Issue 31

SIA

SARs IN ACTION MAGAZINE

UKFIU
UK Financial Intelligence Unit

ORGANISED IMMIGRATION CRIME:
ILLICIT FINANCE

MINI UMBRELLA COMPANIES:
CALL TO TAKE ACTION ACROSS THE FINANCIAL SECTOR

ASK THE UKFIU

"Dear UKFIU, sometimes when I submit a DAML SAR to the UKFIU I receive a response and other times I don't. Why is this?"

A United Kingdom Financial Intelligence Unit publication aimed at all stakeholders in the Suspicious Activity Reports regime

NCA
National Crime Agency

Message from the head of the UKFIU

Vince O'Brien
Deputy Director

Hello and welcome to the 31st issue of the UKFIU's magazine, SARs in Action.

In our second issue of the year, we start things off with an article from the National Economic Crime Centre (NECC) Public Private Partnership (PPP) team about the need for a response to the issue of Mini Umbrella Company (MUC) Fraud.

We then take a deep dive into the growing threat area of organised immigration crime (OIC), how it differs from human trafficking, the illicit finance elements of the criminality and the NCA's response towards the threat.

Included in this issue are a couple of SAR case studies. We have included these to highlight the benefits of partnership working with reporters and law enforcement and to demonstrate the importance of SARs and how they combat money laundering and its predicate offences.

Also included in this issue is an article on how chargeback claims through a credit/debit card can affect a DAML request and valuable advice to tackle this.

We've asked experts at the UKFIU why responses received to DAML SAR submissions can vary from submission to submission and the possible outcomes to a DAML request.

Finally, don't forget to subscribe to the UKFIU podcast – this is available on a number of streaming sites including Spotify, Apple Podcasts, Amazon Music and Audible

Who is the magazine aimed at?

- All law enforcement; this includes senior investigating officers, frontline police officers and police staff
- Reporters
- Regulators
- Supervisors
- Trade bodies
- Government partners
- International partners

Contents

Opinions expressed in articles provided by partners are not necessarily the view of the UKFIU/NCA. The UKFIU exercises the right to edit submitted articles.

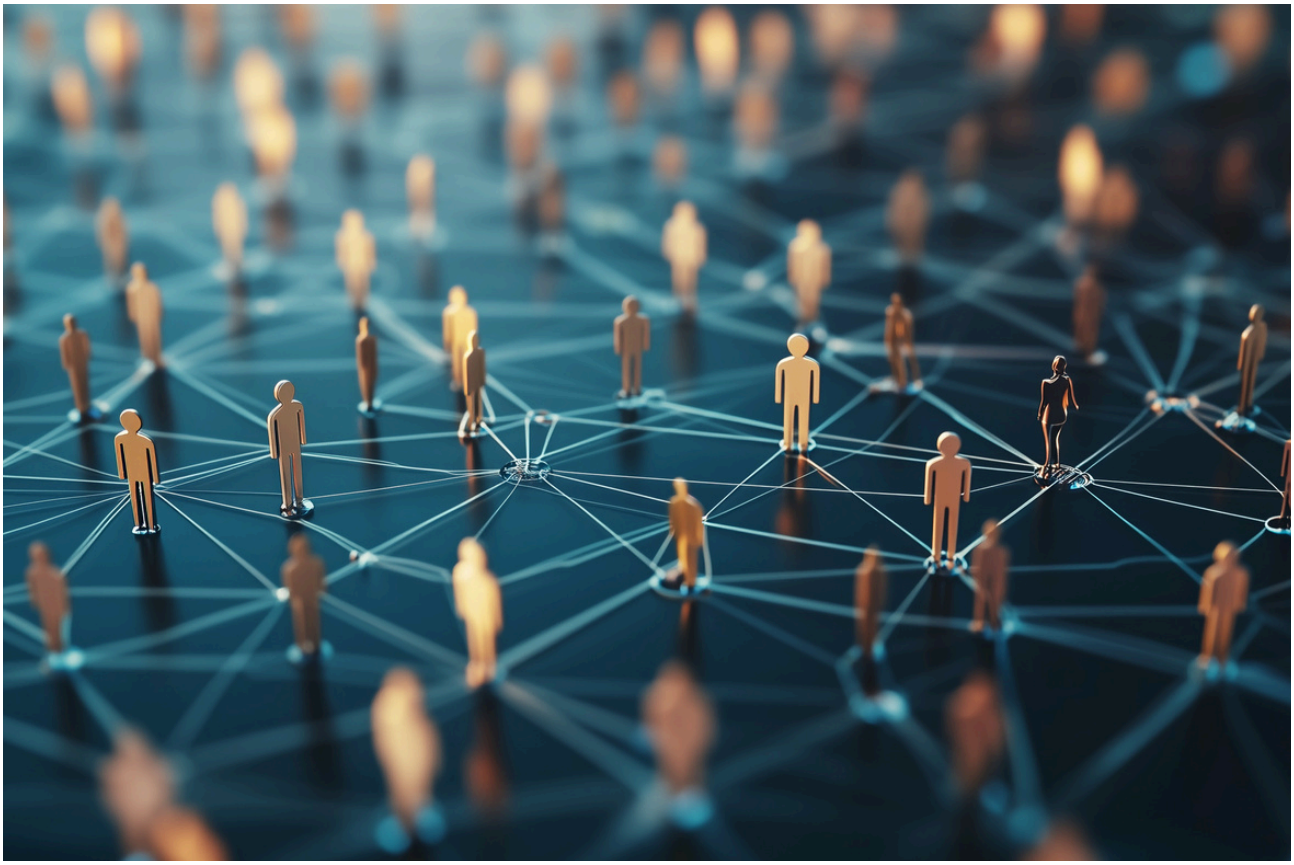
Produced by UKFIU

MINI UMBRELLA COMPANIES: CALL TO TAKE ACTION ACROSS THE FINANCIAL SECTOR

NECC PUBLIC PRIVATE PARTNERSHIP (PPP) TEAM

The Tax Crime & Evasion Public Private Threat Group (PPTG) commissioned a time-limited cell (working group) to look into three strands of organised labour fraud, including Mini Umbrella Company (MUC) Fraud. The cell is chaired by HM Revenue & Customs (HMRC) Fraud Investigation Service and HSBC UK Bank, working to improve understanding and awareness of organised labour fraud across the banking sector.

MUC fraud is the disaggregation of a large, temporary workforce into multiple, small, limited companies (MUCs) by organised crime groups (OCGs). It costs the Exchequer hundreds of millions of pounds every year. HMRC is aware that OCGs regularly target the temporary labour sector and has several ongoing investigations using a full range of civil and criminal powers, in parallel, to provide the most effective and immediate response. SAR intelligence and civil powers to freeze funds acquired from organised labour fraud has led to more than £10 million being frozen in 2024.

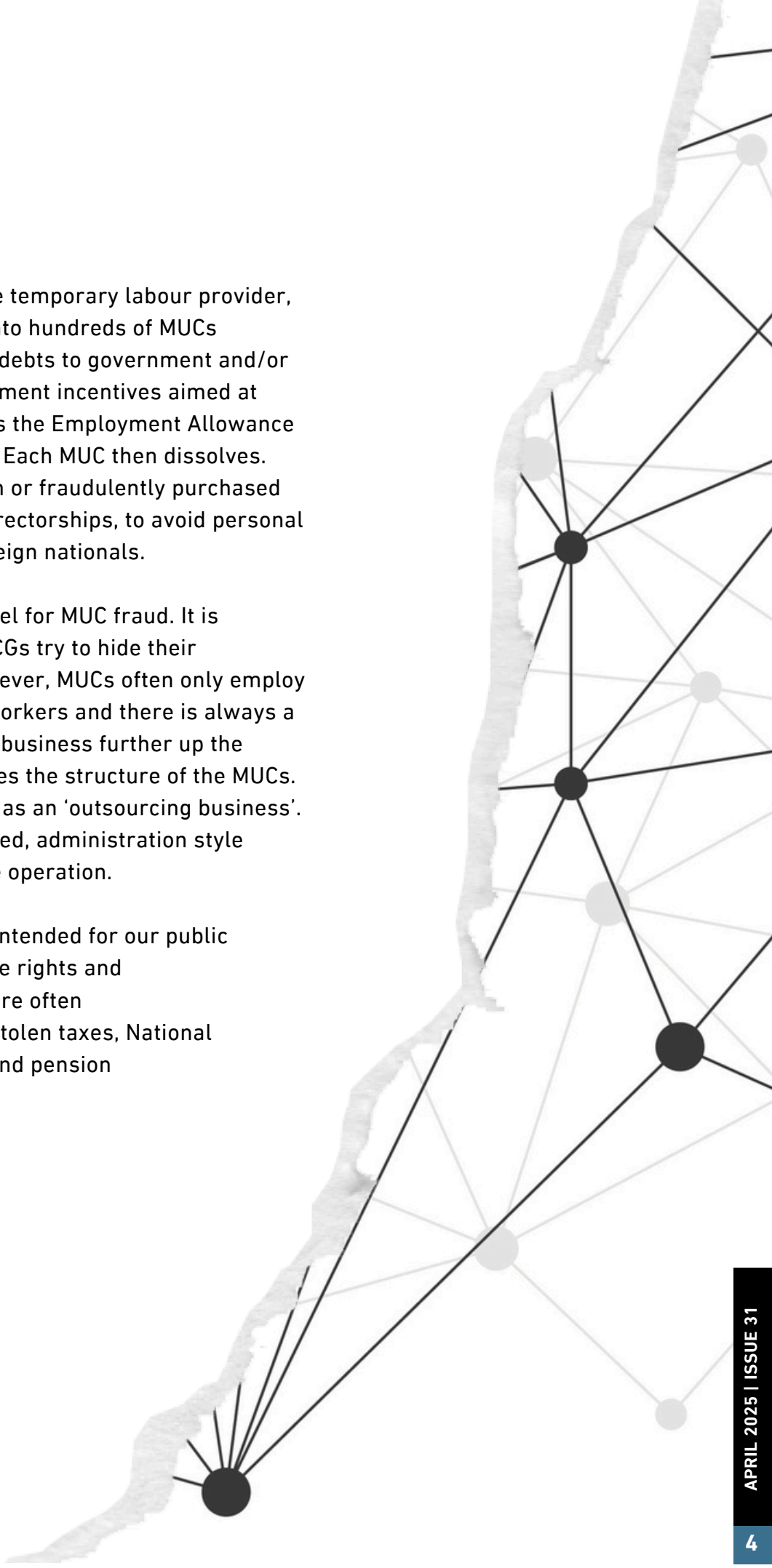


Typologies

The OCGs break down one temporary labour provider, low in the supply chain, into hundreds of MUCs allowing each to build up debts to government and/or take advantage of Government incentives aimed at small businesses (such as the Employment Allowance & VAT Flat Rate Scheme). Each MUC then dissolves. The OCG often uses stolen or fraudulently purchased identities for the MUCs directorships, to avoid personal association, including foreign nationals.

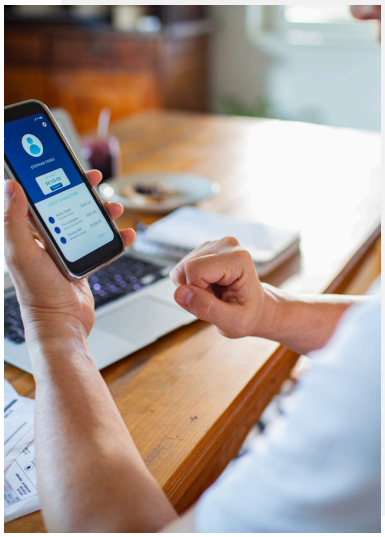
There is no standard model for MUC fraud. It is constantly evolving, as OCGs try to hide their fraudulent activities. However, MUCs often only employ a few (mostly unaware) workers and there is always a promoter/umbrella-style business further up the supply chain that organises the structure of the MUCs. This is sometimes known as an 'outsourcing business'. There are often other linked, administration style businesses to support the operation.

MUC fraud steals money intended for our public services. Furthermore, the rights and entitlements of workers are often compromised, including stolen taxes, National Insurance contributions and pension payments.



Here are some of the signs to look for throughout the supply chain, although each should not be taken in isolation:

- Large volumes of companies registered at the same address, often residential/non-business addresses.
- Periods of dormancy after bank account inception.
- Companies that hold the bank accounts lack an online presence.



- Few or no payments to HMRC.
- Receipts of large payments from recruitment agencies from the opening of the account, far in excess of the anticipated turnover or not consistent with the declared business type.

- Profits from the fraud are often extracted internationally by the OCGs, disguised as fees, admin expenses and other purchases, often through companies and bank accounts also based abroad.
- Links to/use of nonbank Payment Service Providers (NBPSPs) that use FinTech/Blockchain technology and Alternative Payment Systems (APS) to provide financial services without a traditional banking license.

In April 2024, a First Tier Tax Tribunal determined that a specific MUC's model used was fraudulent and the MUCs involved were not entitled to these reliefs. Read the tribunal's decision summary information on judiciary.uk.

Recognising the vital role of the financial sector in tackling MUCs, the PPTG cell published the Mini Umbrella Company Amber Alert on 28 January 2025[1] providing evidence-based indicators and case studies shared by cell members.

HMRC have recently updated their published guidance on MUC Fraud- Mini umbrella company fraud - GOV.UK.

There is also a video available to watch What is mini umbrella company fraud?

If you identify activity demonstrating the key indicators in this article, you may wish to make a Suspicious Activity Report (SAR). It will help our analysis if you would include **PROJECT PHOENIX24** within the text. By reporting concerns, financial institutions are able to reduce the likelihood of reputational damage, loss of customer confidence and potential collateral risks of innocent funds being mixed with illicit finances.

[1] The Amber Alert has been shared with relevant stakeholders and is not publicly available.

Organised Immigration Crime - Illicit Finance (OIC IF)

TACKLING ENABLERS OF OIC | NCA THREAT LEADERSHIP COMMAND

What is Organised Immigration Crime (OIC)?

OIC involves the illegal facilitation of migrants across borders or enabling them to take residence in a country without the required permissions or documentation.

The crossing of the English Channel by small boats is widely reported across all media outlets, however, this is not the only method. Other forms include clandestine entry via concealment in heavy good vehicles, the facilitation by air using either general aviation or non-commercial flights, as well as the abuse of legitimate means to enter and remain in country (visa abuse, use of fraudulently obtained genuine documents etc).

Small boat arrivals were the most detectable method of irregular entry into the UK from October 2023 to September 2024, accounting for over 80% of the total figure of 36,949. Channel crossings generate easy money for Organised Crime Group's (OCG's). OCGs will regularly overcrowd small boats in order to maximise their profit margins. They often lack certification or serial number plates, are made of poor-quality materials and manufacturing and provide inadequate, if any, lifejackets.

These conditions make the small boat crossings incredibly hazardous. The International Organization for Migration (IOM) have estimated that at least 78 migrant fatalities took place in 2024, making it the highest year on record.

How does OIC differ from MSHT?

Modern Slavery/Human Trafficking (MSHT)

Human Trafficking happens when someone facilitates the travel of another person with a view to exploiting this person.

Modern Slavery is the act of holding another person in slavery or servitude. It can happen without trafficking. Where there is a trafficking element, this can be across borders or within one country.

MSHT is a crime against the person and victims can be exploited during the journey and/or at the destination.

Organised Immigration Crime (OIC)/ Migrant Smuggling

OIC involves the illegal facilitation of migrants across borders or enabling them to take residence in a country without the required permissions or documentation.

Migrant smuggling is a mutually agreed service, usually involving transportation and/or fraudulent documents to enter a foreign country illegally, usually in exchange for monetary payment. The person being smuggled consents to the movement.

Migrant smuggling is a crime against the state.

Do OIC and MSHT intersect?

These are separate offences that don't wholly overlap with one another. Migrants may demonstrate vulnerabilities that make them susceptible to exploitation by MSHT offenders, particularly if they still have to pay for their journey to the UK. In the absence of immigration status to remain in the UK and without any legal right to work, offenders often use the threat of reporting the irregular migrant to the authorities as a form of control.

The Illicit Finances of OIC

OIC is a financially motivated crime, with smugglers charging large sums for their illegal services. OIC offending groups prioritise the optimisation of profit margins over migrant safety and welfare.

The financial flows of OIC are particularly complex, in large part due to the widespread use of Informal Value Transfer Systems (IVTS), particularly in the form of Hawala banking.

IVTS facilitates the transfer of the value of funds from one location to another without the money moving physically or through traditional banking structures. The system operates on the basis of trust within a network of payment operators (known as "Hawaladars") who cooperate to settle accounts and execute payments.

These systems are used for a wide variety of reasons – such as cheaper or faster money transmission, cultural preference, lack of confidence in banks or because they are the only channel through which funds can be transmitted in certain conflict regions or less-economically developed countries.

In the UK, Hawaladars are subject to regulations and standards. They must be compliant with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations, and are legally required to report anything suspicious to the UKFIU.

The vast majority of Hawaladars are not aware of the purpose of the payments for facilitating migrant crossings. However, they are an important facilitator of OIC given that:

- Many migrants wouldn't trust OCGs enough to pay them directly. Having Hawaladars acting as escrows for their payment reduces migrants' perceived risk at attempting the crossings.

- The broken audit trails that IVTS generate make the money flows more difficult to trace.

Our response

Tackling people smuggling is a key priority for the National Crime Agency (NCA) and we have around 70 investigations into the highest harm networks and individuals. The transnational nature of OIC makes international collaboration essential if we are to effectively tackle the threat. Breaking the offending business model through the identification and seizure of the illicit money flows associated to OIC is necessary to tackle illegal entry into the UK. This will thereby reduce the likelihood of fatalities due to high-risk smuggling methods.

The NCA's International Liaison Officer (ILO) Network comprises of 160 officers deployed in over 50 countries worldwide and providing a coverage of 130 countries globally. Our ILOs work with international partners and coordinate UK law enforcement overseas to gather intelligence, conduct operational activity (through partner agreement) and enhance international delivery through a variety of means. The methods include capacity building, training and joint European and international taskforces.

Case Studies

A reporter submitted a SAR due to suspicions of money laundering. A subject's account was identified due to an alert being triggered by the reporter's transaction monitoring system. After investigating the account, the reporter determined that the account was being used to deposit cash in order to transfer funds to third parties, which was indicative of money muling. Further review of the account highlighted that the subject had previously been the subject of a SAR, in which the subject had been complicit in layering funds to a prisoner. Further intelligence was developed and transactional links were made to a modern slavery victim. The subject has been arrested for immigration offences and enquiries are ongoing.

Multiple reporters submitted a number of DAML SARs to return funds while exiting their relationship with the same business. Concerns were held regarding multiple accounts held by the business, which frequently received high value payments that were transferred in and out of the accounts, indicating potential money laundering. Some of these payments were received from the subject of a previous SAR. The UKFIU refused the DAMLs and fast tracked the intelligence to the relevant LEA. The LEA was able to launch an investigation into the business, with the business owner refusing to engage when contacted. The LEA obtained multiple Account Freezing Orders (AFOs) and forfeitures on all funds in the accounts, totalling over £100,000.

Europol Project ASSET

NECC ASSET TRACING TEAM

From 13 to 17 January 2025, the UK took part in the first ever Project ASSET (Asset Search & Seize Enforcement Taskforce) event alongside colleagues from 43 law enforcement agencies across 28 countries, and private sector partners. The event, coordinated and hosted by Europol, was a unique initiative aimed at enhancing the number of criminal assets seized globally. Throughout the week specialists pooled their knowledge and expertise to establish a new organisational workstream to identify, freeze and seize criminal assets through all possible means available. During the week, the UK was represented at Europol's HQ in the Hague by colleagues from the NCA's National Economic Crime Centre (NECC) and Asset Confiscation Enforcement (ACE), HM Revenue & Customs (HMRC), and the UK Europol Bureau.

This was mirrored with a multi-agency UK response in the NCA's North West Hub led and co-ordinated by the NECC Asset Tracing Team. NCA officers, working alongside colleagues from HMRC, Companies House, and private sector colleagues, sought to identify UK assets linked to high-level targets from across the globe.

Officers from the UKFIU formed part of the team, and supported the Project by analysing SAR data to identify assets that may have otherwise escaped detection. Their efforts played a particularly important role in identifying crypto asset wallets believed to have been in receipt of the proceeds of crime.

The UK team had the opportunity to speak with Europol Executive Director, Catherine De Bolle, to explain its multi-agency response to the project and reiterate the UK commitment to working alongside Europol to identify and seize criminal assets.

During the course of the week Project ASSET succeeded in identifying:

- 53 properties, of which eight identified by the UK Team were valued at approximately EUR 38.5 million (over £32 million);
- Over 220 bank accounts, including one with a US $5.6 million balance;
- 15 companies, over 20 yachts and luxury vehicles, four of which were valued at more than EUR 600,000 (over £500,000);
- 83 cryptocurrency addresses and wallets.

"This week, the Asset Search & Seize Enforcement Taskforce showcased Europol at its finest. Bringing together over 80 top experts from law enforcement and the private sector, we worked as one to trace, freeze, and seize the profits of organised crime. Together, we're striking criminals where it hurts most – their wallets. As we move forward united, success is inevitable." **– Burkhard Mühl – Head of the European Financial and Economic Crime Centre (EFECC).**

Chargebacks, victim reimbursement and DAML process

MICHAEL JONES
UKFIU REPORTER
ENGAGEMENT TEAM

Chargebacks allow consumers to claim a refund if something has gone wrong with a purchase paid for with a debit or credit card. Section 75 of the Consumer Credit Act 1974 also provides additional protection for some purchases made using a credit card.[1]

The UKFIU is sometimes asked how a chargeback claim affects a DAML request in circumstances where the claim will be paid out of funds subject to either a DAML that is still within the seven working day notice period (a 'live DAML') or a refused DAML that is now in the moratorium period.

To answer this, let's first consider what is happening during these periods.

During the **initial seven working day notice period** for a DAML request, the UKFIU will assess the information provided in the request and consult with partners as necessary. As part of this, the UKFIU will consider the likelihood of law enforcement being able to take positive action against the criminal property (for example, an account freezing order).

If a DAML request is refused, the day the reporter receives the refusal marks the start of a **31-calendar day moratorium period.** During this moratorium period, law enforcement will work to take positive action against the criminal property. For more information on the DAML notice and moratorium periods, see the article on page 13 of Issue 26 of SARs in Action.

It will occur to SIA readers that direct victim reimbursement under either a chargeback claim or section 75 will likely happen quicker than it would through law enforcement channels. So, what's the harm in settling reimbursement claims during the notice or moratorium periods?

[1] For further information about Chargebacks and section 75 protections, see the UK Finance website.

Law enforcement do not wish to cause unnecessary barriers where genuine victim reimbursement has been identified. However, we know criminals use chargebacks to dissipate criminal property to their associates through fraudulent chargebacks or 'victim' notifications.

We also know that investigating and seeking restraint following a refused DAML takes up considerable resource for our law enforcement partners. There have been instances where restraint of funds has been approved by the court, only for the investigating law enforcement agency to be informed that the account balance has been entirely paid away due to chargebacks.

It's important we let reporters know the UKFIU's expectations regarding DAMLs and victim reimbursement.

Important

The NCA considers that, under POCA 2002, all funds in an account or accounts must be 'frozen' during the notice period following submission of a Section 335 DAML request. Any activity relating to those funds, and during any subsequent moratorium period following the refusal of such a request, are vulnerable.

This means that a reporter may be unable to satisfy any external request to pay away those funds, even to a victim through a chargeback claim, until the case is resolved through a court order to recover the funds or a defence is granted.

If a request is received from a victim or through a chargeback scheme for funds subject to a live or refused DAML request, a reporter is likely to be committing a money laundering offence by paying away those funds, unless the reporter has sought to amend their prohibited act with the UKFIU (and received confirmation from the UKFIU that this has been accepted).

Best practice

If you wish to amend your prohibited act during the DAML notice or moratorium period, please email DAML@nca.gov.uk and explain why you are seeking an amendment. You should also email UKFIU DAML if you become aware that the criminal property disclosed in your request has diminished (for any reason).

While this best practice guidance applies to chargeback claims received during the DAML notice or moratorium periods, it is worth us also highlighting the UKFIU's position regarding requesting a DAML for victim reimbursement in general.

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 327-328 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 still obliged to submit a SAR.

If you are submitting a SAR and consider that the purpose of the activity in question is to return money to a victim of crime, select the **XXVICTXX** glossary code on the SAR Portal. In any case where you suspect a criminal offence other than money laundering, in addition to a SAR, we advise you to report the activity through relevant law enforcement channels in the normal way.

If you have any questions about this article, please contact the UKFIU Reporter Engagement Team at UKFIUEngagement@nca.gov.uk.

Ask the UKFIU

EMMA-JAYNE TURNER
UKFIU REPORTER
ENGAGEMENT TEAM

Dear UKFIU

Q Sometimes when I submit a DAML SAR to the UKFIU I receive a response and other times I don't. Why is this?

A When you submit a DAML SAR this triggers a seven working day notice period, during which time the UKFIU will assess the information provided in your defence request and consult with partners as necessary. The notice period starts from the first working day after the day the SAR is submitted, and continues for seven full working days.

You will receive a response during the notice period if:

- we decide to refuse your request for a defence OR
- we decide to expressly grant your request.

The UKFIU may also contact you during the notice period for further information or to clarify your request. We may also close your request for a defence if it does not meet the requirements of an Authorised Disclosure under s338 of POCA. You will receive a written notification if your defence request has been closed.

In other DAML cases, you may not receive any communication or response from the UKFIU before the end of the notice period.

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

For more information about the DAML notice period, and the obligations on reporters after a DAML has been submitted, see Issue 26 of SARs in Action (pages 13-17).

SIA

SARs IN ACTION

UKFIU
UK Financial Intelligence Unit

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

Episode 21

AVAILABLE HERE

THE UKFIU PODCAST

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

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

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