runs a series of daily searches in order to identify SARs that may need to be fast tracked out to particular law enforcement agencies, or suppressed from general searching due to specific sensitivities of the SAR.

In Section 1 of the SAR Portal, you will be asked if you want to make the SAR private or accessible to anyone with a SAR Portal login within your organisation. If you make it private, then no other individual in your organisation can view, edit or submit the report. Please note, marking a SAR as 'private' only affects the way the SAR appears to you and your organisation within the SAR Portal while the SAR is in draft. It does not change the way the UKFIU will receive or manage the SAR once submitted.

Following submission of the SAR

Q7. Can I discuss the submission of my SAR with anyone, or inform a client or customer that I have made a report?

You should not discuss the fact of making a SAR with your client or customer or any other third party, if this risks prejudicing any investigation that might be carried out. Once a SAR has been submitted, all reporters should be mindful of the offences under sections 333A and 342 of POCA and sections 21D and 39 of TACT relating to 'tipping off' and 'prejudicing an investigation'. There are few exceptions to this rule (see s333B to s333D(2) of POCA and s21D to s21G of TACT). Further advice on these exceptions should be sought from supervisors, trade bodies, regulators or via legal advice.

Q8. I am under pressure from the subject. What should I tell them to avoid 'tipping off'?

The UKFIU does not provide or approve standard wording for you to use in such circumstances or give advice on methods to answer client queries or awkward questions, as these will vary by reporting sector. For this reason, this discussion is best had with supervisors, trade bodies, regulators or legal advisors.

If a subject is behaving in a threatening or intimidating manner, then consideration should be given to contacting local police on 999 or 101, as appropriate. See the FAQs in **Chapter 3: Understanding DAMLs and DATFs** for further information.

Q9. If new or additional information comes to light after I submit a SAR, what should I do?

Provided the new or additional information enhances or adds to your suspicion, you should submit a new SAR, in which you can provide the new or additional information that has come to light.

- Include previous SAR reference numbers provided to you by the UKFIU in the relevant SAR Portal fields
- Do not include any internal reference numbers which you may use yourselves

The absence of any previously submitted SAR reference numbers risks the connection between SARs being missed.

Do not submit a new SAR if the new information reduces your suspicion or removes your suspicion entirely. There is a different process if new or additional information comes to light after you submit a DAML or DATF. See Chapter 3: Understanding DAMLs and DATFs for further information.

Q10. Should I stop providing services to my client/customer once I submit a SAR?

It is recommended that you consider how you will handle your relationship with the subject once you have submitted a SAR. This applies particularly if the subject is a client or customer of your business. Whether or not to maintain a client relationship will be a decision for you or your organisations to make, based on your legal obligations and/or risk appetite. You may wish to discuss with your supervisor or professional body if you are unsure. If you decide to continue providing services to the client/customer, you will need to consider whether a DAML or DATF is required for any future activity.

If you have submitted a DAML or DATF, you must not proceed with the prohibted act(s) unless and until you receive a granted decision from the UKFIU or the seven working day notice period lapses without a response from the UKFIU.

Q11. Can I talk to police or other law enforcement regarding my disclosure?

The UKFIU may refer your SAR to police or other law enforcement agencies as part of the process. Law enforcement may contact you for further information or to discuss the circumstances of your disclosure in more detail.

If you are contacted by law enforcement, we recommend that you verify that they are who they say they are, for instance by ringing them back via their force/agency switchboard. SARs can only be shared with law enforcement officers who are either SAR researchers or accredited financial investigators or financial intelligence officers. The individuals contacting you should hold one of these accreditations. You should not assume that all law enforcement officers have access to SARs or should be privy to the information contained in them.

Q12. Can the UKFIU share SAR information with the Financial Ombudsman Service?

There is a process for advising the Financial Ombudsman Service that a SAR has been submitted, if required. See the guidance here: https://www.jmlsg.org.uk/guidance/current-guidance/

Please note, you should not provide a copy of the SAR to the Financial Ombudsman Service.

Acronyms and definitions explained

Acronym	Definition
AML	Anti Money Laundering
DAML	Defence Against Money Laundering
DATF	Defence Against Terrorist Financing
ECCTA	Economic Crime and Corporate Transparency Act 2023
JMLIT	Joint Money Laundering Intelligence Taskforce
LE / LEA	Law Enforcement / Law Enforcement Agency
MLR	Money Laundering Regulations
MLRO	Money Laundering Reporting Officer
NCA	National Crime Agency
NECC	National Economic Crime Centre
NO	Nominated Officer
POCA	Proceeds of Crime Act 2002
POCC	Proceeds of Crime Centre
TACT	Terrorism Act 2000
TOH	Threat of Harm
TTL	Threat to Life
UKFIU	United Kingdom Financial Intelligence Unit

Appendix – Alternative reporting routes

There are a number of routes to report crime if you wish to do so alongside reporting suspicions/ knowledge of money laundering/terrorist financing to the UKFIU:

If you have information on serious and organised crime that you would like to provide to the NCA, but which does not meet the criteria for a SAR, you can use the NCA's public reporting tool available on the NCA website.

Action Fraud

Information regarding how to report fraud related offences to Action Fraud can be found via https://www.actionfraud.police.uk/

Charity Commission

You can report a concern about a registered charity to the Charity Commission for:

England and Wales via https://forms.charitycommission.gov.uk/raising-concerns

Scotland via https://www.oscr.org.uk/raise-a-concern

Northern Ireland via www.charitycommissionni.org.uk/concerns-and-decisions/concerns-about-charities-guidance

Child Exploitation and Online Protection (CEOP)

Information regarding Child Exploitation and Online Protection (CEOP) can be found via https://www.ceop.police.uk/Safety-Centre/

Department for Work and Pensions (DWP)

Information regarding how to report benefit fraud to DWP can be found via https://www.gov.uk/report-benefit-fraud

HM Revenue and Customs (HMRC)

Information regarding how to report business or personal tax fraud to HMRC can be found via https://www.gov.uk/report-tax-fraud

Home Office

Information regarding how to report fraud related to immigration crime (or any other immigration crime) can be found via https://www.gov.uk/report-immigration-crime

Internet Watch Foundation

Information regarding how to report illegal content online report can be found via http://www.iwf.org.uk/

Local Police Force

If you suspect Child Sexual Abuse Material (CSAM) has been sold, distributed or purchased report this to your local Police Force.

If you suspect Child Sexual Exploitation (CSE), report this to your local Police Force.

Office of Financial Sanctions Implementation (OFSI)

Information regarding how to report sanctions related breaches can be found via https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do

Office of the Public Guardian (OPG)

Information regarding how to report a concern about an attorney, deputy or guardian (such as abuse of a power of attorney) can be found via

https://www.gov.uk/report-concern-about-attorney-deputy-guardian

Terrorist Financing and Terrorist relating reporting routes

Report online material promoting terrorism or extremism via https://www.gov.uk/report-terrorism

Tell the Metropolitan Police about possible terrorist activity via https://www.met.police.uk/tua/tell-us-about/ath/possible-terrorist-activity/

Making a referral to Prevent via https://www.gov.uk/guidance/making-a-referral-to-prevent

Important:

This isn't an exhaustive list of alternative reporting routes. There may be other reporting routes you need to consider. If you are unsure, please contact your regulator.

Versions

Version	Date published
1.0	November 2025

UKFIU
UK Financial Intelligence Unit

Key Resources and Contacts

To access other UKFIU guidance documents and SAR related products, see the NCA website **here**

If you have any feedback in relation to this guidance document, please contact **UKFIUEngagement@nca.gov.uk**

Scan the QR code to access all issues of UKFIU SARs In Action magazine

Follow us on X **@NCA_UKFIU**

Follow us on LinkedIn - **UK Financial Intelligence Unit (UKFIU)**