National Crime Agency

# SARs IN ACTION

Issue 5 - May 2020

@NCA_UKFIU

www.nca.gov.uk




**SARs analysis on COVID-19**
page 04

**Reporters' approaches to fighting fraud**
pages 14-21

**UKFIU protecting UK economy**
page 06

**SARs value in combating NHS crime**
pages 12-13

**Modern slavery and human trafficking**
page 03

**A United Kingdom Financial Intelligence Unit (UKFIU) publication aimed at all stakeholders in the Suspicious Activity Reports (SARs) regime**

# Message from the head of the UKFIU

**Ian Mynot**

I am delighted to welcome you to this special edition of our magazine. There were an estimated 3.8m incidents of fraud in the year ending September 2019, and in this issue we shine the spotlight on this crime which has such a profound economic and human cost.

We feature the National Economic Crime Command's support to maximising the exploitation of intelligence, while the UKFIU's own SARs Enquiry and Action Team lifts the lid on their contribution to thwarting those who prey on the vulnerabilities of the public and private sectors.

There are also insightful perspectives from reporters and law enforcement agencies on the challenges faced.

We also focus on an ambitious initiative delivered by the NCA's Modern Slavery and Human Trafficking Unit (MSHTU) to combat these financially motivated crimes.

If you would like to find out more about the MSHTU contact MSHTU3Psteam@nca.gov.uk. If you have a suspicion that modern slavery is taking place in relation to money laundering, please use the glossary code XXMSHTXX in your SAR.

This helps with analysis and fast-tracking processes in place to protect the public.

Alternatively, contact the police:

- in an emergency dial 999
- for non-emergencies dial 101
- for additional advice, you can contact the Modern Slavery Helpline which operates 24/7 on 08000 0121 700

# CONTENTS


| | |
|---|---|
| **MSHT** | **3** |
| **SARs analysis on COVID-19** | **4** |
| **Fusion Cell** | **5** |
| **UKFIU and tackling fraud** | **6** |
| **New SAR glossary codes** | **7** |
| **Fighting fraud in the NECC** | **8** |
| **Inside the world of the SFO** | **10** |
| **City of London Police** | **11** |
| **SARs value in the NHS** | **12** |
| **Legal sector perspective** | **14** |
| **Banking sector perspective** | **16** |
| **Revolut** | **18** |
| **Wirecard** | **20** |


**Who is this 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**

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/collaborations.

Previous issues of this magazine are available on the NCA website.

Please send any feedback to **ukfiufeedback@nca.gov.uk**

PLEASE NOTE: Opinions expressed in articles provided by partners are not necessarily the view of the UKFIU/NCA.

# Modern slavery and human trafficking

**Hardeep Walker and Sarah Shaw of the NCA Modern Slavery and Human Trafficking Unit (MSHTU) describe a nine month journey to deliver a new initiative working closely with the UKFIU.**

MSHT is a financially motivated crime that takes place both in the UK and globally. The pursuit of profit by Organised Crime Groups (OCGs) comes at a high moral price. They coerce victims into providing a service, tricking them into believing they will be offered a good job and the chance of a better life; the reality is the complete opposite. Their criminal methods are cruel, often violent, causing considerable misery for financial gain.

A lot of work has been done with the banking sector through the Joint Money Laundering Intelligence Taskforce to tackle this. The MSHTU identified that there was a significant knowledge gap around how MSHT may present itself within the accountancy and legal sectors. As this is a crime purely driven by money, the MSHTU called upon the UKFIU to discuss its knowledge of the sectors and decide how best to reach out to them.

The UKFIU recommended that the best start would be the Sector Affinity Groups, bringing together supervisory bodies from across the sectors. The Affinity Groups contribute to the Anti-Money Laundering Supervisor Forum; through their channels officers could reach out to large and small firms.

The first major step took place in July 2019. Following considerable planning and meetings the MSHTU and UKFIU created an engagement plan, with the initiative outline given at the Affinity Group meetings and Supervisor Forum. Key aims were to raise awareness and to consult on where the crime would be visible in those sectors. The key proposal was to work together to identify red flags that could indicate MSHT was taking place.

In September 2019 volunteers from across the sectors took part in workshops hosted by the UKFIU and MSHTU. Case studies were discussed and the impact this type of exploitation has on victims was demonstrated with footage from a television documentary featuring Operation Fort, the largest UK investigation of modern slavery. This revealed how legitimate businesses can be infiltrated by MSHT crime groups, not only making those firms unwittingly involved, but also making money laundering harder to spot.

Discussions took place around what accountants and legal professionals were seeing and suggestions were made to help shape and influence the structure of the red flag indicators. Care was taken to ensure that the red flags met the needs and expectations of both sectors. In parallel, the UKFIU produced a new SAR glossary code (XXMSHTXX) for use when completing SARs that suspect MSHT. The MSHT red flag indicator guidance documents were published in Spring 2020.



# SARs analysis on COVID-19

The UKFIU has been conducting analysis of SARs which relate to COVID-19 and/or coronavirus to inform the intelligence picture for partners at home and abroad.

Several SARs have been seen relating to suspicions that individuals are exploiting the COVID-19 outbreak to account for money movements that suggest possible money laundering. COVID-19 is resulting in the general public making a lot of changes to their behaviour. Most of these are not suspicious; however, in the below examples reporters have cited some of these in combination with other money laundering red flags.

- Large credits or cash deposits into accounts, which the account owner explains as funds from a planned holiday, house or car purchase, cancelled due to COVID-19 (sometimes into previously inactive accounts) or business owners claiming to be making deposits for staff wages.
- Sending funds abroad to relatives to buy face masks.
- Customer claim funds, received into accounts from multiple sources, from the importation and selling of face masks.
- Customers in receipt of multiple faster payments then withdrawing large amounts in cash, claiming to have lost faith in the banking system as a result of COVID-19.
- Concerns around the issue of facilitating 'emergency' loans to subjects about whom they hold money laundering concerns.

SARs have reflected how the COVID-19 pandemic is being exploited to further facilitate existing fraud methodologies. Examples include:

- Individuals or businesses suspected of taking payment for, but not supplying, face masks, hand sanitisers and other Personal Protective Equipment (PPE).
- Social engineering whereby fraudsters impersonating high street banks persuade their victims to transfer funds to a new account following a 'security breach'. The fraudsters used COVID-19 as an excuse for changes to normal bank procedures.
- Victims believing they are investing in companies developing a vaccine for COVID-19.



# New drive to tackle COVID-19 crime

The NCA has launched a new initiative, bringing law enforcement and government together with the private sector to tackle criminals seeking to exploit the COVID-19 crisis for financial gain.

The new 'OTELLO COVID-19 Fusion Cell', led by the National Economic Crime Centre (NECC) and co-sponsored by the private sector, brings together experts from across sectors – including the financial sector, insurance companies, trade bodies, law enforcement and the wider public sector.

The Cell aims to rapidly share information on changes to the economic crime threat related to COVID-19 and to proactively target, prevent and disrupt criminal activity, protecting businesses and the public.

This builds on the existing public-private partnerships that exist in the National Economic Crime Centre, including through the Joint Money Laundering Intelligence Taskforce and the UKFIU.

There is concern that criminals are using the pandemic as a hook to harm vulnerable people for financial gain or to continue illicit activity. Whilst the overall level of fraud being reported has not significantly increased, there has been a noticeable shift towards scams directly linking to Coronavirus.

More people working from home and an increase in online activity has left both businesses and people vulnerable to scams. Lockdown has also changed the way people conduct their lives and business, with an increase in mobile banking, e-payments and cash stockpiling.

This means criminals may adapt their methods to continue illicit activity.

The Fusion Cell will work in partnership with industry to identify new trends and threats and decide on the most appropriate way to tackle it, building on the expertise of both the public and private sectors.

The Fusion Cell will remain as a virtual body during lockdown, convening regularly to discuss the economic crime threat picture related to COVID-19.

The Cell produces a weekly public-private threat dashboard, including high-level SARs trend data, to inform areas for proactive tactical development and disruptive action.

Insight from developing the Fusion Cell has the potential to inform a longer term ambition to develop the capability to spot and stop economic crime before it happens, with real-time insight and disruptive activity through public-private data sharing.



# The UKFIU and tackling fraud

Fraud remains an increasing threat to the UK economy as fraudsters continue to prey on the vulnerabilities of the public and private sector. The UKFIU's SARs Enquiry and Action (SEA) Team reviews SARs daily, identifying current patterns and trends.

Technological development has made it easier to identify, contact and manipulate potential victims. The emergence and increasing popularity of social media,without a full understanding/awareness of its risks, makes it easier for criminals to operate. One method identified in SARs is to advertise goods for sale, particularly high value items, priced much lower than the recommended retail price. Victims are given an account number and instructed to transfer payment. The product never arrives and the seller is uncontactable. As a result of the SEA Team viewing and assessing SARs each day the following has been observed.

Cryptocurrency has resulted in a new spin on investment scams, partially due to a lack of an overall understanding. 'Investment opportunities' advertised via social media see victims encouraged to 'invest' in Bitcoin or a 'new virtual currency' offering substantial financial returns. Victims are encouraged to ensure its success and increase their return by continuing to invest. When they request their funds be paid, they are informed that additional investment is required for them to be released or the original contact fails to reply. This often results in a substantial loss to the victim.

Fraudsters also target the vulnerable through romance scams. Online dating allows for easier communication with potential targets. Victims will initially send small amounts; however, as the 'romance' develops and a relationship is formed, the amounts increase, resulting in high value losses to victims. There is also an emerging trend of people concocting fake stories to generate false fraud claims against the bank e.g. using a vulnerability to try and get the bank to process the fraud claim, therefore receiving money that they're not entitled to. Banks are starting to identify such cases and will refuse payment; however, it is a trend to be aware of.

To help obscure the source of fraudulent funds, there is the continued use of money mules, frequently aged under 18 and recruited through social media, allowing their accounts to be used to conceal funds. Funds are also being laundered through multiple mule accounts and then converted into cryptocurrency, therefore making it harder to trace. The UKFIU fast-tracks SARs involving vulnerable people or child money mules to law enforcement, whilst referring others to NCA teams for review.



# New SAR glossary codes

The UKFIU has implemented three new SAR Glossary Codes for reporters as a result of the increased threat posed by OCGs seeking to exploit the COVID-19 situation by means of fraud.

HMRC Self-Assessment Tax Refund system. Whilst the 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 behaviour in accounts which could suggest fraudulent activity.

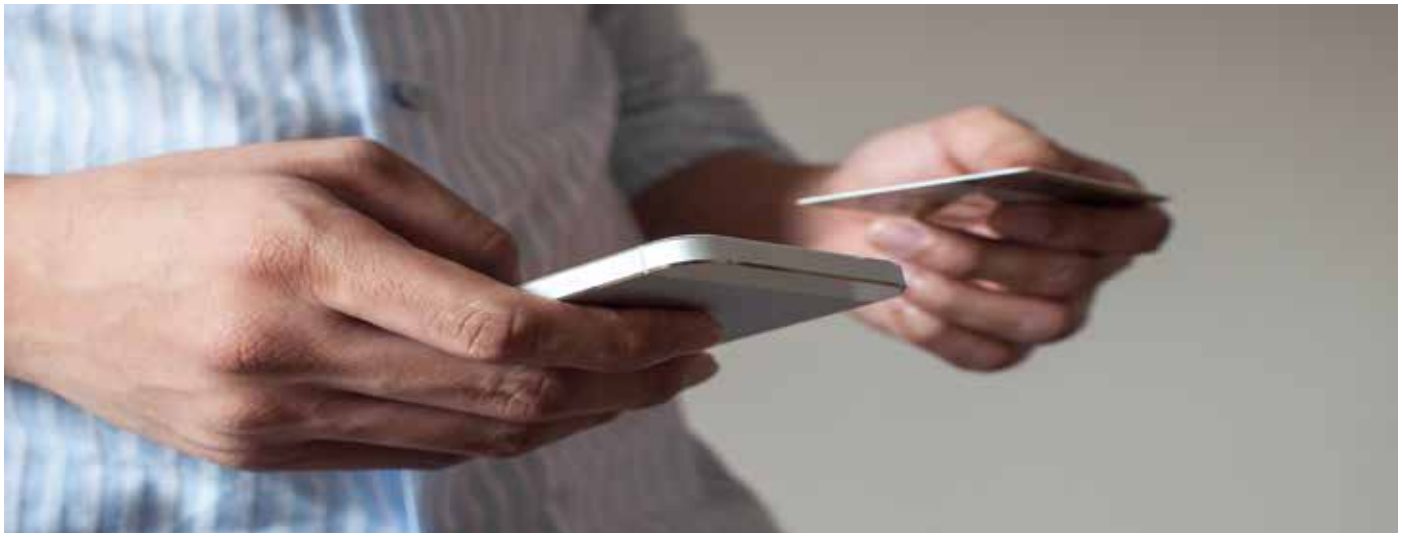
The government has introduced a number of schemes to offer support to businesses/individuals during the outbreak. Reporters should be alert to the potential for these schemes to be exploited by OCGs to commit fraud.

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 behaviour in accounts which could suggest suspicious activity.

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. Please ensure that no other variations of this code are used. XXGPSXX or XXSATXX should ONLY be used if the suspicious activity relates to COVID-19.

For further details on all these new codes please see the updated May 2020 SAR Glossary Codes and Reporting Routes document available from the UKFIU at www.nationalcrimeagency.gov.uk



# The fight against fraud in the NECC

Victims of fraud – particularly, investment and pension liberation – often don't know they have become victims and it can be some time before they realise (often at the point that they expect to receive projected returns). The prosecution of criminals accused of complex fraud often requires resource-heavy investigations that can last years and law enforcement has been servicing competing demands for resources.

In response to this the NECC set up Project Otello, a multi-agency, cross-government taskforce to understand and disrupt the UK threat, involving the NECC, the Financial Conduct Authority, HM Revenue and Customs, City of London Police (CoLP), Serious Fraud Office, Home Office, Cabinet Office, Cifas and UK Finance. There has been an increase in NECC Fraud Team resources by shifting NCA, regional cyber investigative resources and the NCA-CoLP Economic Crime Partnership Team (which is the NCA Complex Financial Crime Team joining with the CoLP Money Laundering Taskforce to provide a more dynamic response to financial intelligence) into fraud related work. Otello concentrates on four fraud types – courier, investment, romance and payment diversion.

Otello's key objectives are to:

- deliver an immediate surge in disrupting criminal activity in fraud followed by a sustainable operational increase in the response to fraud.
- identify and target the highest harm fraudsters and organised crime gangs by targeting intelligence resources upstream.
- protect victims and reduce their vulnerability through increased public awareness and raising confidence in the law enforcement response.
- support Home Office led work to deliver a 'step change' to the entire system of analytical and data technology on fraud.

The NECC Fraud Team is focussing on the response to investment fraud. Working with the NCA National Data Exploitation Capability (NDEC), the NECC Fraud Team conducts data-driven analysis on investment fraud to enable a better understanding and to produce operational benefits with the potential to be developed into analysing data for future. This involves working with data scientists and consultants to exploit bulk data from different sources and conduct analysis.

As a result, the NDEC and the NECC Fraud Team will build a picture of the networks creating the most harm. One of the key data sets for this project is SARs data. This forms the foundation of our fraud analysis, opening up different avenues in identifying large networks. The scope and potential for data exploitation centred on SARs is vast, as they are, by definition, the mechanism by which suspicious transactions are reported. Once SARs data is merged with other NCA and law enforcement databases this increases understanding of the wider fraud threat, looking into patterns/links/trends which will lead to new operational opportunities.

Otello aims to use this methodology widely across economic crime threats. Data-driven analytical capability can potentially set new standards in the understanding of fraud, produce accurate and authoritative assessments and identify tactical opportunities to be delivered back to the wider Serious Organised Crime community

tasked with tackling fraud. The NECC Fraud Team also works with other UK law enforcement agencies/police forces which investigate investment fraud, debriefing them on their investigations to provide further intelligence and to identify the highest harm networks/individuals involved, with a view to building the bigger picture and disrupting those involved. The NECC Fraud Team is currently prioritising work on a public and private sector project to tackle COVID-19 related fraud.

The NECC Fraud Team works with the NCA National Assessments Centre and police, Her Majesty's Government, regulators, Interpol/Europol, SARs data and data from the Dark Web to produce a NECC Weekly Dashboard. This provides an analysis of the latest threats to UK individuals/businesses at an Official-Sensitive level, available to a select number of recipients.

This ensures that the NECC and its stakeholders hold the most up-to-date knowledge of the threat and it is also used to inform tactical responses and prevent/protect messaging to victims. SARs have been of considerable use to the Dashboard in indicating levels/types of COVID-19 related fraud affecting the financial sector. Another document produced by the Fraud Team is the NECC Fraud Grid covering analysis and prioritisation of fraud threats to focus efforts on identifying the highest harm investment fraud networks through data exploitation, and prioritisation of cases which are reviewed and discussed at operational planned meetings.

One of the challenges faced by the team involves data sharing between organisations; this raises a complex set of hurdles over use of the data, legality of sharing data between organisations, General Data Protection Regulation and security of access of data storage. Having key economic crime agencies involved means that these stakeholders work together to resolve these issues.

Bulk data analysis also presents a unique set of challenges in assessing whether data-sets can be modified and more technologically aligned, in order to improve the potential for searching across them. In the long term, data sharing from the private sector will be required for this programme to reach its full potential.



# Inside the world of the SFO

**Paul Tibbenham, Financial Investigator**
**Pietro Boffa, Senior Financial Investigator**
**Serious Fraud Office**

The SFO investigates and prosecutes cases of serious or complex fraud, bribery and corruption. The main role of the SFO's Proceeds of Crime and International Assistance (POCIA) team is conducting post-conviction confiscation investigations and non-conviction based civil recovery investigations. Many of our confiscation cases originate from fraud offences like investment, corporate and pension frauds as well as publicised investigations such as the London Inter-bank Offered Rate (LIBOR) rigging.

The SFO organisational case team structure is called the Roskill Model in which investigators and prosecutors work together from the start to the end of a case, and as such the POCIA team contains a mix of investigative lawyers, investigators and financial investigators.

There are a number of SFO case teams who are assigned several accredited financial intelligence administrators and financial intelligence officers to assist with some of the Proceeds of Crime Act (POCA)-type functions arising during investigations, such as reviewing financial intelligence on Moneyweb (the online portal through which end users access the SARs database) and Arena (a search and analysis tool for SAR end users), as well as carrying out pre-order enquiries.

POCIA provides a team dedicated to the financial investigation of each case on a prioritised basis. This includes providing advice and guidance to each case team on various POCA issues that may arise, such as money laundering regulations, SARs, dealing with EGMONT (the coordinating body for the international group of FIUs) and CARIN (Camden Asset Recovery Inter-Agency Network - an informal network of international law enforcement and judicial contacts aimed at assisting criminal asset identification and recovery) requests, while also dealing proactively with suspects subject to restraint orders.

The POCIA financial investigators are all accredited and as such are trained to deal with and handle SARs. A large quantity of SARs viewed originate from financial institutions; this can provide us with a wealth of information. Moneyweb and Arena play a huge role in our investigations and are interrogated regularly to obtain pertinent intelligence which may be useful to investigations, in particular to obtain bank account details, addresses and details of assets linked to suspects that we previously were unaware of.

POCIA also actions all defence against money laundering (DAML) requests assigned to the SFO. Once the DAML request is received, the SAR is reviewed, sanitised and disseminated to the appropriate case team. POCIA is responsible for managing the process and providing a recommendation to the NCA on whether consent should be granted or refused. The POCIA team also provides advice and guidance to all sections of the SFO in respect of SARs. Information received via DAML SARs has also recently enabled POCIA to commence investigations under the Criminal Finances Act 2017, in particular account freezing and forfeiture investigations.

# City of London Police and SARs

**Mark Forster**
**Detective Inspector**
**City of London Police**

The Pro-Active Money Laundering Taskforce (PMLTF) is a partnership between the NCA and City of London Police (CoLP) aimed at tackling organised crime. The PMLTF dynamically reacts to illicit finance activity whilst also providing a proactive capability to disrupt it. The unit uses powers bestowed under POCA and the Criminal Finances Act to achieve the asset denial of organised crime groups engaged in fraud and money laundering. The PMLTF routinely uses SARs, which support our operational work in a number of ways.

The PMLTF has conducted numerous pro-active investigations into large money laundering networks, responsible for depositing substantial amounts of cash into business bank accounts. Unlike personal accounts, identifying business accounts across the financial sector is far more problematic. The use of SARs has greatly assisted in identifying these accounts and the recipients of onward payments. In turn, searches against SARs are then completed against these entities to map wider money trails.

SARs have assisted our operations by providing us with suspect IP addresses, mobile telephone numbers and vehicle registration marks via Hire Purchase Information payments. Ordinarily, these would not have been available to law enforcement, and have assisted in the identification of criminals committing fraud and money laundering.

Within the PMLTF we have formed a productive and close working relationship with the UKFIU. The UKFIU, upon request, can fast-track SARs to our unit so that SARs can be viewed before the seven days it takes for them to be published on Moneyweb or Arena.

This early access to SARs is vital for the proactive element of the unit. It enables us to protect the financial sector in respect of DAMLs and protect those who have fallen victim to fraud. Ultimately, it increases our chances of early interception and prevents the dispersal of illicit funds before they dissipate out of the UK financial system.

Many LEAs, who are initially forwarded a DAML request, do not have the resources available to allocate to investigating the origin of the money. Therefore a number are returned to the UKFIU suggesting consent for monies to be paid away. The UKFIU regularly consults with the PMLTF on a number of these DAMLs and many are referred for further assessment. Often, following an initial investigation, the PMLTF reverses the original decision and suggests refusing consent before taking steps towards achieving an account freezing order (AFO). In just four months this year this working relationship has resulted in the PMLTF securing a total of £1.5 million of frozen funds held under AFOs, of which £200,000 has already been forfeited.



# SARs value in fighting NHS fraud



**David Hall**
**National Health Service**
**Counter Fraud Authority**
**Fraud and Financial Investigation Lead**

When the NHSCFA was launched around three years ago we made it clear we were going to be intelligence led; we would deepen the understanding of how fraud occurs against the NHS and, wherever possible, prevent fraud before valuable funds for patient care are diverted into criminal pockets. Our annual Strategic Intelligence Assessments give the best picture we can of the landscape, breaking down the headline figure of over a billion pounds a year of NHS money vulnerable to fraud.

In the November 2019 issue of this magazine I wrote about how the NHSCFA is increasingly using SAR enquiries pro-actively within investigations. I gave an example of a £1m mandate fraud against an NHS Trust where it is proving extremely useful to work closely with police forces hooked into the Arena system.

A variety of NHS frauds, particularly in procurement, can also be cracked through a similarly collaborative approach, especially going forward. In the short time since November, there has of course been a tsunami of change to the NHS landscape in the shape of the COVID-19 pandemic. Rapid injections of large amounts of money, while absolutely necessary to tackle this extraordinary virus and its impact on our society and economy, will inevitably attract the attention of fraudsters. From minor opportunists to organised criminals, we must be ready to pounce before they do. If they think NHSCFA is going to stop advocating for the necessary checks and balances to protect NHS resources, they are mistaken.

NHSCFA, alongside many others, has participated enthusiastically in supporting the cross-government counter fraud effort led by the Cabinet Office, including all the initiatives of the Government Counter Fraud Profession. Nobody knew that COVID-19 was around the corner, but fortunately the efforts to build up the capacity of the UK's counter fraud sector were already advancing – from the sharing of best practice to setting up apprenticeships in counter fraud (a programme NHSCFA helped to shape).

We now have a strong and experienced team on the financial investigation side, spread across several departments, the human capital to help us extract the most from the technology around SARs. When sifting a great deal of intelligence, of inevitably varied quality, the nuggets we receive via the NCA, for example leads from regulatory figures in banks, are of a welcome high grade.

All nominals within national level investigations led by NHSCFA are "washed" by financial investigators and financial intelligence officers across the Moneyweb/Arena database to harvest any financial intelligence. This has led to the identification of additional bank accounts, offenders laundering money and telephone numbers used by subjects. Even if such a scenario turns out not to be a criminal diversion of NHS funds – placing it outside our economic crime remit – we will still flag it up to our contacts in other NHS branches. As every law enforcement officer knows, prosecution is not the only way to disrupt deeply antisocial activities.

NHSCFA participates in the SARs IT Transformation Project, part of the SARs Reform Programme, including the related Change Impact Assessment. We are encouraged by the work the NCA team has completed to date and excited about the launch of the new platform with its enhanced features to aid investigators, transforming the existing Moneyweb and Arena systems.

We will be feeding back on the specified features of the new IT system, including how our various users expect to be impacted in NHSCFA. We are also pleased to have been consulted on our preferred methods for communication and training – a good sign that this project is determined to listen to its end users and make access to shared intelligence as user friendly as possible.

It is not a one way street. SARs sometimes highlight interest in a subject under NHSCFA's spotlight from other law enforcement bodies, encouraging joint working or at the very least, the avoidance of crushed toes. SARs are a powerful tool for those investigating fraud against the NHS and in the new landscape, that is going to be more true than ever.

**Use of SARs for intelligence analysis**

SARs financial intelligence was made use of by NHSCFA's Senior Intelligence Analyst to develop original intelligence reported into the NHSCFA and via the National Fraud Intelligence Bureau, regarding an alleged mandate fraud against the NHS. Moneyweb and Arena enabled details such as sort codes, bank accounts, business names, addresses, telephone numbers and email addresses to be cross referenced with those held within SARs.

Any matches have a high chance of unveiling the real identity of those involved, given the inescapable need for fraudsters to provide at least some respectable contacts and channels to banks to access 'their' money (such as the clean/official phone for talking to the bank, to complement the fleet of burner phones).

SARs interrogation also pointed up themes and methodologies such as: the prominence of office supply invoice fraud, using correspondence details of virtual offices; the use of prepay bank accounts having less oversight than more established and conventional banks; patterns in timing of certain frauds; and NHS system weaknesses to close. In turn, this enriched intelligence picture assists our Fraud Prevention Unit in targeting threat awareness messages to the NHS.

# Meeting the challenges of COVID-19



**Jonathan Fisher QC**
**Lead Counsel**
**Bright Line Law**

Fraud is pervasive and COVID-19 presents fraudsters with great opportunities. The challenge for the business community is to help investigating authorities identify and apprehend the fraudsters. In some instances, frauds will not be difficult to spot. In others, the fraudulent activities will be sophisticated and will sometimes hover over the line between sharp practice and dishonest conduct.

Offers of fantastic financial returns on making investments associated with fighting COVID-19 which turn out to be bogus are an obvious example of blatant fraud. The NCA and police have already warned that criminals are targeting vulnerable people looking to buy protective face masks, hand sanitiser and other products online  A new term, "smishing", has entered the criminal lexicon, where criminals send text messages pretending to be another organisation intending to trick individuals into providing personal information.

The government schemes for furlough relief, tax breaks and other financial support will attract the attention of fraudsters. Identity fraud is an obvious exposure, with criminals assuming the identities of those who have sadly died in the pandemic. The retrospective manipulation of financial accounts will also confer significant advantages. Benefits flowing from fraudulent conduct will generate criminal property.

The risk of COVID-19 fraud needs to be reflected in a business's AML risk assessment, policies, procedures and staff training. Companies and individuals should revise risk assessments as a priority. The remote establishment of new relationships needs to take the enhanced risk of identity fraud into account.

It is sad to say that if a business comes across a person who indicates that the source of their income has some connection with COVID-19, then caution must be exercised. Questions about the history of the business, the nature of the trading and source of funds should be asked, and where necessary a report to the NCA will need to be made. Turning a blind eye to asking the right questions exposes otherwise law-abiding businesses and individuals to the potential for committing money laundering offences.

The more challenging area for the business community and the regulated sector involves conduct which is more borderline.

Take a director of a healthcare company who secretly establishes a rival company to develop COVID-19 anti-viral tables. Is this sharp practice or criminal conduct which contravenes the Fraud Act? The answer turns on an assessment of whether the director was under a legal duty to disclose his interest in the new company, and if so, whether the secretion of his interest was dishonest or not.

A more common scenario is bootlegging. A 500 ml bottle of established brand hand sanitiser costs around £5. Mr Smith is selling a bootlegged bottle for £50. The bottle carries similar but not the same branding and is 75% as effective as the genuine article. Has Mr Smith committed a criminal offence? The goods are not counterfeit and the answer depends on an application of the law of theft, and whether, when he obtains £50, Mr Smith is dishonestly appropriating this money, even though he obtains the money with the purchaser's consent. Can it be said that Mr Smith's conduct would be regarded as dishonest by the standards of ordinary reasonable people, or is the overcharging no more than legal, albeit immoral, sharp practice?

In discharging their AML reporting obligations, the business community and the regulated sector have difficult decisions to make where a question mark can be raised over whether a person's conduct was dishonest or not. According to the Court of Appeal, a person suspects or has reasonable grounds for suspecting that another person is engaged in money laundering when he or she recognises that this is a possibility which is more than fanciful (R v da Silva, 2016).

This begs the question as what is meant by "fanciful". The dictionary says that the word connotes something "over-imaginative and unrealistic" or "highly ornamental or imaginative in design". This suggests that the AML reporting obligation should be discharged, even where the possibility of involvement in criminal activity is slim.

The temptation to express the chance of money laundering as a percentage should be resisted. Is a 20% chance less than slim? What about a 15% chance? The better way to approach this is to scrutinise the factual position and ask – is there anything about this situation which looks unusual or inconsistent with expectations? If the answer is yes, there are concerns to be explored, and an appreciation of reasonable grounds for suspicion, with disclosure to the NCA, may follow.



# A banking sector approach to fraud



**Shahbaz Mohammad**
**Senior Manager**
**Financial Crime and Operational Risk Oversight TSB Bank**

**Additional content provided by Garry Parker, TSB Senior Fraud Investigations Manager**

The effects of fraud are felt not only by banks and other financial institutions, but also by our mutual customers and their local communities. Fraud is not a victimless crime – it's a tool for organised gangs, who use the funds that they steal to bring drugs, violence and other crimes to our streets. Tackling fraud is not only a financial imperative, it's a moral one. All banks and financial institutions invest heavily in monitoring systems and tools to detect fraud and protect themselves and their customers from becoming fraud victims. However, the fraud threat environment is constantly changing.

Fraudsters are extremely organised and use highly sophisticated methods to exploit vulnerability within an organisation's control environment, as well as targeting customers directly. For instance, social engineering is becoming more prevalent and this type of scam is becoming increasingly sophisticated in nature, especially in the current situation where COVID-19 can exacerbate the vulnerability of customers. Across the industry, we are seeing an increase in purchase scams (for example in relation to fraudulent COVID-19 home testing kits), smishing (with fraudsters sending 'spoof' text messages pretending to originate from an official source such as the government) and phishing (where fraudsters send scam emails – such as the offer of a refund while impersonating a recognised company).

TSB has a very simple fraud strategy: Prevent, Protect and Pursue – and we work in partnership with the rest of the financial services industry, broader industry, charities like Crimestoppers and LEAs to make a difference. Fraud detection is often a top priority for banks, but we believe broader prevention measures should be equally important. TSB invests a great amount of time and resources on staff training and awareness, as well as on customer education. We delivered 182 Community Fraud Awareness Workshops to over 11,000 people in 2019, with a particular focus on vulnerable customers.

Sadly, we know that fraudsters get smarter, and the scams get harder to detect every year. Despite our best efforts, fraud can happen to anyone; and when it does, it is our job to look after those customers. At TSB, we don't believe that a victim of fraud should be financially penalised for falling for a sophisticated scam. That's why, in April 2019, we launched our Fraud Refund Guarantee. If a customer has lost money from

their TSB account, and is an innocent victim, they will receive a full refund. And to prevent customers from becoming repeat victims we provide bespoke education for each customer depending on the type of fraud they've fallen victim to.

TSB and the wider industry continue to invest in new systems, tools and initiatives to better protect customers from fraud. UK Finance reports that £1.8bn in unauthorised fraud was stopped in 2019 alone, and technological changes continue to be developed, including initiatives such as Confirmation of Payee and Strong Customer Authentication.

Finally, at TSB we firmly believe that committing fraud must have consequences. If someone tries to defraud our customers, we will work tirelessly to bring them to justice - to answer for the crime that they've committed and the hurt that they've caused a victim. TSB reports fraud to the National Fraud Intelligence Bureau and where required to the NCA via SARs, and works directly with local forces, providing useful intelligence for the detection and disruption of serious organised crime - preventing further fraudulent activity and harm.

Meanwhile, we continue to invest in partnerships with police forces and other agencies across the UK to supply equipment, specialist training and insight into fraud - which has led to some great results, breaking up thousands of attacks and arresting dozens of fraudsters. These partnerships form part of TSB's strategy to bridge the gap between the banking sector and policing and has already seen significant results in disrupting organised crime rings behind millions of pounds' worth of fraud across customers of all banks.

We firmly believe that the only way to tackle fraud is by working together. Not only together in the finance industry, but across all industries and sectors throughout the UK and abroad to help keep customers of all banks safe.



# Shades of fraud



**Leonid Komov**
**Group Money Laundering Reporting Officer for Revolut**

**Revolut is an e-money institution in the UK servicing more than 11 million retail and business users**

Revolut offers consumers a prepaid multi-currency card and mobile app focused on offering free currency exchange to customers. Five years on and Revolut - with more than 2,000 employees in 26 different offices globally – now includes travel and device insurance, ability to hold exposure to cryptocurrency, make donations, perform free commission stock trading, open savings accounts, set up direct debits and more, all accessible via a single app. The expanding product range and geographical span creates a serious challenge for our anti-financial crime programme specifically when dealing with fraud risk.

Fraud is a broad term encompassing instances of internal fraud, laundering of funds deriving from fraudulent activity (which we refer to as acquiring fraud), card compromise fraud (issuing fraud), cyber-related fraud (such as account takeovers [ATO]), application fraud, authorised push payment fraud and others.

Revolut utilises in-house technology to tackle various frauds. This is a combination of machine learning techniques, rule and scenario based fraud detection systems and preventive mechanisms e.g. additional authentication measures on the device. A combination of these tools allows Revolut to constantly improve precision and accuracy of anti-fraud measures and drives significant benefits from an effectiveness and efficiency perspective.

A good example is a real-time fraud detection system developed by Revolut called Sherlock which enables us to reduce and maintain the level of compromised cards fraud to less than 0.01% of transactions - significantly lower than industry average. The accuracy of Sherlock alerts is high and efficiency stems from the fact that users can discount false positive alerts via the mobile app themselves following certain authentication steps.

While the Revolut customer base has been growing exponentially and now comprises millions of users making it similar in size to incumbent banks, its transactional activity is characterised by a high number of low value payments and transfers which affects the sensitivity of the tools used to detect funds derived from fraudulent activity.

At the same time high precision and detection capabilities of our transaction monitoring systems also determines a need to submit DAMLs if suspicion of holding criminal property derived from fraud is formed. This often results in identification of whole clusters of accounts associated with layering illicit funds and which remain on the accounts that require subsequent DAML requests to be filed for the balances to be removed from Revolut books.

A large part of work related to mitigation of fraud risk should involve measures applied on the customer onboarding stage. A combined application of in-house techniques based on internal data sets, as well as external industry-wide fraud databases, is a key driver of effectiveness of controls which are put in place to address this risk.

When it comes to ATO risks, customers must be vigilant in the current turbulent environment driven by the global outbreak of COVID-19. According to available data a number of scams related to COVID-19 are on the rise, including: sending phishing emails and text messages; fraudsters physically approaching elderly and vulnerable people pretending to be NHS health officials; and online purchase frauds offering COVID-19 related tests and medicaments. Action Fraud reported a 400% increase in COVID-19 related scams in the UK in March 2020 compared to February. Revolut also witnessed an increased number of (unsuccessful) account takeover attempts in March (specifically for users in massively affected countries) and closely monitors the situation to minimize the risk for our customers of being defrauded.

It is vitally important to make consumers aware of elevated fraud risk and proactive communication is key in mitigating the risk of account takeover and minimising the number of victims and potential harm caused by fraudsters.

A holistic approach to handling fraud risk in a fintech company should comprise a complex of measures ranging from application of cutting-edge technology to customer onboarding and ongoing monitoring of customer activity to proactive engagement with the customers in order to drive better awareness and vigilance.



# Preventing the exploitation of fraud

**Daniel Watson**
**Head of Compliance, Wirecard**
**Rebecca McLean**
**Financial Crime Manager, Wirecard**

**Wirecard Card Solutions (CS) is a full-service provider (offering a full range of services and solutions to other companies) in electronic payments, risk management solutions, prepaid cards and back office services. It is authorised by the FCA as an electronic money issuer.**

Wirecard CS provides products to consumers and companies through a network of 'Programme Managers' – companies that have contracts with customers to provide innovative payment solutions and services to corporate and private customers. There are approximately 50 Programme Managers across the UK and European Union who use Wirecard for two reasons: it is a regulated firm and has the relevant regulatory permissions to support e-money and payment accounts; and the Programme Managers need a sponsor to issue Visa or Mastercard, the cost of which can be prohibitive for small firms.

Although Wirecard is accountable under the regulations for all the products its Programme Managers operate, it does outsource some operational aspects of its AML compliance to the Programme Managers whose responsibility is to apply risk-based customer due diligence measures, conduct transaction monitoring and take other steps to prevent products from being used for money laundering or terrorist financing - following approval of these measures by Wirecard, who then oversees these internal controls and procedures to effectively monitor and manage the Programme Managers' – and therefore their own – compliance with legal and regulatory obligations.

Wirecard's policy is driven by actively participating in preventing its payment solutions from being exploited by criminals and terrorists. It is committed to ensuring compliance with all applicable laws, regulations and supervisory-body requirements, thereby protecting against the risk of reputational damage and ultimately making a positive contribution to the fight against crime and terrorism.

Wirecard's Compliance Team has compliance oversight and is responsible for on-boarding Programme Managers, assessing their systems and controls and ensuring that all appropriate measures and procedures are in place. The role of the Financial Crime Team, which is tasked with the detection and prevention of money laundering and fraud, includes transaction and profile monitoring, dealing with internal SARs and their appropriate referral to the NCA, and handling enquiries from law enforcement such as Subject Access Requests, Production Orders and Court Orders.

With Wirecard offering more than 50 different products and solutions we see a wide variety of fraud offences. Advance fee fraud (where fraudsters target victims and persuade them to make advance or up-front payments for goods/services), and/or financial gains that do not materialise, are the most common and pose a significant challenge due to the small amounts of funds usually involved.



Social engineering such as phishing (where fake emails, text messages or telephone calls purporting to be from a legitimate source such as a bank or e-commerce site are used to induce individuals to reveal personal or financial information), telecom fraud, romance scams and investment or boiler room fraud are also commonly seen, where fraudsters exploit a person's trust to obtain either money directly or confidential information to facilitate a subsequent crime. Social media is the preferred channel, but it is not unusual for contact to be made in person or by telephone –e.g. a fraudster might call claiming to be from a bank, to persuade the victim to move funds to a 'safe' account.

Capturing the information required for regulatory compliance without hindering customer experience is a delicate balancing act faced by all reporting entities. It is difficult to deliver business efficiency, allowing the customer the freedom and ability to use and gain maximum benefit from the payment solutions, while applying necessary controls such as transaction monitoring to meet compliance obligations and protect against the criminals who are quick to exploit any vulnerability.

Wirecard is unequivocal in its assessment of the role SARs play in tackling fraud and ensuring that its services are not used to further criminality. Internal SARs are very beneficial and a vital source of information, especially when they can identify links across Programme Managers, which would not otherwise have been made and can in some cases be instrumental in exposing fraud rings.

SARs enable Wirecard to collate information, identify patterns and trends and contribute to the understanding of the various types of fraud, their prevalence and nature. This enables Wirecard to better focus its detection and prevention activity and to put measures in place to mitigate fraud offences and educate Programme Managers. We emphasise the need to take care when looking for the next opportunity. It is important to listen to our instincts and be wary of unsolicited calls, emails or online adverts offering deals that sound too good to be true.

Fraudsters often pretend to be from a trustworthy organisation. Genuine banks or other trusted organisations will never ask for confidential information or pressure anyone into making a financial transaction. Fraudsters often ask for money up-front, sometimes in exchange for nothing but promises. If someone sounds too eager for payment, we need to consider whether they are genuine.

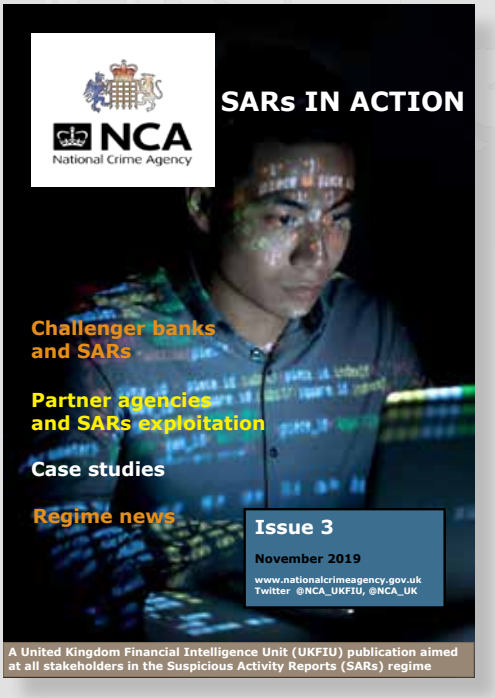
We should also all be aware that, with bank transfers, no matter how sophisticated the scam, there is no legal protection to ensure that the money can be recovered. However, if a victim falls for a scam and pays by card, it is usually possible to recover the funds.

# 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










NCA
National Crime Agency

@NCA_UKFIU

www.nca.gov.uk