



**UKFIU**  
UK Financial Intelligence Unit



**NCA**  
National Crime Agency

# **Suspicious Activity Report (SAR) Glossary Codes and Reporting Routes**

United Kingdom Financial Intelligence Unit (UKFIU)

## **PLEASE NOTE:**

This booklet replaces all previous glossary codes publications.

**April 2023 (V3.0)**

## Overview

The purpose of this booklet is to provide guidance on the use of Suspicious Activity Report (SAR) glossary codes and reporting routes.

## Key points

1. The **use of glossary codes is considered good practice**. They are crucial for enabling the UK Financial Intelligence Unit (UKFIU) and wider law enforcement to conduct analysis to identify money laundering trends, high risk cases for development and take immediate action where necessary. They also enable the production of feedback to reporters on trends and patterns identified in SARs.
2. The SARs regime is **not a route to report crime or matters relating to immediate risks to others**. The SARs regime is for reporting knowledge or suspicions of money laundering, or belief or suspicions relating to terrorist financing. As such, in addition to a SAR, you may have to report the matter via other routes to ensure the right information gets to the right organisation. Where you do report a crime alongside a SAR it will be good practice to include the crime reference and the organisation details in the SAR.
3. When submitting a SAR, the relevant glossary code should be **included in the 'Reason for Suspicion' text space** (see SAR examples pages 21-27).
4. It is acceptable to have a SAR with **several codes** (see example 6, page 27). If in doubt as to whether a particular code applies, always work on the basis that it is better to include one than not. When using **multiple codes** in a SAR, ensure you include a space between each code. It is also **possible** that a code does not match the set of circumstances faced by the reporter so in some cases it is acceptable that "**no codes apply**" be populated into the 'Reason for Suspicion' text space.

## Contents of booklet

- **Walkthrough checklist** (step by step guide, pages 3-6)
- **Detail on codes** (definitions and context, pages 7-18)
- **Alphabetical list** (menu of key themes signposting where they are in this guidance, page 19-20)
- **Examples** (location for codes and good practice tips, pages 21-27)
- **Aide memoire** (annex overview of all the codes, page 28-29 – *reporters may find it useful to have this summary available when inputting SARs*)

## Walk-through checklist

### Step 1: Do the circumstances require immediate attention?

Priority is given to SARs indicating high risk victims of crime (such as children and vulnerable adults) and requests for a defence against money laundering (DAML) and terrorist financing.

- Do you require a **defence under POCA<sup>1</sup>** ('consent')? Use code XXS99XX and if submitting via SAR Online tick the 'consent' box. Also use the code XXGVTXX if the suspected money laundering is of a value of £3,000 or less (see page 7). The code XXGVTXX should not be used if the reporter is aware of any law enforcement agency or terrorist financing interest. For **requests for a defence under TACT<sup>2</sup>** submit under 'Terrorism' and tick the consent box (see example 1b, page 22).
- Does the money laundering/terrorist financing relate to a **vulnerable person at risk of immediate harm**? Call the police on 999. To report a fraud, do so via Action Fraud [see pages 13-14] or report other crime by ringing 101. Include code XXV2XX in any SAR relating to money laundering/terrorist financing concerning vulnerable people (see page 14 and example 3, page 24).
- Does the money laundering/terrorist financing relate to a **child at immediate risk of harm, including sexual abuse and exploitation**? Call the police on 999. If a non-emergency crime has occurred ring 101. Include code XXV3XX in any SAR relating to money laundering/terrorist financing concerning child exploitation. Additionally consider other reporting routes (see page 14-15 CEOP and example 2, page 23).
- Do you suspect **modern slavery/human trafficking**? If there is an immediate risk of harm call the police on 999. (See pages 17-18 and example 6, page 27).

### Step 2: Other factors to consider

- Do the circumstances involve professionals or **others in the financial sector** who are providing a service which is potentially wittingly or unwittingly enabling money laundering? Use code XXPRFXX (see page 7 and example 5, page 26).
- Are there indicators of **trade-based money laundering<sup>3</sup>**? Use code XXTBMLXX (see pages 8-9).
- Is the laundering connected with the **purchase, sale or rental of real estate property (e.g. dwelling house, factory building or office premises)**? Use code XXPROPXX (see page 9 and example 4, page 25).

<sup>1</sup> Proceeds of Crime Act 2002.

<sup>2</sup> Terrorism Act 2000.

<sup>3</sup> Trade based money laundering has been defined by the Financial Action Task Force (FATF) as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins."

- Do your suspicions/knowledge relate to **politically exposed person/s (PEPs)**? For international PEPs use code XXD7XX; for UK domestic PEPs use code XXD8XX (see page 15-16).
- Does it relate to **proceeds of bribery and corruption**? Use code XXD9XX (see page 15).

### **Step 3: Does the laundering relate to specific predicate economic crime offences? (See page 13)**

- Does the laundering relate to **tax evasion offshore** (code XXTEOSXX) or does it relate to **UK-based tax evasion** (code XXTEUKXX)?
- Does the laundering relate to tax evasion by a **corporation/business or an individual**? Use codes XXF3XX and XXF4XX respectively.
- Does the laundering relate to **benefit fraud** or **excise evasion**? Use codes XXF1XX and XXF2XX respectively.
- Does the laundering relate to **VAT fraud**? This could include carousel/missing trader intra-community (MTIC) fraud. Use code XXF5XX.
- Does the laundering relate to **fraud against the private sector**? Report to Action Fraud. Use code XXF9XX in any SAR relating to laundering/terrorist financing.

### **Step 4: Is the laundering linked to sanctioned entities? (See pages 11-12)**

- The identification of sanctioned entities, or linked non-sanctioned entities, may be made by the reporter and form part of the reasons for submission when submitting a SAR.
- In March 2022 the UKFIU introduced a new SARs glossary code for entities associated to sanctioned individuals and companies on the sanctions list.
- Use the code **XXSNEXX** where you suspect the activity is consistent with money laundering and is linked to entities sanctioned by the UK, US, EU and other overseas jurisdictions.

## **Step 5: Do the circumstances relate to other predicate offences?**

- Relate to the supply of firearms? If there is an immediate risk of harm **ring the police on 999**. Report non-emergency offences via 101. Use code XXFIREXX in any SAR relating to money laundering/terrorist financing.
- Links to **organised immigration crime, modern slavery and human trafficking**? If you suspect modern slavery is taking place call 999 in an emergency; 101 for non-emergencies. Alternatively contact the Modern Slavery Helpline – 0800 0121 700 for advice.

For further information about the work of the Modern Slavery Helpline go to <https://www.modernslaveryhelpline.org/>

Report non-emergency organised immigration crime offences via 101 or via the Home Office <https://www.gov.uk/report-immigration-crime>

- Use codes XXOICXX and/or XXMSHTXX in any SAR relating to money laundering/terrorist financing which involves organised immigration crime or modern slavery/human trafficking (see pages 17-18 and example 6, page 27).
- Links to the **supply of illegal drugs**? Report non-emergency offences via 101. Use code XXDRUXX in any SAR relating to money laundering/terrorist financing.

## **Step 6: Does it relate to a specialist initiative?**

- Is it a **counter-proliferation report**? This relates to counter proliferation financing (counter-proliferation refers to diplomatic and military effort to combat the rapid increase of weapons). Use code XXPCPXX.

## **Step 7: Should I still use an NCA Alert reference?**

SAR glossary codes are different to NCA Alert references. NCA Alerts are warnings produced by the NCA for the wider community in order to also reach beyond the SAR regulated sector. They can be used to inform a range of business, financial institutions and industry about serious organised crime and its effects, but can simultaneously be related to money laundering.

The Alerts process is a recognised and established way by which 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 or a glossary code. If you submit a SAR as a result of the information contained in an Alert please include the keyword within the free text field.

As such, an NCA Alert reference is specific to whichever Alert it pertains to. The Alert reference should be included in the body of your SAR 'Reason for Suspicion' text if money laundering is suspected.

SAR glossary codes are always prefixed and suffixed with 'XX', whereas Alert codes follow the format of 'xxxx-AAAA' (with 'x' being numbers and A being letters). To note: previous NCA Alerts did use 'FF' or 'AA' as part of their codes. If appropriate, the NCA Alert code should be used **in addition to** the relevant SAR glossary code/s in the body of your SAR text.

## **Step 8: Victim refunds**

Are you intending on returning money to the victim of crime? The UKFIU view is that a DAML is unnecessary if the reporter's position is that they are returning money to a victim of crime and that they will not be carrying out activity which falls within Sections 327-8 of POCA. The submission of a DAML is therefore entirely the decision of the reporter. If you have a suspicion of money laundering you are obliged to complete a SAR. Use code XXVICTXX for any cases where the reporter is submitting a SAR and considers that the purpose of the activity in question is to return money to a victim of crime. In any case where you suspect a criminal offence other than money laundering we advise you to report the activity to your local police force in the normal way.

## Detail on glossary codes

### **XXGVTXX – Requiring a defence under POCA ('consent') if the value of the suspected money laundering falls below a value of £3,000**

Use code XXGVTXX in any SAR relating to suspected money laundering where the activity value is £3,000 or less and you are unaware of any law enforcement or terrorist financing interest at the time of reporting.

Law enforcement interest does not have to be confirmed and could for example be an article that has appeared in the press or on social media as well as an awareness of a previous interest.

In addition, the victim code XXVICTXX should not be used concurrently with the XXGVTXX code. If the majority of funds are less than £3,000 and being returned to a victim of crime, please only use the victim code.

The UKFIU is committed to ensuring a risk-based and consistent approach to decision making and operates a triage system for DAMLs in date order. The introduction of this code is to assist with the triage processes and the early identification of key-risk areas and asset recovery opportunities.

### **XXPRFXX – Professional enablers: persons providing professional services or specialist knowledge that wittingly or unwittingly facilitates money laundering.**

The laundering of criminal proceeds is sometimes reliant on access to the professional skills of, among others, lawyers, accountants, investment bankers and company formation agents. Professional enablers can also be highly organised criminals who develop products and services specifically to facilitate criminal enterprises. The use of professional enablers increases the complexity of money laundering activities, for example with the setting up of shell companies, trusts and other instruments providing anonymity.

The 2015 National Risk Assessment (NRA) describes professional enablers as those persons having the skills and/or knowledge to (wittingly or unwittingly) assist criminals in laundering the proceeds of crime.

Professionals can effectively act as private banks to individual clients. Client accounts offer criminals relative anonymity, the ability to obscure the origins and beneficiaries of criminal proceeds, and the perceived protection of legal privilege. The hallmarks of money laundering facilitated by professional service providers are very visible in trust and company formation, conveyancing and client account services environment.

The SAR should clearly state how a professional enabler was used. An explanation of why a subject is considered a professional enabler should be included in the SAR. See example 5, page 26.

## XXTBMLXX – Trade-based money laundering (TBML)

The Financial Action Task Force (FATF) defines TBML as “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins”.<sup>4</sup> At its core, it relates to the use of the international trade system to obscure the origin of illicitly obtained funds.

The UK Joint Money Laundering Intelligence Taskforce (JMLIT) Trade Based Expert Group suggests that criminals will commonly utilise the following two defined techniques to achieve this aim: (1) the abuse of trade finance products and (2) the abuse of commercial client open account payments.

The SAR should explicitly state TBML in the intelligence provided. An explanation of what specific actions the subject has performed to warrant a suspicion of TBML should be included in the SAR.

### **Trade finance based money laundering – the abuse of trade finance products**

Trade finance can, in its broadest interpretation, be described as being the finance and/or facilitation of the trade related payment by financial institutions relating to the movement of goods and services between two points, both domestically and cross border. The standard products used are Documentary Letters of Credit (LCs) and Documentary Bills for Collection (BCs). These standard products have trade related documents (invoices, transport document etc.) that are sent through financial institutions and are examined by the financial institutions for consistency with the terms of the trade transaction. Both these products are governed internationally by sets of rules and practice issued under the auspices of the International Chamber of Commerce. Approximately 10% of global trade is done in this way using trade finance products.

It is the discrepancies found in the verification checks of the trade related documents that often reveal strong indicators of criminal abuse of the trade activities.

### **Trade based money laundering – the abuse of commercial client Open Account payments**

More commonly, world trade is conducted on ‘Open Account’ terms, whereby a ‘clean’ payment is made by the buyer of the goods or services direct to the seller, i.e. without presentation of the supporting trade documentation to the financial institution through which the payment is affected.

Open Account trade involves the movement of goods or services between two companies, either domestically or internationally, based on mutual trust. In Open Account transactions, unlike transactions where trade finance products are used, the bank is only aware of, and in receipt of, the instruction to effect payment and will not be aware of the underlying reason for the payment.

<sup>4</sup> FATF, Trade Based Money Laundering, June 2006.

In a typical Open Account transaction, the seller and buyer contract for the delivery of stated goods from the seller to a place designated by the buyer. Banks involved in handling a payment related to an Open Account trade transaction generally do so in one (or both) of two capacities:

- a) the seller or buyer is their commercial customer
- b) the seller or buyer is the commercial customer of the bank's correspondent banking customer.

Banks handling trade-related payments will be able to perform the basic screening and monitoring related to payments transactions, but they will not, given the absence of availability of underlying transactional information, generally be in a position to otherwise discern suspicious activity.

Open payment methods can facilitate:

- using criminal cash/stockpile to fund a trade payment on behalf of a **third party (goods do not become criminal property)**
- paying for goods to move value directly across borders (goods become criminal value)
- paying for and moving goods through multiple companies/jurisdictions to:
  - disguise origin of funds
  - disguise criminal profits
  - provide reason for wealth/profit at destination
- manipulating the value of goods to move value across borders.

#### **XXPROPXX – Purchase, sale and rental of real estate property**

Purchasing, selling and renting real estate property as a method of money laundering provides the criminal with the opportunity to clean large amounts of illicit funds in a single transaction. It is likely that a significant proportion of criminals purchase or sell property through estate agents to launder the proceeds of crime. Other professionals, in particular solicitors and conveyancers, are likely to be unwittingly or unwittingly involved.

Real estate property could include dwelling houses, apartments or flats, commercial buildings such as office or factory premises. It can also include investments in property developments that build dwelling or commercial premises.

## **XXVAXX - Virtual assets**

The FATF defines virtual assets as digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account and/or a store of value.<sup>5</sup> The UKFIU is using the term virtual assets in line with changes to the FATF Recommendations and the FATF Glossary that have added new definitions of “virtual assets” and “virtual asset service providers”. It is the more all-encompassing term since it includes virtual currencies, cryptocurrencies and digital currencies, but also covers the fact that anything can be tokenised as an asset and transferred on a blockchain or other digital peer-to-peer format.

Offering a secure, anonymous method of transferring value, with global reach, fast transaction times and low fees, virtual assets provide a powerful tool for criminals to move and store illicit funds. While they have the potential to spur financial innovation, efficiency and improve financial inclusion, they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities.

The main criminal use of virtual assets is as a method of payment for illicit commodities and services, particularly on the dark web. On the whole, SARs on virtual assets link to fraud, dark web market places and suspicions surrounding unusual third party payments swiftly transferred to exchanges.

The role virtual assets are increasingly playing in money laundering, the investigative challenges associated with tracing illicit virtual asset transactions and the lack of regulation all continue to pose considerable risks. The scale of value laundered through virtual assets is unknown, and while it is assessed to be relatively low compared to other methods, it is expected to increase as new types of virtual assets continue to emerge and their use becomes more widespread.

**Please note that the use of virtual assets/virtual currencies/ cryptocurrencies/digital currencies is not illegal. This code relates to where there is a suspicion that virtual assets are being used to facilitate money laundering. The visibility of virtual assets in isolation should not automatically suggest that a SAR is required.**

<sup>5</sup> FATF, Regulation of virtual assets’, 19 October 2018

## **XXMLTMXX – Money laundering through markets**

In May 2021 the UKFIU introduced a new SAR glossary code for money laundering through markets (MLTM). MLTM in its simplest terms is money laundering taking place within capital markets in which shares, derivatives, bonds and other instruments are bought and sold.

The glossary code should not be used for market abuse such as insider trading or market manipulation unless specific reference is made to the subsequent laundering of the proceeds of these crimes.

MLTM activity has serious implications for the reputation of the UK as a global financial centre and, in addition, any firm found to be facilitating this type of money laundering could be liable to prosecution and/or damaging regulatory fines.

There is a collectively-held recognition across law enforcement, regulators and reporters that there are significant intelligence gaps relating to the scale of illicit finance generated in the UK and overseas but whose MLTM impacts the UK specifically.

## **XXSNEXX – Money laundering linked to sanctioned entities**

The NCA has received requests from reporters for a defence against money laundering, concerning entities sanctioned by the UK, US, EU and other overseas jurisdictions.

The Defence Against Money Laundering (DAML) and Defence Against Terrorist Financing (DATF) regime is distinct from the Sanctions regime. Where DAML and DATF interact with the Sanctions regime is when sanctioned entities, and by extension persons not sanctioned but linked to sanction entities, are referred to in DAMLs and DATFs submitted by SAR reporters.

Where DAMLs are submitted, it is for the purpose of reporting a suspicion of money laundering or criminal property; where DATFs are submitted it is for the purpose of reporting terrorist financing. They are not for the purpose of reporting a suspicion of a sanction breach.

The identification of sanctioned entities, or linked non-sanctioned entities, may be made by the reporter and form part of the reasons for submission when submitting a SAR. The NCA cannot tell the reporter what to report within the SAR submission.

In March 2022 the UKFIU introduced a new SARs glossary code for entities associated to sanctioned individuals and companies on the sanctions list.

Use the code **XXSNEXX** where you suspect the activity is consistent with money laundering and is linked to entities sanctioned by the UK, US, EU and other overseas jurisdictions.

**To note:** the filing of a SAR does not absolve you of your responsibilities to contact the Office of Financial Sanctions Implementation (OFSI) for a license to move the funds for a sanctioned entity or sanctioned individual.

## **COVID-19**

In April 2020 the UKFIU implemented three new SAR glossary codes for reporters as a result of the increased threat posed by organised crime groups (OCGs) seeking to exploit the COVID-19 situation by means of fraud.

### **XXSATXX – HMRC Self-Assessment Tax Refund system**

Whilst the Self-Assessment Tax Refund system was introduced by HM Revenue & Customs (HMRC) prior to COVID-19 there is the potential for it to be exploited in the current climate. Use code XXSATXX in any SAR relating to suspected fraudulent use of the Self-Assessment Tax Refunds system. This may relate to identifying a change in pattern or behavior in accounts which could suggest fraudulent activity.

### **XXGPSXX – Government Priority Schemes**

The government introduced a number of schemes to offer support to businesses/individuals during the outbreak. Reporters should be alert to the potential for these schemes to be exploited by OCGs to commit fraud. Use code XXGPSXX in any SAR relating to suspected fraudulent use of Government Priority Schemes established as a result of COVID-19. This may relate to identifying a change in pattern or behavior in accounts which could suggest suspicious activity.

### **XXCVDXX – General code**

The UKFIU is conducting specific analysis to inform partners of observations on what is being seen in reporting around COVID-19 and SARs. It would assist UKFIU analysis if reporters also used the code XXCVDXX in any SAR relating to suspicious activity connected to COVID-19.

- XXCVDXX should be used for **all** suspicious activity related to COVID-19.
- XXGPSXX or XXSATXX should ONLY be used if the suspicious activity relates to COVID-19.
- For any SAR relating to the suspected fraudulent use of the Government Priority Scheme, XXCVDXX should be used alongside the glossary code for this scheme e.g. XXCVDXX and XXGPSXX.
- For any SAR relating to any suspected fraudulent use of the HMRC Self-Assessment Tax Refund system, XXCVDXX should be used alongside the glossary code for this scheme e.g. XXCVDXX and XXSATXX.

**Glossary codes XXGPSXX and XXSATXX should not be used without the XXCVDXX code.**

If the circumstances have no connection to COVID-19 but there are suspicions relating to the abuse of the Self-Assessment Tax Refund system or the Government Priority Schemes please consider using other relevant glossary codes e.g. the tax evasion codes (offshore or UK based) instead.

**Predicate offences - economic crime**

Fraud and tax offences are the largest known source of criminal proceeds from offending in the UK and involve a variety of crime types, victims, and perpetrators.

If you are reporting suspicions/knowledge of money laundering or terrorist financing concerning the below predicate offence please use the appropriate code from the table below in the SAR.

<b>XXTEOSXX</b>	Tax evasion offshore
<b>XXTEUKXX</b>	Tax evasion UK-based
<b>XXF1XX</b>	Proceeds from benefit fraud
<b>XXF2XX</b>	Excise evasion (duty on alcohol, tobacco, fuel etc.)
<b>XXF3XX</b>	Corporate tax evasion (tax evasion by businesses, corporations)
<b>XXF4XX</b>	Personal tax evasion (tax evasion by individuals e.g. income tax)
<b>XXF5XX</b>	VAT fraud e.g. carousel – Missing Trader Intra-Community (MTIC) fraud
<b>XXF9XX</b>	Frauds against private sector
<b>XXD9XX</b>	Bribery and corruption

**Fraud reporting alongside this:**

When you encounter a fraud (or attempted fraud) you will have to consider whether you want to report a crime **alongside** any responsibilities you have to report suspicions/knowledge of money laundering and terrorist financing to the NCA via a SAR. If the funds involved are not yet the proceeds of crime then it is not money laundering, but attempted fraud.

**You cannot report a crime to the NCA.**

There are a number of routes to report fraud-related offences if you wish to do so alongside reporting suspicions/knowledge of money laundering/terrorist financing to the NCA. The main route is via the national fraud and cyber-crime reporting centre, Action Fraud, which is run by City of London Police and works alongside the National Fraud Intelligence Bureau.

## **Action Fraud**

- Report online via <https://www.actionfraud.police.uk> or **or call 0300 123 2040 (Monday – Friday, 8am – 8pm)**
- If you are calling from outside the UK please call **+44 300 123 2040**

However, if you wish to report business or personal tax fraud you should do so to HM Revenue & Customs via <https://www.gov.uk/government/organisations/hm-revenue-customs/contact/report-fraud-to-hmrc> or call **0800 788 887 (Monday to Friday: 9am to 5pm)**. If you are calling from outside the UK **+44 203 080 0871**.

Additionally, to report a benefit fraud, do so to the Department for Work & Pensions via [Report benefit fraud - GOV.UK \(www.gov.uk\)](#)

To report a fraud related to immigration crime (or any other immigration crime) do so to the Home Office via <https://www.gov.uk/report-immigration-crime>

## **Vulnerable persons**

### **XXV2XX – Risk to vulnerable adults**

#### **If you think a vulnerable adult is at immediate risk call 999.**

A vulnerable adult is any person aged 18 years or over who is or may be in need of community services by reason of mental, physical, or learning disability, age or illness AND is or may be unable to take care of themselves or unable to protect themselves against significant harm or exploitation.<sup>6</sup> Risks to vulnerable adults include (but is not limited to) sexual and other physical abuse, financial abuse (including fraud), and they may be the victims of modern slavery.

If you are reporting suspicions/knowledge of money laundering or terrorist financing concerning a vulnerable person include the XXV2XX glossary code in any SAR (see example 3, page 24).

#### **Alongside this:**

If you also wish to report a fraud contact Action Fraud. For another non-emergency crime contact your local police force via 101. If you wish to report a vulnerable adult (or child) who is a victim of modern slavery ring 101 or the Modern Slavery Helpline telephone number 0800 0121 700 or seek advice at <https://www.modernslaveryhelpline.org/report>

<sup>6</sup> Association of Chief Police Officers (ACPO), Safeguarding and Investigating the Abuse of Vulnerable Adults.

## **XXV3XX – Risk to children – particularly including sexual abuse and exploitation**

### **If you think a child is at immediate risk call 999.**

A child is regarded as someone under 18 years of age. A child is always considered to be vulnerable, irrespective of the adult vulnerability criteria. A child may show mental, physical or learning disabilities or show illness, but this should be considered as an additional reporting factor reinforcing the child's inability to protect themselves against significant harm or exploitation. If you are reporting suspicions/knowledge of money laundering or terrorist financing relating to risk to children, include the code XXV3XX in any SAR (see example 2, page 23).

### **Alongside this:**

If you wish to report the abuse of a child please follow the guidance at  
<https://www.gov.uk/report-child-abuse>

If you want to report suspicious behaviour online with or towards a child, use the Child Exploitation & Online Protection (CEOP) Centre online report form

(<https://www.ceop.police.uk/ceop-reporting/>)

CEOP Centre enquiries: 0370 496 7622 (24/7 telephone)

If you want to report illegal content online report to the Internet Watch Foundation (<http://www.iwf.org.uk/>)

## **XXD9XX – Bribery and corruption**

The UK Anti-Corruption Strategy 2017-2022 states that "there is no universally accepted definition of corruption, but it is generally understood to involve the abuse of office and position to benefit a third party (an individual, business or other organisation), in return for payment or other reward. These features are captured in Transparency International's definition: 'the misuse of entrusted power for personal gain'".

In view of the public profile of persons in a prominent public function it is likely that they would wish to avail themselves of a sophisticated smokescreen to conceal their corrupt illicit corrupt gains. Bribery and corruption therefore have significant links to money laundering. The individual does not have to have a public facing role for them to commit bribery and corruption.

## **Politically exposed persons (PEPs)**

The 2015 NRA defined PEPs as:

International PEP: a term describing someone who has been entrusted with a prominent public function in a state other than the UK in the preceding year, or a

relative or known associate of that person. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

The 2020 NRA states that the UK remains a prime destination for foreign corrupt PEPs to invest in.

In February 2012 FATF defined PEPs as:

**International (Foreign) PEPs:** individuals who are or have been entrusted with prominent public functions by a foreign country, for example heads of state or heads of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

**Domestic PEPs:** individuals who are or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

**International PEP** – glossary code to be used **XXD7XX**

**Domestic PEPs** – glossary code to be used **XXD8XX**

### **XXILTXX – Illegal lotteries**

In simple terms a lottery is gambling that has three elements: payment to participate; prizes awarded; and prizes awarded by way of chance.

It is an offence under the Gambling Act 2005 to facilitate or promote a lottery unless the operator holds an operating licence. The profits from an illegal lottery may also be considered criminal property under POCA and therefore the operator may have committed a money laundering offence. It is not an offence to participate in an illegal lottery.

The Gambling Commission has seen that the majority of illegal lotteries are promoted via social media sites.

#### **Action required**

If you suspect money laundering is taking place as a result of illegal lotteries please briefly describe the activity taking place in your SAR.

If social media is being used to promote or facilitate the lottery please identify clearly which platform is being used e.g. Facebook, Instagram, Twitter etc.

To assist analysis, please include additional information such as: identified

weblinks; whether the subject of the SAR is an organiser or user of the lottery; and turnover of the account for the last 12 months.

Do the accounts have a large turnover of small amounts that are inconsistent with the profile of the customer? Do larger payments make reference to terms like "prize" or "Congratulations!"? Are there multiple credits and debits to third parties who don't live close to the account holder?

Please confirm if there are any red flags visible e.g. type of prizes or words used like "Congrats", "prize", "thunderball", "tb", "entry", "raffle", "bonus ball", "bb", etc.

Please include details of what your next steps will be e.g. are you intending to exit the relationship, are you conducting further due diligence etc.?

## **Priority crime types**

The National Strategic Assessment (NSA) of Serious and Organised Crime 2021 provides a single picture of the threat to the UK from serious and organised crime. The threats, which can be cross-cutting, are grouped into: Vulnerabilities – child sexual abuse and exploitation (CSAE); organised immigration crime (OIC); and modern slavery and human trafficking (MSHT). Prosperity – money laundering; fraud and other economic crime; bribery, international corruption and sanctions evasion; and cyber crime. Commodities – firearms and drugs.

Some of the priority crime types are featured in their own sections in this glossary codes document.

**If you think there is an immediate urgent risk to public safety call 999.**

### **XXFIREXX – Firearms**

The NSA illustrates that handguns and shotguns are the most commonly used criminal firearms in the UK, with automatic weapons on the rise, albeit from a low level. If you are reporting suspicions/knowledge of money laundering or terrorist financing relating to firearm criminality include the code XXFIREXX in any SAR.

### **XXDRUXX – Illegal supply of drugs**

The NSA illustrates that demand for all common drug types remains high in the UK. It is likely that the UK drugs market and the associated crime will continue to grow and cause increased harm to the UK. If you are reporting suspicions/knowledge of money laundering or terrorist financing relating to drugs include the code XXDRUXX in any SAR.

### **XXOICXX – Organised immigration crime**

The NSA identifies the risks of serious and organised criminals enabling migrants to

enter the UK clandestinely. The unlawful activities of such criminal networks to avoid UK border controls are known as organised immigration crime.

### **XXMSHTXX – Modern slavery/human trafficking**

The term ‘modern slavery’ includes the offences of human trafficking, forced labour and debt bondage.

**Human trafficking** – involves transporting, recruiting or harbouring people for the purpose of exploitation, using violence, threats or coercion.

**Forced labour** – any work or services which people are forced to do against their will normally under the threat of some form of punishment.

**Debt bondage** – when people borrow money they cannot repay and are required to work to pay off the debt, then losing control over the conditions of both their employment and the debt.

A victim of MSHT should always be considered to be a vulnerable person so in all MSHT-related SARs it is also normal to additionally include the vulnerable person code (for adults XXV2XX, for child victims [under 18] XXV3XX).

### **The difference between OIC and MSHT**

It is possible for OIC to not involve modern slavery where the intention is purely to enter the UK clandestinely and the crime committed is only against the state.

It is also possible for modern slavery not to involve OIC where the victims are legally in the UK but are then transported for the purpose of exploitation. Here the crime is against the person.

If you are reporting suspicion/knowledge of money laundering or terrorist financing with a belief that the circumstances involve clandestine entry into the UK, and is not MSHT, then you should use XXOICXX.

If you are reporting suspicion/knowledge of money laundering or terrorist financing with a belief that the circumstances involve MSHT and not clandestine entry to the UK then you should use XXMSHTXX e.g. the MSHT victims seem to be legally in the UK.

### **Use of both codes XXOICXX and XXMSHTXX**

The NSA states that serious organised crime threats such as OIC and MSHT are increasingly interlinked. There are significant overlaps between MSHT and OIC, with offenders often moving seamlessly between both of these crime threats.

Consequently OIC and MSHT SARs are often connected so it is acceptable to use both codes together. Always ensure you include a space between each code when using multiple codes in a SAR (see example 6, page 27 on the use of multiple codes).

### **Alongside using these codes in SARs**

If you also wish to report a non-emergency crime relating to firearms, OIC, MSHT or drugs contact your local police force via 101.

## Alphabetical reference list of contents

<b>A</b>	Adult vulnerable person – pages 3, 14 (see example 3, page 24) Alert codes from the NCA – page 5-6
<b>B</b>	Benefit fraud – page 4, 13-14 Bribery – page 15
<b>C</b>	Carousel fraud (see MTIC) – page 13 Child exploitation – pages 3, 15 (see example 2, page 23) Consent – pages 3, 7 (see example 1, page 21) Corruption – page 15 (see PEPs, pages 15-16) Counter proliferation – page 5 COVID-19 – page 12-13
<b>D</b>	Drugs (illegal supply of drugs) – pages 5, 17
<b>E</b>	Excise evasion – page 13
<b>F</b>	Firearms – page 17
<b>G</b>	Government priority schemes – page 12
<b>H</b>	Human trafficking – pages 5, 17-18 (OIC pages 17-18; modern slavery pages 17-18) HMRC Self-Assessment Tax Refund system – page 12
<b>I</b>	Illegal lotteries – page 16 Immigration crime (see OIC) – pages 17-18
<b>M</b>	Modern slavery – pages 5, 17-18 Money laundering – pages 7-10 Money laundering through markets – page 11 MTIC (Missing Trader Intra Community) fraud (carousel fraud) – page 13
<b>N</b>	NCA Alert codes – pages 5-6
<b>O</b>	Offshore tax evasion – page 13 Organised immigration crime (OIC) – pages 17-18 (cross refer with modern slavery human trafficking [MSHT])
<b>P</b>	Politically exposed persons (PEPs) – pages 4, 15-16 Professional enabler – pages 3, 7 (see example 5, page 26) Projects – page 29 Property market – pages 3-4, 9 (see example 4, page 25)

<b>R</b>	Real estate (cross refer [property market page 9])
<b>S</b>	Sanctions – pages 4, 11-12
<b>T</b>	Tax evasion – pages 4, 13 Trade based money laundering – pages 8-9
<b>U</b>	UK tax evasion – page 13
<b>V</b>	Vulnerable persons – pages 3, 14 (see example 3, page 24) (child exploitation pages) (cross refer with modern slavery, human trafficking) VAT fraud (MTIC) (carousel fraud) – page 13 Victim refunds – page 6 Virtual assets – page 10

## **Glossary code example 1a) – requesting a defence from the NCA relating to money laundering**

### **SAR Online view**

**REASON/SUBMIT**

#### **What is your Reason for Suspicion/Knowledge?**

*Insert **glossary code(s) here** at the start of reason for suspicion.*



**Example 1a): code and content – requesting a defence from the NCA relating to Money Laundering ('consent' SAR)**

"XXS99XX This SAR seeks a defence to a money laundering offence in relation to our suspicion of money laundering. The circumstances are..."

#### **Good practice tips – always:**

- identify as clearly as possible the suspected benefit from criminal conduct (the 'criminal property') including, where possible, the amount of benefit
- identify the reason(s) for suspecting that property is criminal property
- identify the proposed prohibited act/s you seek to undertake involving the criminal property
- identify the other party/parties involved in dealing with the criminal property, including their dates of birth (DOB) and addresses where appropriate (such information should be held routinely by reporters in the regulated sector to comply with the requirements of the Money Laundering Regulations)

For further guidance relating to requests for a defence to a money laundering offence please refer to the document 'Requesting a defence from the NCA', published on the NCA website [www.nationalcrimeagency.gov.uk](http://www.nationalcrimeagency.gov.uk)



## **Glossary code example 1b) – requesting a defence from the NCA relating to terrorist finance**

### **SAR Online view**

*Insert **glossary code(s) here** at the start of reason for suspicion.*



#### ***Example 1b): code and content – requesting a defence from the NCA relating to Terrorist Finance ('consent' SAR)***

“ This SAR seeks a defence to a terrorist finance offence in relation to our suspicion of terrorist financing. The circumstances are...”

#### **Good practice tips – always:**

- identify as clearly as possible the suspected terrorist property including, where possible, the value and whereabouts of the property
- identify the reason(s) for suspecting that property is terrorist property
- identify the proposed prohibited act/s you seek to undertake involving the terrorist property
- identify the other party/parties involved in dealing with the terrorist property, including their dates of birth (DOB) and addresses where appropriate (such information should be held routinely by reporters in the regulated sector to comply with the requirements of the Money Laundering Regulations)

For further guidance relating to requests for a defence to a terrorist finance offence please refer to the document ‘Requesting a defence from the NCA’, published on the NCA website [www.nationalcrimeagency.gov.uk](http://www.nationalcrimeagency.gov.uk)



## **Glossary code example 2 – risk to children**

### **SAR Online view**

**REASON/SUBMIT**

#### **What is your Reason for Suspicion/Knowledge?**

*Insert glossary code(s) here at the start of reason for suspicion.*



#### ***Example 2: code and content – risk to children (person under 18 years of age)***

"XXV3XX This SAR concerns a child we believe is being exploited. The circumstances are that the person is 15 years old ....."

#### **Good practice tips – always :**

- describe fully the reasons for suspicion in relation to the money laundering. As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How?
- describe fully all personal information concerning the child – full name, DOB, address and post code, nationality.
- describe if law enforcement are already aware of the circumstances, in particular the exploitation of the child. Confirm if contact has been made with CEOP (CEOP ref number) (officer contacted).
- describe fully if any additional vulnerabilities exist e.g. if the child is unable to properly protect him/herself against exploitation due to what appears to be mental, physical or learning disability, or illness related condition.



## **Glossary code example 3 – risk to vulnerable adult**

### **SAR Online view**

**REASON/SUBMIT**

#### **What is your Reason for Suspicion/Knowledge?**

*Insert **glossary code(s)** here at the start of reason for suspicion.*



#### ***Example 3: code and content – risk to vulnerable adult (person over 18 years of age)***

"XXV2XX This SAR concerns a person we believe is a vulnerable adult. The circumstances are that ....."

#### **Good practice tips – always :**

- describe fully the reasons for suspicion in relation to the money laundering. As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How?
- describe fully all personal information concerning the adult – full name, DOB, address and post code, nationality.
- describe if law enforcement or social services are already aware of the circumstances (include any ref number) (persons contacted).
- describe fully the vulnerabilities you believe suggest the person cannot protect him/herself against exploitation e.g. do your concerns relate to what appears to be mental, physical or learning disability, or an illness related condition?
- If you have invoked the Banking Protocol please include this in your reason for suspicion.



## **Glossary code example 4 – property market**

### **SAR Online view**

**REASON/SUBMIT**

#### **What is your Reason for Suspicion/Knowledge?**

*Insert **glossary code(s)** here at the start of reason for suspicion.*



#### ***Example 4: code and content – property market***

"XXPROPXX This SAR involves the purchase/sale of a property. The property address is ....."

#### **Good practice tips – always:**

- describe fully the reasons for suspicion in relation to the money laundering. As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How?
- also include:
  - describe the full address of the property and post code
  - describe the value of the property
  - the date of activity, how the activity will take place or has taken place AND
  - the full identity, where known, of the other party/parties involved in dealing with the property, including, in particular, if they are providing professional services e.g. solicitor, estate agent, accountant or company formation agent etc. Where a professional enabler is visible also use the code XXPRFXX (see good practice tips in example 5, page 26).



## Glossary code example 5 – professional enabler

### SAR Online view

REASON/SUBMIT

#### What is your Reason for Suspicion/Knowledge?

Insert **glossary code(s)** here at the start of reason for suspicion.



#### **Example 5: code and content – professional enabler**

"XXPRFXX The circumstances of this SAR involves the use of a Professional Enabler. The circumstances are ....."

#### **Good practice tips – always:**

- describe fully the reasons for suspicion in relation to the money laundering. As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How?
- describe the services being provided e.g. "the professional services being provided are..." (e.g. accountancy insolvency, audit, company formation, property conveyance, legal services etc.)
- remember to include:
  - the date of activity
  - how the activity will take place or has taken place
  - full identity, where known, of the other party/parties involved in, including in particular, the type of professional services being provided e.g. solicitor, estate agent, accountant or company formation agent etc.
- describe if suspicion relating to the services being provided appear to be wittingly or unwittingly facilitating the money laundering described. Describe the indicators suggesting complicit criminal behaviour or negligent behaviour of the professional(s) involved.
- The SAR should clearly state how a professional enabler was used. An explanation of why a subject is considered a professional enabler should be included in the SAR.

Examples of how a professional enabler may be used might include: a solicitor used to draw up contracts; company formation agent to make a shell company; an accountant to help liquidation/ insolvency an accountant completing tax returns; a conveyancer helping buy or sell property.



## **Glossary code example 6 – modern slavery and multiple codes**

### **SAR Online view**

**REASON/SUBMIT**

#### **What is your Reason for Suspicion/Knowledge?**

*Insert glossary code(s) here at the start of reason for suspicion.*



#### **Example 6: code and content – modern slavery (use of multiple codes)**

"XXMSHTXX, X XOICXX, XXV2XX and XXV3XX. This SAR concerns some persons who we believe may be victims of modern slavery. Some victims appear to be under 18 years of age and other victims appear to be adults. There are indicators that suggest some of these persons may be in the UK illegally.

#### **Good practice tips – always :**

- describe fully the reasons for suspicion in relation to the money laundering. As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How?
- describe the red flag indicators you are seeing for modern slavery which relates to your suspicion for the money laundering.
- describe the red flag indicators you are seeing for organised immigration crime which relates to your suspicion for the money laundering.
- describe fully all personal information concerning the child – full name, DOB, address and post code, nationality.
- describe fully all personal information concerning the adult – full name, DOB, address and post code, nationality.
- describe if social services are already aware of the circumstances (include any ref number) (persons contacted).
- describe if law enforcement are already aware of the circumstances, in particular the exploitation of the child. Confirm if contact has been made with CEOP (CEOP ref number) (officer contacted).
- describe fully if any additional vulnerabilities exist e.g. if the child or adult is unable to properly protect him/herself against exploitation due to what appears to mental, physical or learning disability, or illness related condition
- separate the glossary codes with a space when using multiple codes.



## Glossary code overview (April 2023) Aide Memoire

<b>Request for a defence under POCA/TACT</b>	
XXS99XX	Request for a defence under POCA
XXGVTXX	Request for a defence under POCA for £3,000 or less
Tick 'Consent' and submit under TACT	Request for a defence under TACT
<b>Money laundering</b>	
XXPRFXX	Relates to person(s) providing professional services or specialist knowledge that wittingly or unwittingly facilitates money laundering
XXSNEXX	Money laundering and linked to sanctioned entities
XXTBMLXX	Trade-based money laundering
XXPROPXX	Relates to purchases and rental of real estate property
XXVAXX	Virtual assets
XXILTXX	Illegal lotteries – operating or facilitating illegal lotteries
XXMLTMXX	Money laundering through markets
<b>Predicate offences - economic crimes</b>	
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 e.g. carousel – Missing Trader Intra-Community (MTIC) fraud
XXF9XX	Frauds against private sector
XXD9XX	Bribery and corruption
<b>Politically Exposed Persons (PEPs)</b>	
XXD7XX	International PEPs
XXD8XX	Domestic PEPs
<b>Money laundering/terrorist financing relating to vulnerable persons</b>	
XXV2XX	Risk to vulnerable adults
XXV3XX	Risk to children – including sexual abuse and exploitation

<b>Other predicate offences</b>	
XXFIREXX	Firearms
XXOICXX	Organised immigration crime
XXMSHTXX	Modern slavery and human trafficking
XXDRUXX	Illegal supply of drugs
<b>Projects/other</b>	
XXPCPXX	Counter-proliferation
XXVICTXX	Where the purpose of the activity is to return money to a victim of crime
XXSATXX	Relating to suspected fraudulent use of the HMRC Self-Assessment Tax Refunds system
XXGPSXX	Relating to suspected fraudulent use of Government Priority Schemes established as a result of COVID-19
XXCVDXX	Relating to any suspicious activity connected to COVID-19