NCA
National Crime Agency

UKFIU
UK Financial Intelligence Unit

SARs IN ACTION

Issue 20 - May 2023

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

Message from the head of the UKFIU

Vince O'Brien
Deputy Director

Hello and welcome to the 20th issue of the UKFIU's magazine *SARs in Action*.

In this fraud focused issue, we look at key fraud trends and threats within the UK and highlight ongoing work to combat fraud.

The criminal offence of fraud is defined in the Fraud Act 2006 (England, Wales and Northern Ireland) as involving dishonesty with an intention to make gain for oneself or another, or to cause another to experience or be exposed to risk of loss.

This leads to a general understanding that fraud refers to a wide range of criminal activities where deception is employed to steal money, physical assets or data, and is often used to fund other crimes.

We look at recent analysis of fraud, including a word from the National Economic Crime Centre's Director on page 3 followed on by an article on key trends in fraud. We also address specific fraud threats, including romance fraud on page 9 and fraud in the accountancy sector on page 16.

There are also articles addressing how SARs have been used to combat fraud, including West Midlands Police Economic Crime Unit and the National Economic Crime Centre.

We also look on page 23 at some of the success stories that have arisen from good quality SARs being submitted by reporters and utilised effectively by law enforcement.

Who is the magazine aimed at?

- All law enforcement; this includes senior investigating officers, front-line 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.

NECC DIRECTOR COMMENTARY

Adrian Searle
Director
National Economic Crime Centre (NECC)

The statistics do not tell a pretty picture. Fraud is over 40% of all crime – there were an estimated 3.7 million fraud offences in England and Wales in the year ending September 2022.[1] One in 15 people were a victim of fraud.[2]

Despite these high numbers, many question the impact of fraud. The banks reimburse many of the victims, so some people might say no harm is done. However, this ignores the fact that ultimately these costs will be passed back to all of us as customers of the banks.

Fraud also undermines trust in our ways of working with, and using, online services and, even more importantly, fraud can cause significant emotional damage. I starkly remember hearing for the first time a call into Action Fraud in which a distraught wife explained that her husband had committed suicide the previous week because he had lost the family savings in an investment fraud.

The Government is very aware that if we don't respond more effectively to fraud, we also have little chance of reducing crime in the UK overall. Another telling statistic is that only 2% of policing is dedicated to combating fraud.[3] So what are we doing about it? The Government has published a new national fraud strategy. This recognises that we need a whole 'system' response to the threat. We need to 'pursue' more criminals, 'empower' people to help them avoid and recover from frauds, and work with partners to 'block' the frauds from happening in the first place.

Our 'pursue' response will shift from a primarily reactive response driven by victim reporting to Action Fraud, into a more proactive intelligence-led approach directly targeting the fraudsters. We will develop our fraud communications to provide clearer and more targeted advice to the public. We will work with partners in both the public and private sectors, here in the UK and overseas, to prevent fraud.

All of this activity can be informed and enhanced by SARs reporting. The more we understand the evolving nature of the threat, including where the fraudsters are operating from (a current judgment is that three quarters of all fraud in the UK has an overseas component to it),[4] the better we can target our 'pursue' efforts, shape advice to empower the public, and stop the fraud from happening in the first place.

The NECC, working with partners across government and the private sector, needs your help to turn the tide of fraud we all face. I hope this edition of the *SARs in Action* magazine with its focus on fraud will encourage and support your efforts.

---

[1] Office for National Statistics; Crime in England and Wales: year ending September 2022.

[2] Office for National Statistics; Crime in England and Wales: Appendix tables: year ending September 2022.

[3] House of Commons Justice Committee, Fraud and the Justice System, Fourth Report of Session 2022–23.

[4] ibid.

KEY TRENDS IN THE FRAUD THREAT

The National Assessments Centre (NAC)

This article was written by the NCA's National Assessments Centre, responsible for producing a wide-range of strategic intelligence reporting on the key serious and organised crime threats facing the UK.

Estimating the scale of fraud is difficult; often reports of fraud and fraud losses include cases where there was no financial loss or where the loss was reimbursed. Despite this, with fraud being the most commonly experienced crime in England and Wales,[1] with nearly 90% of fraud going underreported and taking into account its economic and emotional/psychological costs, fraud remains a prevalent threat to UK individuals, and the public and private sectors.

In 2022, victim losses to fraud increased, whilst victim reporting decreased. Public concerns about their financial situation due to cost of living pressures meant that some criminals implemented a more targeted approach to convince victims to part with their money.

UK victims were targeted by criminals using a range of fraud types. They sustained high losses to investment fraud schemes, many of which involved cryptoassets. The growth in investment fraud was also seen after the 2008 recession as the public looked for higher financial returns on their investments. Criminals recognise that investment fraud savings can provide large returns and that it can often take time before the fraud is apparent to the victim.

[1] Office for National Statistics; Crime in England and Wales: year ending September 2022.

Reporting levels of cyber-enabled fraud increased in 2022. Criminals exploit online growth and social media to reach as many potential victims as possible. Cyber-enabled fraud can be committed from any jurisdiction in the world, and offenders are able to use a range of tools and techniques to obfuscate their identity and location.

Criminals also exploit social, political and economic events to target victims. Examples of this in 2022 included the Ukraine conflict and the death of the UK monarch. In the latter part of 2022, energy rebates were used by criminals to target people seeking to make and save money. Due to financial pressures it is likely that a wider range of people were attracted to becoming involved in money mule activity, which is already a key enabler for laundering the proceeds of fraud.

Impersonation remains a key enabler, with criminals often tricking victims by pretending to be relatives, friends, trusted officials or brand representatives. In September 2022 the NCA acted swiftly with domestic and overseas partners to disrupt an overseas fraud that systematically targeted victims on a massive scale, often through impersonation of domestic regulatory bodies. In November 2022 international law enforcement agencies also dismantled a website allowing criminals to spoof the numbers of trusted organisations.

To circumvent enhanced controls used by organisations, criminals used data breaches and other cybercrimes to harvest personal and financial information to commit fraud. Criminals involved in fraud also focussed on Authorised Push Payment (APP) fraud, which is when the victim is tricked into actively making a payment.

FRAUD INTENSIFICATIONS

The National Economic Crime Centre (NECC)

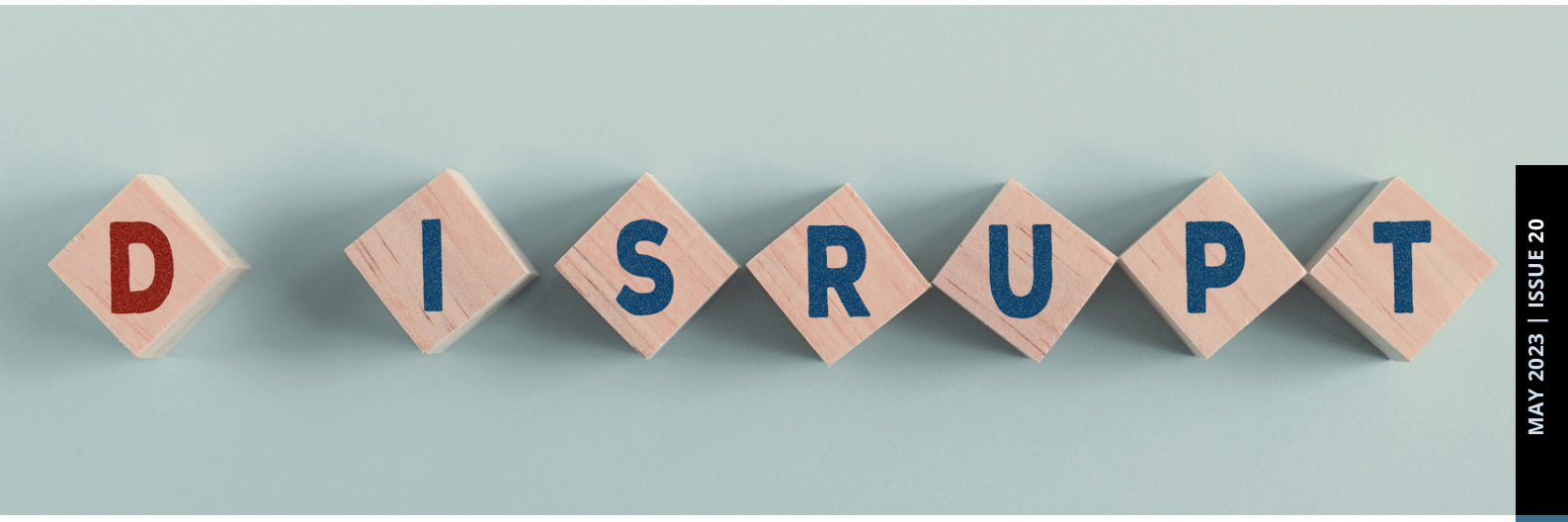
The NECC was created to deliver a step change in the UK's response to, and impact on, economic crime. The NECC brings together partners from law enforcement and justice agencies, government, regulatory bodies and the private sector with a shared objective of driving down serious organised economic crime , protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.

To tackle this threat, the NECC has been working with a wide range of partners to run a series of fraud intensification initiatives throughout 2022/2023.

Fraud intensifications are an opportunity to disrupt fraud activity and gain a greater understanding of opportunities for the system. They are time bound, increased surges of activity to encourage and support new initiatives, build upon existing capabilities, and increase opportunities for multi-agency work.

Intensification activity undertaken within this financial year has included:

1. working with the UKFIU to identify opportunities to increase the response to fraud DAML (Defence Against Money Laundering) SARs
2. delivery of multi-agency activity against suspected boiler rooms
3. a period of activity relating to money mules[1] alongside a supporting national communications campaign
4. and an intensification period focusing on fraud pursue activity.



[1] A person who transfers illegally acquired money on behalf of others knowingly or unknowingly.

SARs have played a key role within intensification activity. A good example is with the intensification on money mules, which took place throughout November 2022. **The NECC worked with partners to obtain data identifying suspected money mule activity.** SARs were a key component within this process enabling the corroboration and development of this data, leading to targeted activity. This enabled appropriate law enforcement action to be taken, including issuing of cease and desist notices.[2]

As part of this activity a number of victims were identified and safeguarded. Operational activity was supported by a national communications campaign to increase public awareness of the prevalence and impact of money mules. The six-week social media campaign was specifically targeted at children and young adults, parents and carers and educational professionals, achieving over 4.8 million views on social media.

An additional period of intensification on fraud pursue activity was actioned in February 2023. This activity facilitated a UK wide uplift on fraud. The month long activity resulted in 290 arrests and interviews under caution by police forces, Regional Organised Crime Units (ROCUs) and the NCA, included high-value seizures, such as a BMW M5 Competition worth £96,000 and multiple luxury items including Rolex watches and jewellery. In total more than £6.3 million in assets were seized or restrained.

Each period of intensification is debriefed and enables reflection by those involved. This gives an opportunity to understand any challenges arising from activity, identify intelligence gaps, and **establish how activity can be improved with lessons learned used to inform the future response.**

> **“290 arrests and interviews under caution... more than £6.3 million assets were seized or restrained.”**

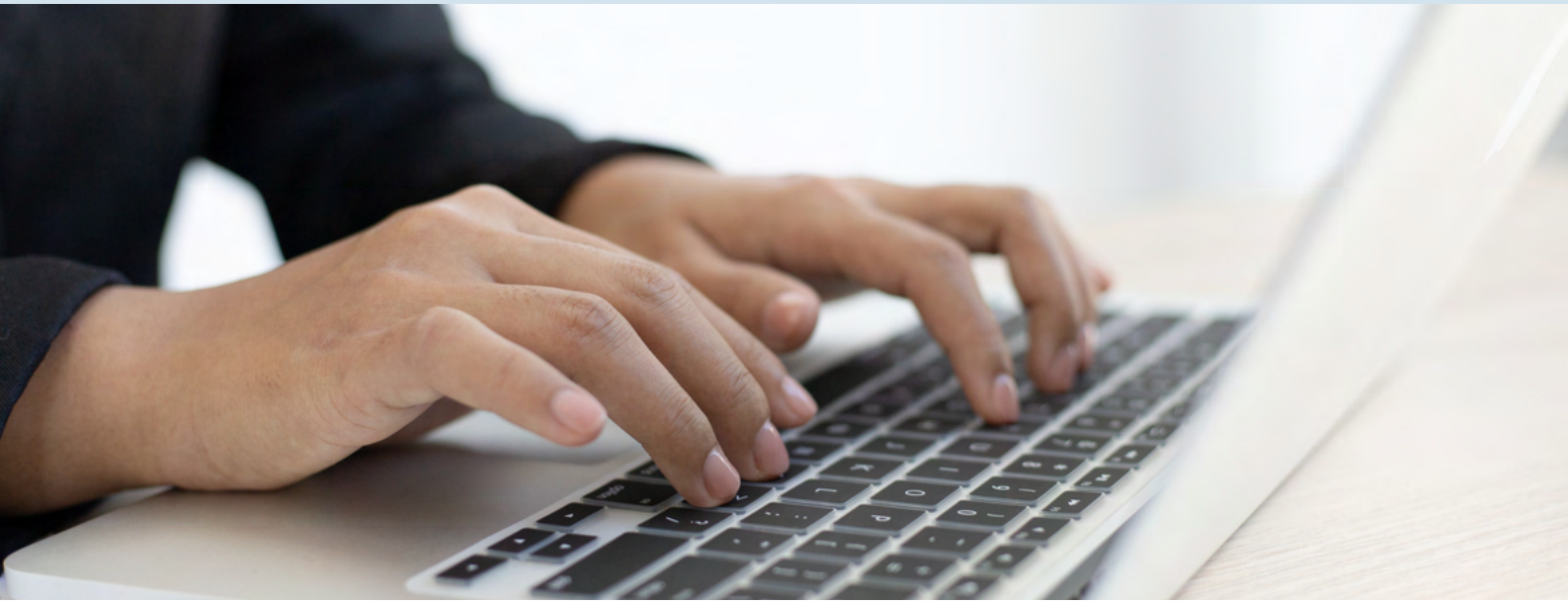
The NECC is currently considering intensification opportunities for 2023/2024 and is looking at ways to increase the number of partners involved with each phase. If you would like further information on the initiatives, have suggestions for future intensifications, or want to get involved, please contact ukfiufeedback@nca.gov.uk.

[2] A notice warning individuals to stop certain harmful actions and refrain from continuing them in the future.

PROTECTING THE PUBLIC FROM FRAUD

Detective Sergeant Vicky Kelleher
Economic Crime Unit
West Midlands Police

West Midlands Police's Economic Crime Unit (ECU) has an Investigation Management Team (IMT) which triages all fraud reports that come into the force. When making a decision on how the case is investigated the IMT will review the allegation and complete intelligence checks (including SARs enquires). In some cases these checks will help decide if an allegation is filed at source or an investigation is commenced. This is particularly useful with lower level offences, if the suspect has no previous offending on police systems but concerns are raised from reviewing SARs. Any SARs identified at this stage are sanitised and placed on our intelligence systems should they hold any information that would benefit the investigation.



The Complex Team in the ECU investigates the more serious and complex frauds. When SARs are reviewed there have been cases where further victims and/or suspects are identified which will then be brought into the enquiry. SARs research can identify further lines of enquiry with cases – on some occasions this has been the difference between filing or continuing with a case.

The West Midlands Police Economic Crime Victim Care Unit also responds to vulnerable person SARs. SARs provide our team with a vital source of intelligence that we may not otherwise be privy to. These SARs allow us to identify and engage with potentially vulnerable victims of fraud, cybercrime and exploitation to prevent financial loss and harm and in turn disrupt organised crime. They also allow us to implement interventions and any safeguarding as appropriate.

ROMANCE FRAUD

UKFIU SARs Enquiry and Action Team (SEA Team)

Fraud is the use of deception to take advantage of an individual, typically for financial gain. It is the most commonly experienced crime in England and Wales. The Crime in England and Wales: year ending September 2022 estimates that it accounts for 40% of all crime and **affects over 3 million people each year**. In 2020 Action Fraud reported losses of £3 billion.

There are many types of fraud but one which can cause the most harmful impact to a victim is romance fraud.

Romance (or dating fraud) occurs when someone believes that they have met the perfect partner online but, a fake profile has been used to form the relationship. The perpetrators often use online platforms such as dating websites or apps, social media such as Facebook and Instagram or gaming sites. Trust is typically built over a number of weeks or months, leading the victim to believe that they are in a loving and caring relationship. However, the offender's motive is only ever to gain money and/or personal information.

When a victim understands that they are a victim of a romance fraud, the impact is two-fold as they potentially have to accept **financial loss** and, importantly, the **loss of the perceived relationship.**

More than a third of couples in the UK meet online and most of the online accounts will be genuine, but there are a few things that people can do to keep themselves safe:

- If you have fallen victim to fraud or cyber crime, report it any time at **www.actionfraud.police.uk** or call **0300 123 2040**. In Scotland report it to Police Scotland by calling 101. If you are a victim of fraud, report it to your bank.
- Ask for your online partner to send you a specific photo of them such as a selfie with something specific.
- Get advice from family and friends.
- Be alert to spelling and grammatical mistakes in communications and inconsistencies in stories.
- Reverse image scanning to identify if the pictures of the online partner has been previously used before on dating profiles or belongs to someone else.
- Be wary of any requests for money from someone you only recently met online, especially if you have never met them face to face.

Some signs that someone might be a victim of a romance fraud are:

- Being secretive about the relationship and withdraw from conversation when asked.
- They have never met in person or over video call.
- They have strong emotions for the individual and are committed early in the relationship.
- They have sent or are planning to send money to someone they have never met in person and may be borrowing money, drawing on pensions to support the person.

If you think someone is showing signs of being a victim of romance fraud there is a 'crime in action' Banking Protocol, which can be invoked. The Banking Protocol is a UK-wide scheme that enables bank branch staff to alert their local police force when they suspect a customer is being defrauded. Police will then visit the branch to investigate the suspected fraud.

In cases where there is a belief that an individual is at risk of any immediate harm **it is essential that this information is not just contained in a SAR and that it is reported to the police via Action Fraud as soon as possible or if it is an emergency via 999.** There is a chance it could be missed by the SEA's triage team despite their best efforts. Additionally, any information shared in a SAR needs to be sanitised by our law enforcement partners prior to onward sharing with non-accredited recipients, taking up valuable resource and time.

The UKFIU received more than 1,000 SARs in 2022 referencing romance fraud; a number of these required fast-tracking to local law enforcement for safeguarding. If a SAR is submitted in relation to a romance fraud victim and associated money laundering, it is helpful for the UKFIU and law enforcement to include any information on where this has been reported, such as an Action Fraud reference. Similarly, if the Banking Protocol has been utilised, it is very helpful and time saving if this can be referenced in the SAR. By including this information we are then able to de-conflict with our partners and, as such, are able to save valuable law enforcement resource and time. Relevant SAR Glossary codes are also very helpful to the triage team so please continue to include them, where relevant.

MONEY MULES

The National Economic Crime Centre (NECC)

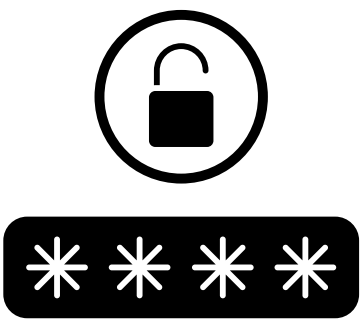
A key mechanism to cash-out the proceeds of fraud against individuals in the public and private sectors is money mule activity. Money mule activity refers to a money laundering process in which proceeds of crime (POC) are moved and transferred through personal and/or business bank accounts.

Mule networks use collections of linked accounts to complete this process, allowing them to disguise the origin of criminally derived funds and extract them elsewhere. Complex transaction chains make it harder for banks to freeze or recover victim funds and for law enforcement to investigate.

Mules are used to facilitate fraud against people and businesses as an essential part of the laundering of fraud POC, be it from low-tech attacks like impersonation or high-tech attacks like malware. Evidence suggests that most proceeds of organised fraud activity use mule accounts to extract and launder funds. Money mules also launder cash generated by a variety of other crimes, such as drugs and firearms supply, human trafficking and tax/excise fraud.

Mule accounts are defined as intermediary accounts used for money laundering, acting to create complex transaction chains in order to reduce detection by the financial services sector and law enforcement of an organised crime network (OCN) and/or individual offenders.

Mule accounts might be operated by a money mule, which is a person who transfers illegally acquired money on behalf of others knowingly or unknowingly. Often, however, a mule account is controlled by a recruiter (sometimes known as a herder), potentially on a temporary basis, after the account holder has provided the recruiter with their account details, bank card, pin and/or passwords in exchange for a fee.



Mule accounts can also be acquired through exploiting vulnerable persons. They can also be opened and operated by criminals who commit fraud using false representation, such as through the use of stolen personal information, without the knowledge of the original account holder.

Money launderers and criminals who commit fraud are likely to use an array of tactics to acquire a multitude of mule accounts, adapting their activity on an iterative basis, according to vulnerabilities identified in industry and law enforcement control frameworks.

Mule account holder profiles

Mule account holders will largely fall into one of three involvement categories:

Witting:

- **Complicit:** Account holder is a complicit money mule, aware of the criminal source of funds, acting through their own choice and typically motivated by a financial incentive.
- **Negligent/Naive:** Account holder should reasonably have had some suspicion - for example, after receiving no assurances or credible cover stories from their recruiter regarding the source of funds. However, they have insufficient information about the original crime ('predicate offence') or full knowledge of the criminal nature of the work to be considered complicit in a money laundering offence.

Unwitting (Victim):

- **'Active' Victim of Fraud:** Actively engages in mule activity albeit under fraudulent, non-employment pretences. The mule may be a victim of crime themselves, such as a romance fraud victim.
- **Unwilling:** Mules engage in activity due to vulnerability or under coercion – for example, abuse of indebted drugs mules in County Lines.

Unknowing (Victim):

- **'Inactive' Victim of Fraud:** Account is acquired and used without the knowledge of the account owner. The account holder may be a victim of identity theft or may be impersonated by criminals.
- **Fake Accounts:** Accounts created wholly using fraudulent documents – for example, it may be created using false identification.

Mule Recruitment

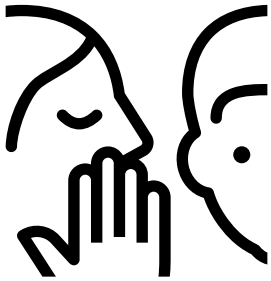
Mule recruitment can be broken into two distinct categories, with a variety of methods:

Online

- Social media/digital messaging
- Seemingly 'legitimate' work/investment opportunities
- Fraud/scam recruitment
- Online social engineering techniques i.e. phishing, vishing etc. leading to ID fraud.

In-Person

- 'Stranger' recruitment (i.e., pubs, schools, universities)
- Friends and family or peer to peer
- Favour for members of 'community'
- Physical job offers posted.



Mule Account Indicators

It is worth noting that OCNs and offenders are highly likely to use a combination of different methods to obtain as many mule accounts under their control as possible.

This list is not definitive and there will be crossovers between different types of mule accounts. Criminals will be dynamic in their deployment and development of new methods.

1. Significant branch or Post Office cash deposits without legitimate explanation.
2. Same day/closely-spaced cash deposits across multiple branches or regions.
3. Deposit values below arbitrary round numbers (e.g. £10,000).
4. Purchase of significant volumes of high-value luxury goods.
5. High concentrations of Scottish and Northern Irish banknotes.
6. Test payments (also known as 'coupling') to make small payments to link accounts together to legitimise new payees and IP addresses.
7. Suspicious activity continues despite being contacted by financial firm.
8. Transactions to/from crypto-currency exchanges.
9. Transactions to/from payment service providers/electronic money institutes.
10. For cryptocurrency wallets, funds may re-merge after they have been through a tumbler service.

11. Company accounts linked with a UK company newly registered with Companies House or purchased 'off-the-shelf' from a formation agent.

12. Company accounts used to co-mingle funds from multiple crime types alongside legitimate income.

13. Significant cash deposits or transfers from another account in receipt of cash deposits, followed by a bulk shopping spree on luxury goods.

14. Use of second personal account in order to keep activity from impacting on their primary account.

15. Thousands of pounds being spent at the same retailer or within short periods of time with repeat purchases of the same amounts, indicating purchase of duplicate goods.

16. Low value/quantity of fraud transactions received into account.

17. Types of document used to pass Know Your Customer (KYC) checks may include:
    - **Fraudulently obtained genuine documents** – documents issued authentically but applied for using false information.
    - **Counterfeit documents** – a reproduction from scratch of an officially issued document.
    - **Forged documents** – a genuine document altered in some way, such as with changed personal details (often a utility bill or bank statement).
    - **Pseudo documents** – documents with the appearance of a legitimate document, but which are not officially recognised.
    - **Impersonation documents** – person is a 'look-alike' presenting someone else's genuine documents.

18. Account holder is a person who, for physical or health reasons, can reasonably not be expected to manage their finances.

If you identify activity which may be indicative of the activity detailed above, and your business falls under the regulated sector, you may wish to make a SAR. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the SAR Glossary Code **XXJMLXX** within the text.

Identifying mule accounts may present opportunities to stop further money laundering by those accounts or individuals, freeze criminal funds and identify the beneficiaries of fraud. All financial institutions are encouraged to check their fraud and money laundering controls against the typologies listed above, to ensure those controls are as effective as possible.

FRAUD AND SAR UTILISATION

The National Assessments Centre (NAC)

The NAC Fraud Team conducts **proactive and ongoing fraud risk monitoring** and assessment to deliver a suite of products. These can include response options and intervention opportunities, which may be drafted by partners based on the NAC's analysis of the threat. These products are used by decision-makers across law enforcement, government and the private sector for their strategic and operational responses. SARs are used by the NAC Fraud Team in several ways to help shape this work.

Examples include using fraud-related SARs, alongside other indicators, to understand how the scale of the fraud threat develops. **SARs analysis is also used to enhance understanding of the nature of the fraud threat in the UK and overseas.** SARs are used by the team to identify and corroborate red flag indicators of suspicious activity. SARs help identify jurisdictions of risk, common methods for laundering the proceeds of fraud and key enablers of different fraud types. In 2022 SARs helped determine the types of fraud most commonly connected with a particular sector (see article immediately below). **The results are shaping preventative fraud measures** in this sector to help protect future victims.

The Multi-Agency Fraud Targeting and Insight Centre (MAFTIC) is a multi-agency team of analysts established in September 2021, funded by the Home Office. MAFTIC is an analytical team looking at high harm investment, payment diversion, impersonation/courier and romance Fraud. The team is responsible for identifying high harm networks across these fraud types and contributing to the understanding of fraud impacting the UK. **SARs have been crucial in the identification of these networks.**

MAFTIC has applied a prioritisation of key words to pull out those SARs most likely relevant and charted to their connectivity. These networks are then enriched. This is achieved through the analysis of large amounts of intelligence and data from different sources in an environment optimised for analysis. MAFTIC then identifies links, for example, subjects of NCA investigations who are in communication with victims or offenders of fraud. An example is the identification of a network of UK based fraudsters who are committing payment diversion and investment fraud internationally. Their turnover is estimated to be in excess of £25 million.

These networks feed the fraud pipeline, which in turn will progress in intelligence developments/investigations and contribute to the Agency's knowledge and response to fraud. MAFTIC has also identified numerous money laundering enablers that are essential to these fraud networks, with these packages disseminated accordingly for tactical and strategic purposes.

FRAUD IN THE ACCOUNTANCY SECTOR

The National Assessments Centre (NAC)

In 2022 the NAC conducted analysis on the nature of fraud threats prevalent in the accountancy sector and the vulnerabilities these highlight. This work is informing the design of fraud preventative measures by the Home Office and accountancy sector professional bodies. It is hoped that the following article will assist not just the accountancy sector, but all reporting sectors, in terms of offering support to avoid falling victim to fraud.

The NAC identified that the accountancy sector was an attractive target for payment diversion fraud (PDF), being employees or external service providers who regularly make and request payments. However, PDF is not unique to the accountancy sector and is one of the most likely frauds to be committed against all businesses.

PDF involves criminals contacting employees who can legitimately authorise payments, pretending to be an employee, supplier, or other organisation who would legitimately request payments. The criminal will advise that bank details have changed and ask the employee to update the records or use fake invoices to make direct payment requests.

Looking at the period of April 2021 to January 2022, the NAC assessed that in relation to the accountancy sector, PDF made up two thirds of reports during the period. The reports encompassed accountants as victims in a number of ways:

1. Those experiencing direct financial loss.

2. Those whose email accounts had been compromised by network intrusion, leading to a client losing money through fraud.

3. Those whose reputation had been damaged by falling victim to a fraudulent request for payment/change of bank details, or by having their computer networks compromised.

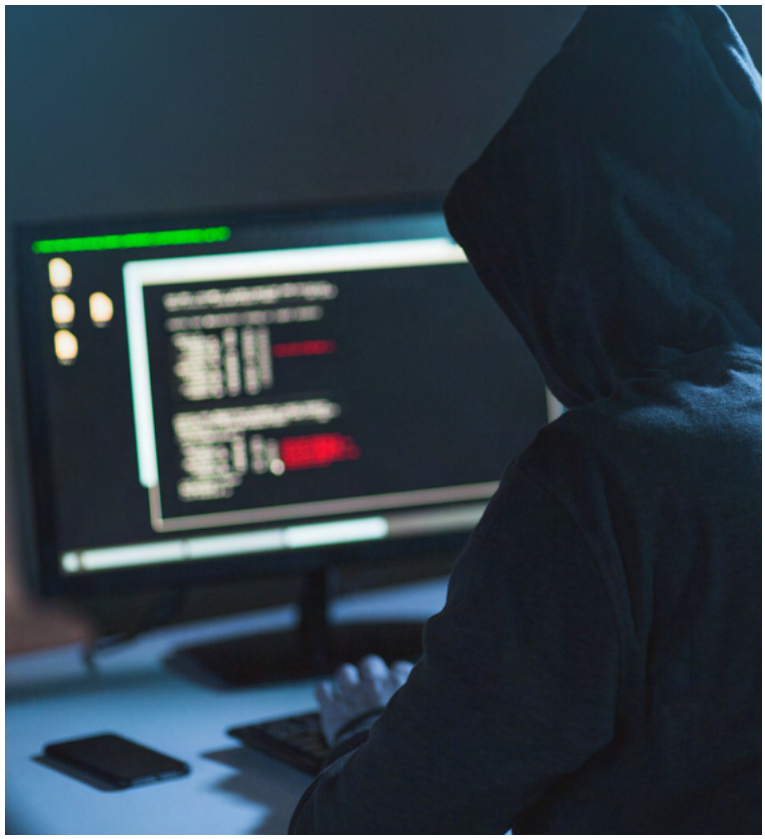
Almost all reported corporate identity frauds in the sector related to criminals copying publicly available company records and using them to facilitate or hide the origin of criminal activity. In half of these cases the accountancy firms were the primary victim of the identity fraud.

The misused company details were primarily used in the following ways:

1. Accountants' brandings, company and/or staff details are used to falsify accountancy documents (such as accountants' certificates) to obtain financial products and other services.

2. Company names and registered addresses are used to obtain credit without the firm's knowledge, consent or benefit. The accountant then receives debt collection letters/visits.

3. Company names and registered addresses are used to add legitimacy to fraud targeting the public, for example investment fraud.



In terms of vulnerabilities, company identity details available online on Companies House, company websites and social media are often used in corporate identity fraud and PDF.

A precursor to PDF is often business email compromise. This is often achieved through malicious links contained in phishing emails.

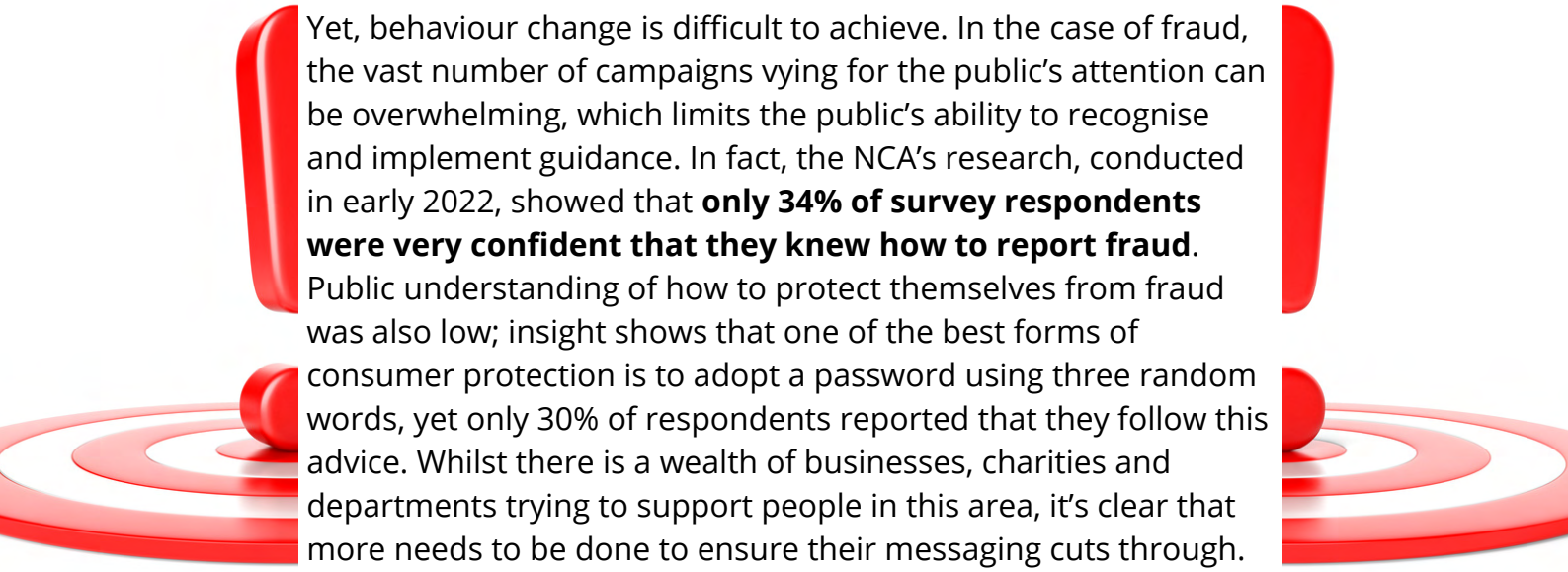
Social engineering used in PDF can be extremely convincing and criminals conduct research to make it effective. Action Fraud has published guidance about the risk of PDF. Continued fraud cases show that there is still a gap in awareness/in the implementation of polices to combat PDF, such as verifying emails or calls stating a change in bank details through an independent source.

The NAC also assessed that the sector may also be disproportionality affected by corporate identity fraud because it is not unusual for accountants to have multiple client companies registered to their address. Legitimate businesses have various reasons for using an alternative registered address – this might be for reasons of confidentiality, or for companies working without an office space of their own.

FRAUD COMMUNICATIONS

The National Economic Crime Centre (NECC)

Communications campaigns can play a vital role in supporting those who work with SARs. They can help to increase the amount of reports, so law enforcement can get a clearer picture of the overall problem. They can even reduce the amount of people who get involved in illegal activity, such as money laundering, tackling the problem at its core. Of course, their most well-known role in tackling financial crime is educating the public on how to protect themselves from fraud, making it harder for criminals to access money illegally. In this way, influencing the public's behaviour can bolster the fight against financial crime.



Yet, behaviour change is difficult to achieve. In the case of fraud, the vast number of campaigns vying for the public's attention can be overwhelming, which limits the public's ability to recognise and implement guidance. In fact, the NCA's research, conducted in early 2022, showed that **only 34% of survey respondents were very confident that they knew how to report fraud**. Public understanding of how to protect themselves from fraud was also low; insight shows that one of the best forms of consumer protection is to adopt a password using three random words, yet only 30% of respondents reported that they follow this advice. Whilst there is a wealth of businesses, charities and departments trying to support people in this area, it's clear that more needs to be done to ensure their messaging cuts through.

In response to this problem, government and law enforcement have come together to coordinate the many campaigns tackling fraud. The Home Office, NCA, National Cyber Security Centre and City of London Police have developed a strategy to cut down on conflicting advice, making it easier for audiences to remember key pieces of guidance. Their framework sets out the core behaviours the public should adopt to protect against, recognise, report, and recover from fraud. These behaviours are based on insight from across sectors, building upon existing guidance, such as Cyber Aware, to create an evidence-driven, streamlined approach.

Underpinning this work is the development of a **fraud communications toolkit,** which provides guidance for partners on how to communicate a number of the core behaviours in a clear and engaging way. The toolkit includes messaging that they can integrate into future campaigns, ensuring that everyone is singing from the same hymn sheet.

Communications is a powerful weapon in our fight against financial crime. The NCA and its partners are committed to working together to maximise its impact.

RECYCLING CREDITS FRAUD

Waste Regimes Operational Services
Investigations Team
Environment Agency

As the environmental regulator for England, we are responsible for implementing environmental regulations across England. Those regulations require companies who handle electrical goods, batteries and packaging to pay for the recycling of the equivalent amount of waste.

Packaging producers (e.g. supermarkets), who create and handle packaging must help fund the recycling of packaging waste by purchasing recycling credits – Packaging Waste Recovery Notes (PRNs) – from UK recyclers and waste exporters.

Prevalence of fraud
There is considerable money to be made from PRNs and this has not gone unnoticed by unscrupulous companies who are exploiting the system for their own financial gain.

The annual PRN revenue is on average around £300 million; 25% (£75 million) of that is estimated to be potentially fraudulent. PRN prices fluctuate due to supply and demand and other market factors. 2022's plastic PRN average price was £232 per tonne; however, this did vary from £60 to £425 per tonne.

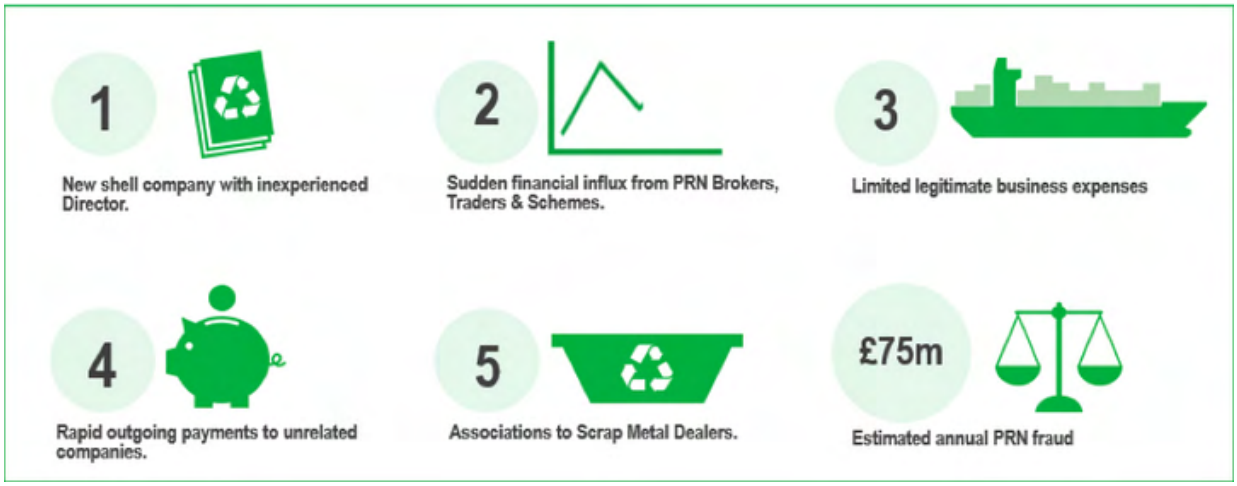
What is PRN fraud?
Our recent focus on plastic waste exporters has identified large PRN claims on fictious waste, i.e. no waste existed, was exported or recycled and the paperwork is forged.
PRN funds acquired by a fraudster will appear on face value to be from a legitimate source, (such as a supermarket or Compliance Scheme) despite being acquired unlawfully. These criminal assets can be utilised to facilitate further money laundering.

Red flags

Here are some common themes fraudulent waste operators use to facilitate their criminality:

1. Newly incorporated company, with shell company attributes.
2. Director(s) new to waste management.
3. Following a period of inactivity, sudden financial acquisition in short period (e.g. £1 million over two weeks).
4. Limited ingoing and outgoing payments demonstrating legitimate business, i.e. payments to hauliers, shipping lines, waste suppliers, staff. Or payments from overseas recycling companies.
5. Large unprecedented incoming payments from PRN brokers, trading platforms or Compliance Schemes. Email us for a list of known PRN brokers.
6. Rapid substantial outgoing payments, particularly to 'non-waste' entities e.g. financial services, IT services and restaurants (PRN revenue should finance improving recycling rates).
7. Associations to scrap metal dealers, involved in money laundering and serious organised crime.

Fraudulent PRN abuse and illegal waste exports pose a persistent international reputational risk and ultimately threatens the UK's Circular Economy and Net Zero commitments.



Contact us

If you think you have come across PRN fraud, you can email us about it at:
prores_investigationteam@environment-agency.gov.uk

SAR FRAUD INTELLIGENCE

The Fraud Intelligence Team (FIT)

Fraud is one of the highest priorities for the NCA. It covers a multitude of methodologies, from romance fraud to boiler room fraud. Fraud flourished even during the Covid-19 lockdown, with criminals exploiting the British public and the Exchequer taking advantage of a stretched National Health Service. In the year to September 2022 there were over 3.7 million fraud offences, accounting for 40% of all crime[1] and according to some estimates caused £137 billion[2] in losses to the UK each year. Monetary value alone does not fully cover the adverse effects of fraud, with lives frequently ruined as a result of individuals being defrauded of savings. The shame and stigma of being a victim of this kind of criminality has ramifications far beyond the financial.

The National Intelligence Hub's FITs are committed to disrupting those individuals and organised criminal groups (OCGs) who seek to take advantage of the vulnerable. In order to develop high quality investigations aimed at combatting fraud and for inclusion on the High Priority Grid,[3] the FIT works with partners internal and external, domestic and international. A fundament of the FIT's work is the identification of money flows, particularly where this is emblematic of fraud.

The ability to review and analyse SARs is key to the intelligence development process, and to the identification of those fraudsters doing the most damage to the UK. A measure of the worth of SARs to the development of fraud investigations is provided by FIT officers themselves:

A reporting bank submitted a SAR linking an address to an account assessed to be in receipt of fraudulent funds. I had previously been able to link a Subject of Interest (SOI) believed to be engaging in fraud to the same address and as such was able to further link them to fraud, giving further credence to the hypothesis that the SOI was linked to fraud.

SARs have frequently yielded intelligence which I've been able to parallel and/or break out as a form of words, thereby developing the intelligence picture

Officer – Belfast

[1] Office for National Statistics; Crime in England and Wales: year ending September 2022.

[2] https://www.crowe.com/uk/insights/financial-cost-fraud-data-2021

[3] A monthly generated grid document providing an understanding on current high priority activities. Includes operational updates contributed by the NCA and partners.

SAR intelligence checks are a core component of all of my fraud intelligence developments. They greatly assisted me early on in corroborating intelligence in relation to fraud. On a number of occasions, SARs checks have aided me in identifying previously unknown criminal counterparties. I have also used SARs intelligence to increase my confidence statements[4] in briefings, when making assessments of a subject of interest's involvement in fraud. It can take time to fully analyse SARs, but the benefit of a richer intelligence picture is a worthy reward.

Officer - London

SARs are vital in triaging and formulating assessments of intelligence referred to the agency by partners. They provide a wealth of searchable information, providing insight into the scope and criminal methodology of fraud, and how this is use used to generate and launder the proceeds of crime.

In one example, a SARs search for a subject's mobile number identified links to a high volume of bank accounts. These accounts were used by different individuals, forming a money mule network to launder an OCG's proceeds of crime.

On a separate development, a search of a company linked to one of the subjects identified a linked business account likely being used to launder the proceeds of crime. Further analysis of SARs identified this account was part of a much larger money laundering network involving companies across Asia and Europe.

Officer – NCA North West Hub

SARs will continue to play a major part in the development of fraud related intelligence, enabling and furthering the NCA's ability to strike at those inflicting the most harm on the UK's finances and on its population.

[4] Confidence statements - descriptions designed to indicate an officer's/analyst's confidence in their assessments based on available intelligence.

CASE STUDIES

1 SARs were submitted after the primary subject in an investigation had amassed a large amount of funds from cryptocurrency trading commonly linked to money laundering offences. Enquiries revealed that the main subject and an associate had received fraudulent business loans, the funds from which had likely become the initial investment for the cryptocurrency account as no consistent income had been seen previously from any personal or business accounts related to the subject prior to the loans being obtained. The subjects used the money from the loans to make a series of large transactions pertaining to luxury goods and services and had transferred funds multiple times to each other and close contacts, a possible indication of layering. Reporters submitted DAML requests which were subsequently refused and Account Freezing Orders were obtained on the subject and their associate's accounts totalling upwards of £3 million. Investigations are ongoing.

2 A DAML request was submitted after the reporter decided to exit a relationship with a customer who had been subject to inquiries by a Law Enforcement Agency (LEA) that had resulted in allegations of fraud. The funds were believed to have originated from fraud outside of the UK. The UKFIU refused the DAML request and the case was forwarded to the relevant LEA who obtained an account freezing order for funds in excess of £10,000, which were subsequently forfeited.

3 A DAML was submitted around a subject who was involved in a fraud investigation in relation to stealing funds from their employer by false representation. A restraint order had been obtained in relation to the subject's share in a property and two vehicles. The reporter submitted the DAML after this decision, having been alerted to the subject due to adverse media indicating that they had a previous conviction for fraud-related offences. The subject had stolen over £100,000 of public funds in order to pay back fraudulent gains. The subject could not explain the remaining balance in the account related to the DAML, and these funds of over £8,000 were added to the restraint order.

4 A DAML request was submitted to pay away remaining funds to a subject due to concerns they had provided fake payslips to justify their account activity. The subject claimed that the account was used for day to day spending but transactions did not reflect this, with the account also being accessed in the UK and abroad simultaneously, indicative of fraud. An LEA confirmed that they only had knowledge of this subject through an ongoing investigation around a different account. The funds within this account were also believed to derive from fraud. Account freezing orders were subsequently granted on both accounts for over £50,000.

Missed an issue?

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

We'd love to hear what you think of the publication, what topics you'd like us to consider and we're always open for possible articles and collaborations. Please send any feedback to ukfiufeedback@nca.gov.uk

The UKFIU Podcast

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

Updates can also be found on Twitter at NCA_UKFIU and via our LinkedIn page.