



NCA

National Crime Agency

SARs IN ACTION

**Challenger banks
and SARs**

**Partner agencies
and SARs exploitation**

Case studies

Regime news

Issue 3

November 2019

www.nationalcrimeagency.gov.uk
Twitter @NCA_UKFIU, @NCA_UK

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

It is with great pleasure that I welcome you to the third edition of the UKFIU's magazine, 'SARs In Action'. Since we started these in the Spring we have had positive feedback from law enforcement agencies (LEAs), reporters, regulators and even partners overseas. If you haven't seen the first two editions (March, August) I strongly encourage you to visit the UKFIU section on the NCA website to check them out.

In this issue we focus on the use of SARs by partner agencies, for instance the NHS Counter Fraud Authority and the Environment Agency, and how they exploit and maximise the financial information to aid their investigations. We also examine challenger banks and the contributions they make to the SARs regime.

There is also a round up of news relating to the SARs regime and UKFIU engagement, as well as excellent case studies from LEAs illustrating the wide range of crimes that SARs intelligence assists in tackling.

The 2019 SARs Annual Report will be published shortly. This will show that the UKFIU received over 478,000 SARs during 2018-19, as well as over 34,000 requests for a defence against money laundering. We also identified and fast-tracked over 3,700 SARs relating to potential vulnerable persons. The report will be available via the NCA website.

CONTENTS

News round up	3
UKFIU engagement	4
Case studies	5
SARs usage by partners	6
Challenger banks	12
SAR Glossary Codes	17

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 hope that you find this magazine useful.

We'd love to hear what you think of the publication, what topics you'd like us to consider in the future and we're always open for possible articles/collaborations.

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

Issues 1 and 2 of this magazine are available on the NCA website www.nationalcrimeagency.gov.uk

Don't forget to follow us on Twitter at @NCA_UKFIU or visit www.nationalcrimeagency.gov.uk

NEWS ROUND UP

SARs Programme update

As well as the SARS IT Transformation project (see August issue of this magazine) the SARs Programme is looking at the whole regime to make it more effective and efficient. There has been much activity over the last few months to get the Programme Team in place and formally commence Programme Initiation. Over the next period the focus will be on scope, plans, governance, benefits and developing the Outline Business Case (more information in the next issue).

If you currently work within the SARs regime and wish to get involved please get in touch with the Programme Business Change Team via SARsBC@homeoffice.gov.uk

NCA to transform existing SARs IT suite based on end user feedback

In the second issue of the magazine (August 2019) we outlined the SARs IT Transformation project – a part of the SARs Programme which aims to strengthen the UK's response to money laundering and terrorism financing, as well as improving policing outcomes across all-crimes through use of the information captured in SARs. The scope of the SARs IT Transformation project includes the remit to transform the existing SARs IT suite into a stable and expandable solution and make improvements to its functionalities to ensure it is fit for the future. The UKFIU currently provides end users of SARs with a search and analysis tool as well as training in how best to exploit SARs using it.

The SARs IT Transformation team has started to engage with various end users to obtain feedback on how to improve system functionalities with the aim of further enhancing officers exploitation capabilities.

The following positive feedback was received from an officer following training on how to exploit SARs data using the current analytical tools provided by the UKFIU. This identified a second nominal linked to a subject of interest who had not been previously picked up by any other searches. The officer was able to quickly download the link analysis and share with his analyst to update their intelligence package.

The officer stated: "None of this would have been possible a few days before and [it has] saved a lot of work and also made a link we were unaware of up to that point". Subsequent feedback from the same officer reported that they had had a live job and the officer had managed to identify both the suspect and his accounts through SARs data and the tools provided by the UKFIU. The officer commented: "Prior to this it would have probably taken me a considerable amount of time to have identified the suspect, so overall [I am] very impressed with the analysis tools and training provided".

The SARs IT Transformation Project will be delivering new exploitation capabilities, training materials and assistance in their use over 2020 and 2021.

UKFIU ENGAGEMENT

UKFIU assists foreign FIU child exploitation enquiries

The UKFIU was very proactive in supplying a foreign financial intelligence unit (FIU) with valuable and timely reporting relating to child sexual exploitation. The results from enquiries conducted with financial service providers influenced a number of arrests of paedophiles as well as the disruption of paedophiles' streaming and selling online content internationally. The UKFIU received positive feedback for its support in helping the foreign FIU to apprehend individuals exploiting vulnerable children.

UKFIU engagement at private sector forum

In July the UKFIU presented at the FinCrime and FinTech Exchange Forum (an event organised by the private sector to exchange information and provide industry networking opportunities). This was the UKFIU's first engagement with this group. In attendance were representatives from challenger banks, internet payment services and a number of software IT companies involved in helping clients with solutions to manage SARs. The UKFIU's presentation was well received and it is very likely that the UKFIU will have regular engagement at this forum.

Collaboration with Law Society

In April, with collaboration with the Law Society of England & Wales, the UKFIU chaired a workshop with the intention to produce guidance and good practice products to improve the quality of solicitor DAMLs. In attendance were a number of experienced Money Laundering Reporting Officer (MLRO) solicitors, representatives from the Law Society Anti-Money Laundering Task Force and the Solicitors Regulation Authority. The constructive advice and ideas from all parties resulted in an action plan being built on phase one to build case studies with good and bad examples of solicitor DAMLs.

UKFIU leads on project

During the July Plenary Egmont meeting (the Egmont Group is a unified body of 154 financial intelligence units) FIUs agreed to a UKFIU proposal to undertake a project on the financial flows associated with online child exploitation online streaming, which will be led by the UKFIU and the Australian and Philippines FIUs. This will develop strategic intelligence, enable international tactical intelligence flows and produce indicators for the financial sector. It complements existing tactical intelligence works between the three FIUs.

Positive feedback regarding Wells Fargo presentation

In August the UKFIU visited Wells Fargo to deliver a presentation around good quality SAR reporting. The reporter's UK MLRO praised the presentation as being very engaging. Wells Fargo UK's senior leadership team and US colleagues welcome similar engagements in the future.

CASE STUDIES

Fast time support from SAR intelligence safeguards victim

A foreign national became a victim of modern slavery after being duped via a romance scam to travel to London. She managed to use her controller's phone to call the police in her country. She informed them that she believed she was being held in South London and provided details of the 'boyfriend' of the romance scam. The overseas authorities contacted their police attaché who immediately called the Modern Slavery Unit within the Metropolitan Police Service (MPS). The detective used Arena to search the Elmer database and identified a potential match for the 'boyfriend' within payment details of a SAR relating to a different male suspected of being linked to modern slavery, due to spending patterns matching red flag indicators previously shared with reporters by the UKFIU.

The officer identified and contacted the financial institution of the 'boyfriend', who were able to provide a potential new address for him. Within two hours of the victim notifying her national police, MPS officers were able to attend this new address and safeguard the victim. It further transpired that the victim was due to be moved to another address that evening and that only the 'fast time' support of the reporter meant that the MPS was able to safeguard the victim.

SARs identify offenders

Multiple SARs raised concerns about numerous suspicious payments into accounts. An LEA investigation established that an individual altered account details to divert over £100,000 in salary payments into other accounts. Once payments were received into these accounts, the funds were withdrawn as cash from ATMs. The SARs assisted in identifying offenders and recovering proceeds. Enquiries are ongoing.

SARs assist in confiscation

A number of SARs were received regarding the bank accounts of a subject in different areas of the UK. Police had received information of women being transported to a particular address in one of the areas. SARs assisted in identifying further lines of enquiry as an alert was initially raised due to third parties paying cash into the subject's account from third parties. A warrant was executed and arrests were made. The subject received a prison sentence. A confiscation order for £30,000 was secured.

SARs and partner agencies

How SAR end users exploit financial intelligence

Department for Environment, Food and Rural Affairs

Michael Hill Financial Investigation Officer

The Department for Environment, Food and Rural Affairs (Defra) consists of the core Government department, a number of executive agencies such as the Animal and Plant Health Agency (APHA) and the Rural Payments Agency (RPA) and several arms-length bodies such as the Environment Agency. Defra Investigation Services is based in the core-department and provides investigation services to APHA, RPA, the Forestry Commission England and the Veterinary Medicines Directorate and has one accredited financial investigator (AFI), around 12 investigators covering the UK and a Digital Forensic Unit (DFU).

We investigate a range of offences reported to us by our clients and we also conduct digital forensic examinations independently from across government as well as supporting the work of Defra investigators.

Generally, our investigations fall into two categories: criminal investigations, usually under the Fraud Act 2006, or breaches of the various Defra regulations which range from Forestry Commission regulations, the Veterinary Medicines regulations to the RPA regulations – in essence all regulations covering the rules governing our clients' procedures.

From the outset of every investigation the Proceeds of Crime Act 2002 (POCA) is considered; if it is believed that the subject may have made any 'criminal benefit' as a result of or in connection with their criminal conduct then we attempt to recover that benefit.

SARs are used in two primary ways. A general search is conducted regularly upon the term 'Defra' – as a proactive enquiry to identify any suspected wrongdoing by either Defra employees or partner agencies, and to identify if any 'Defra' funding is thought to be used inappropriately; we look to safeguard the valuable public funds and ensure that they are used as intended. The second way is I check that the subject of every case has no SAR which may assist the investigation into their activities.

The subjects of Defra investigations are researched to identify if the regulated sector have made any disclosures which may strengthen the intelligence case or reveal further lines of investigation. In one case the various SARs identified a pattern of offending using shell companies based overseas to disguise the origin and non-availability of funds.

We consider the full range of investigation options in all our cases to maximise the use of our resources, and SARs intelligence will enable Defra investigators to consider other investigation opportunities, such as search warrants when digital devices might be seized and subsequently analysed in-house by the DFU resulting in best evidence.

Environment Agency

Environmental Crime

The European Commission defines environmental crime as “acts that breach environmental legislation and cause significant harm or risk to the environment and human health”.

Europol has identified two primary categories of environmental crime in Europe:

- Waste crime, which covers improper disposal of waste in breach of national or international law. Waste crime is a drain on the economy and hurts legitimate business, due to waste criminals undercutting law-abiding waste companies. It cheats the taxpayer of money as it costs millions of pounds to clear up the mess the criminals leave behind.
- Wildlife crime, which covers harm to wildlife within that country, as well as the illegal wildlife trade, which is any trade in prohibited wildlife or plant material. This is not the remit of the Environment Agency.

Environmental crime also incorporates illegal resource extraction - including fishing - pollution and fraud around sustainability and carbon trading permits.

Environmental crime has also been linked to other types of serious crime, including the drugs and arms trade, human trafficking, money laundering and, according to Interpol, the funding of terrorist organisations.

Financial Investigations Team

The Environment Agency’s Financial Investigations Team sits within the National Investigations arm of the Agency’s National Enforcement Service.

The team comprises of a team manager, team leader, six AFIs, a senior accredited financial intelligence officer (AFIO) and five accredited FIOs. The team is dispersed across the country from Newcastle to Exeter.

The Financial Investigations Team covers all of England and works with local Area Crime Teams, the Environment Agency’s National Investigations Team and within the Major Investigations Rooms who tackle large scale, national waste crime or persistent offenders.

The Environment Agency has its own in-house Legal Team who work with the criminal investigation teams to take the environmental prosecutions to conclusion. The Financial Investigations Team work is largely confiscation investigations following successful convictions, some of which are ordered by the Judges, whilst others are taken on following requests from the investigation teams. The in-house Legal Team then continues to work with the AFI until the conclusion of the confiscation process.

During the 2018/19 financial year, the Environment Agency successfully obtained seven confiscation orders to the value of £2,158,516.

Environment Agency

The Agency and SARs

The Environment Agency mainly use SARs as a valuable source of intelligence finding bank account details and possible property assets to support our confiscation investigations. Relevant sanitised intelligence also aids in building the general intelligence picture for the Agency identifying linked companies and associations.

The Environment Agency does not have the same volume of SARs as our partner LEAs do. It is difficult to identify environmental offending by the movement of money due to the regular involvement of legitimate limited companies used to conceal the illegal activity or shell companies purely set up to distance individuals from the offences.

However the motivation for environmental offences, due to their nature, is almost always financial which makes them prime for POCA confiscation proceedings. The AFIOs are able to monitor SARs on a daily basis dealing with any allocated SARs, conducting keyword searches to identify SARs of possible interest and DAML SARs when they arise.

All SARs are researched against our intelligence and case management systems and relevant information converted into suitably sanitised intelligence or highlighted to the relevant AFI. Due to the nature of environmental offending, SARs have not been able to be used to identify environmental offending, although they have been used as a valuable source of intelligence.

SARs, prevention and disruption

SARs have also been used to assist in the Environment Agency's prevention and disruption (P&D) activities. Since July 2018 the P&D team in the Agency has had an AFI and AFIO assigned to them. Their task is to assist with identifying P&D opportunities through financial sources such as revisiting outstanding confiscation orders to take more money off persistent offenders, identifying and disrupting funding sources used to further criminal activity and providing current intelligence and financial profiles on individuals and companies.

With the assistance of the North East Asset Confiscation Enforcement team the P&D AFI/AFIO were successful in obtaining a £110,000.00 uplift of an order following a revisit under Section 22 of POCA.

Further information

The Financial Investigations Team will be presenting at the Serious & Organised Crime Exchange (SOCEX) conference in November 2019 which will expand on the work done on financial investigations and how the available tools are being used to help the P&D Team and the successes seen so far. If you would like to find out more about us and what we do then you contact us on finance.investigator@environment-agency.gov.uk or catch a member of the team at the SOCEX conference.

Northern Ireland Environment Agency

**John Kinkead – Intelligence Manager
Assessment Unit, Enforcement Branch**

The Assessment Unit within the Enforcement Branch, NIEA, includes two AFIOs.

On a bi-monthly basis we search SARs using a query search utilising the following words: recycling, waste, scrap metal and skip hire. We regularly find information such as new addresses and telephone numbers linked to waste offenders which assists in our intelligence development. A waste offender could be classed as an individual or business who, without waste authorisation under the Waste and Contaminated Land (NI) Order 1997, keeps, treats or disposes of controlled waste. Controlled waste is waste that is subject to legislative control in either its handling or its disposal. The types of waste covered includes domestic, commercial and industrial waste.

We have also been able to create incidents, carry out site visits and investigate unauthorised waste disposal sites from information reported via the SARs process.

Between May and July 2019 a total of 147 SARs was retrieved. Further research and development identified 39 SARs of interest involving 30 entities.

A number of SARs have been used to create intelligence documents to assist the NIEA Environmental Crime Section regarding current investigations and enforcement strategies around waste

enforcement strategies around waste crime incidents.

As part of a joint working relationship with HM Revenue & Customs, NIEA meets bi-monthly to discuss and share information regarding environmental taxes and investigations. As part of this process a number of SARs have been shared which relate to a variety of potential offences varying from money laundering, tax evasion and fraud.



NHS Counter Fraud Authority

David Guy Hall Fraud and Financial Investigation Lead

The NHS Counter Fraud Authority is increasingly using SAR enquiries more pro-actively within our investigations and a current investigation below provides a good example of the way we are working with a number of UK police forces.

We are currently investigating an estimated £1m mandate fraud believed to have been perpetrated against an NHS Trust. It appears that funds intended for a genuine NHS contractor were diverted to another company's account (subject A). It seems the bulk of the funds were transferred onto two other accounts (subjects B and C) before being dissipated further.

As the investigation has progressed and more nominals have come to light, the Arena database has been searched for any 'hits' in relation to any of the nominals, businesses or accounts involved.

A number of 'hits' have proven fruitful in building a rich intelligence picture, which identified subject A appearing in various SARs linked to potential illegal activities. This is in addition to subjects B and C appearing on hits which are linked to other potential investigations of illegal activities.

The ongoing investigation is complex. The information gleaned from the SARs thus far has been sanitised for use in the investigation. An intelligence picture is building whereby links not previously overt or obvious have been made using intelligence gathered from SARs. They have led to further enquiries being made in relation to tracing the criminal property and also assets of those involved.

The lesson is that SARs are a powerful tool in the box for those of us investigating fraud against our precious National Health Service.

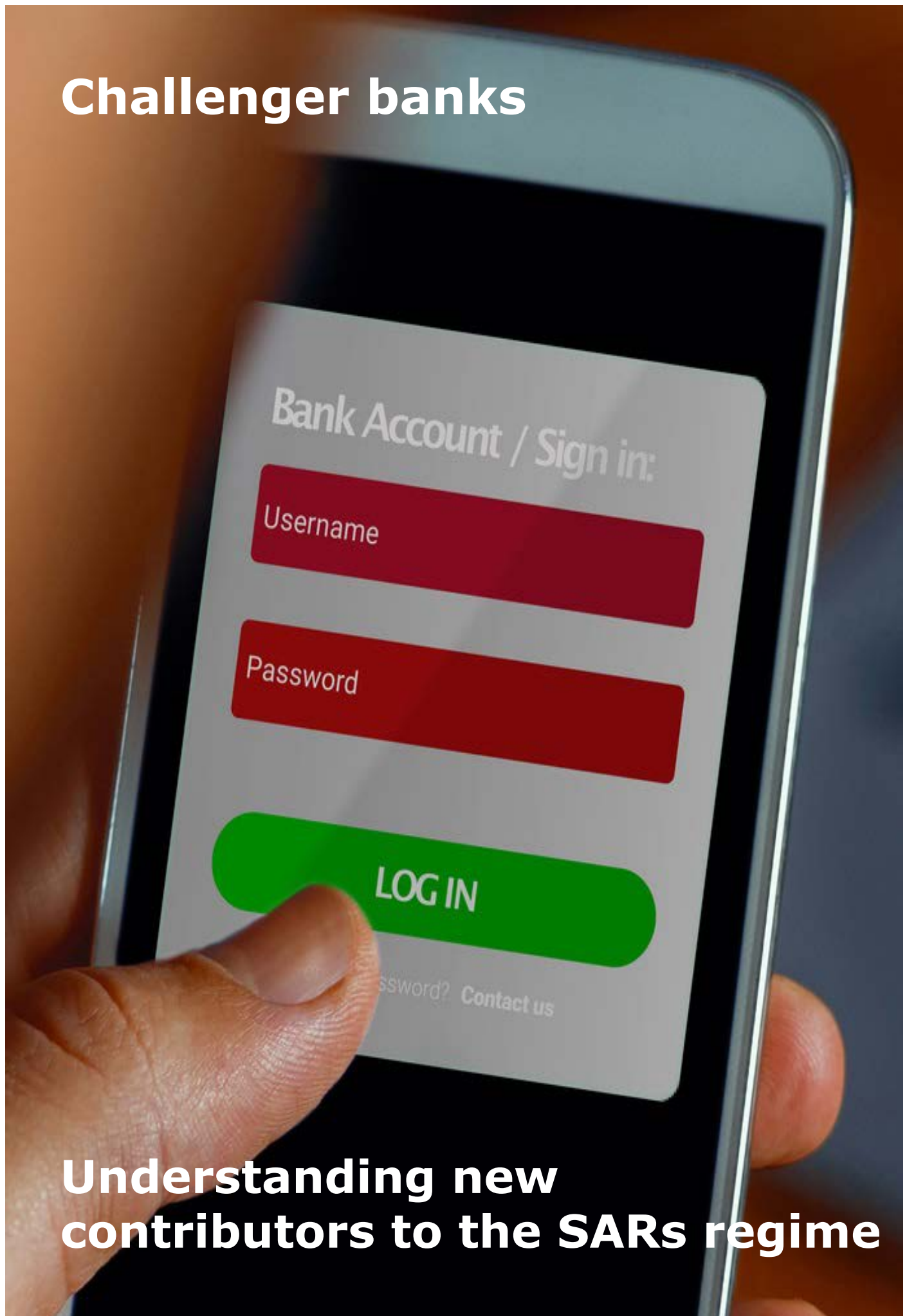
NHS fraud
Spot it. Report it.
Together we stop it.

If you hear/see anything suspicious call
0800 028 4060
Powered by Crimestoppers



Counter Fraud Authority

Challenger banks



Understanding new contributors to the SARs regime

It's challenging defining a challenger bank

As the number of choices available to banking customers in the UK has grown to include non-traditional platforms, the pool of institutions that regularly report SARs has expanded and diversified. Terms such as "FinTech", "e-wallet" and "cryptocurrency exchange" are now commonplace within the SARs regime and the terminology used to discuss these reporters can be crucial to understanding the different services that they offer.

It could be considered that for a UK-based SAR reporter to be termed a 'challenger bank', it should be a prerequisite that they hold a UK banking licence. This has perhaps become a bit less clear where emerging, often mobile-based, firms offer particular services to challenge the market, but without themselves becoming licenced banks.

Examples might include pre-paid cards, currency exchange and peer-to-peer payments. Whilst these firms are offering services that might see them compete with established banks in certain areas, without holding full banking licences enabling them to pay interest and accept deposits, technically these are not banks, but these companies are valued contributors to the SARs regime, due to the value of the financial intelligence deriving from the services they offer their customers.

A number of UK challenger banks have taken the decision not to have physical branch locations for their customers to visit. This lack of high street presence means that these companies have to utilise innovative methods for conducting their Know Your Customer (KYC) checks.

For example, video-based authentication for account holders is used by some as an alternative to account opening in-branch, which also means new financial intelligence opportunities. However, it is also important to make the distinction that not all challenger banks are purely mobile-based.

A further consideration when categorising SARs reporters is that the range of services they provide do not remain fixed. Just because a financial company does not currently hold a UK banking licence, does not mean that it never will.

When an institution obtains its banking licence, its role as a SAR reporter can change, because, for instance, the financial intelligence provided on current account users is different to that where a pre-paid card is used. Using the above understanding of what constitutes a 'challenger bank' means that it is then easier to realign definitions when circumstances change.

For those involved in the SARs regime day-to-day, it is crucial to clarify what we mean when we group reporter types. Understanding who SAR reporters are and the services they offer their customers means categorising them clearly. Much as 'challenger bank' can be a useful term to use, it is important that it is done so accurately and with consistency.

Starling Bank



Mark Savill
MLRO and Head of Compliance

I often get asked how things are different at a challenger bank as opposed to more established banking brands; to be honest the core obligations are the same for all banks, so on the face of things we are very similar. For many of the roles in the financial crime teams, relevant experience is essential and we have people with broad experience gained at other financial institutions/banks, legal firms, regulators and at least one former police officer.

Where we do differ is our use of technology, our speed of deployment and our focus on development and improvements. This makes a difference throughout the product lifecycle starting with, for example, our use of video as one of the anti-impersonation tools (all our customers are onboarded in line with the relevant rules, regulations and guidance) through to the way the fraud/anti-money laundering rules work.

We deliver these and other things by including engineers in the discussions about what we are seeking to achieve. When it comes to dealing with financial crime this means we can update and reconfigure rules in almost real time and, through our segmentation of alerts, then work the priority alerts in real time. It is also a huge advantage that we do not have multiple legacy systems, so that the information necessary for investigations and to be presented in SARs is to hand and in a form that can be easily extracted for reporting. This means that witness statements and the like are presented in a clear and easy to read manner.

We are very aware of our responsibilities to educate customers regarding fraud and financial crime. As a financial crime team we write and publish blogs on topics such as protecting businesses from fraud, authorised push payment scams, spotting fakes/avoiding fraud and account restrictions. We are also the only FinTech bank to have signed up to the Contingent Reimbursement Model Code for Authorised Push Payment frauds which means that we have the controls in place to comply with the Code, and will ensure that any victims who bank with us will get reimbursed when they have met their obligations under the Code.

We are active in many of the industry and financial crime forums and we're always seeking new ways to engage with other banks, regulators, the police and other agencies to improve the way information is shared and to learn how we can do things better.

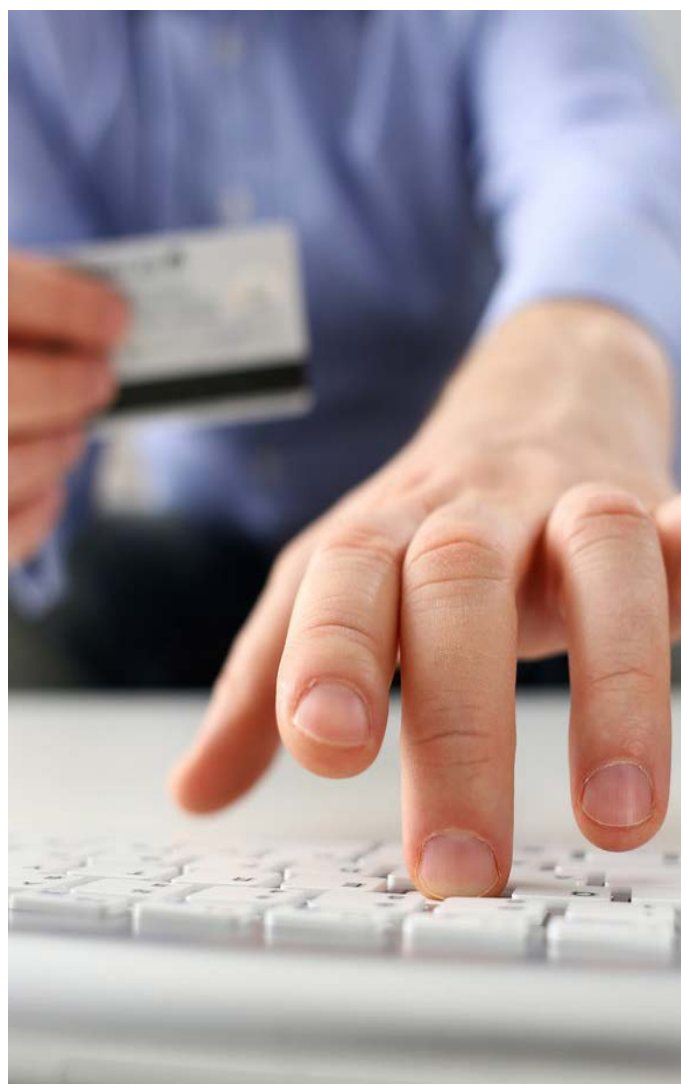
A good example is a conversation I had with a detective presenting at a conference regarding SARs and how the police use the information, as well as the difficulty that they have in dealing with SARs from across all industries – often those populating the SARs do not see how they are presented to the recipients, so sometimes extracting the relevant information can be difficult.

As a result we have briefed all our investigators on how to present SARs to make it easier for the recipients to quickly identify the key points and contact details.

With regard to investigations we are very similar to any other bank. We react to the automated transaction monitoring rules, internal SARs, intelligence information received and reviews undertaken by the risk teams. These are investigated with SARs being submitted as relevant. Where technology helps us is in the collation of the information to populate the SAR and respond promptly to any follow up questions.

It's rewarding to see the cases develop overtime with the initial SAR being followed up by the relevant authorities and action being taken based on intelligence that we have provided.

In line with our bank vision, we work really hard to prevent fraud and financial crime and, when investigating, we never forget that behind every SAR are people who have been the victims of many different crimes.



Tesco Bank



Danny Higgins
Nominated Reporting Office
Team Manager

Tesco Bank is passionate about its corporate and social responsibilities, in particular our input to preventing and detecting Financial Crime. Following the redesign of our Financial Crime and Customer Security model in 2018, we have been engaging with the NCA and other financial institutions to ensure we have positive relationships to aid the sharing of intelligence where appropriate.

Being a challenger bank in the UK market, we focus on making customer interactions with us as convenient and easy as possible. Most of our customers use our online banking or mobile apps to service their accounts and apply for products. Given this, our ongoing strategy is to continue to improve our online and mobile journeys whilst focusing on our processes and controls based on these types of customer interactions.

Tesco Banks Anti-Money Laundering, Sanctions and Countering Terrorist Financing Operational teams investigate all unusual customer behaviour/transactions to identify suspicious activity which may be indicative of money laundering or terrorist financing. Suspicions are referred to our Nominated Reporting Office which is responsible for reviewing investigations and, where appropriate, disclosing the details of these to the NCA under the SARs regime. Our approach and strategy to SARs is directly aligned to the NCA's guidance on SARs and DAML submissions to best support law enforcement.

A couple of trends we're looking at are:

- Cash deposits using Tesco stores which, for a digital bank, is one of our unique selling points. With this comes the risk of accepting the proceeds of crime into our accounts in cash so our processes and controls are designed to detect unusual activity and to record the source of these funds to aid investigations.
- Online gambling activity and syndicates using spread/match betting. We're sharing intelligence with the Gambling Commission to improve detection rates of where we believe the activity to be suspicious and in turn improve the quality of disclosures to the NCA.

We focus our resources on those areas which pose most risk and/or that we can make the biggest impact under the Financial Conduct Authority's recommended risk based approaches.

New SAR glossary codes

The use of glossary codes is considered good practice. They are crucial for enabling the UKFIU and wider law enforcement to conduct analysis to identify money laundering trends, high risk cases for development and take immediate action where necessary. They also enable the production of feedback to reporters on trends and patterns identified in SARs. New codes introduced in November 2019 are:

XXGVTXX - do you require a defence under POCA ('consent')? Use SAR glossary code XXS99XX and, if submitting via SAR Online, tick the 'consent' box. For requests for a defence under the Terrorism Act 2000 submit under 'Terrorism' and tick the consent box.

Also use code XXGVTXX in any SAR relating to suspected money laundering where the value is £3,000 or less and you are unaware of any existing law enforcement interest at the time of reporting. The introduction of this code is to assist with the UKFIU DAML triage processes and the early identification of key-risk areas and asset recovery opportunities.

XXVICTXX - use for any cases where the reporter is submitting a SAR and considers that the purpose of the activity in question is to return money to a victim of crime. In any case where you suspect a criminal offence other than money laundering we advise you to report the activity to your local police force in the normal way.

XXMSHTXX - use in any SAR relating to modern slavery/human trafficking. A victim of MSHT should always be considered to be a vulnerable person so in all MSHT-related SARs it is also normal to additionally include the vulnerable person code (for adults XXV2XX, for child victims [under 18] XXV3XX). There are significant overlaps between MSHT and organised immigration crime (OIC); consequently OIC and MSHT SARs are often connected so it is acceptable to use both codes together.

XXILTXX - use if you suspect that money laundering is taking place as a result of illegal lotteries. It is an offence under the Gambling Act 2005 to facilitate or promote a lottery unless the operator holds an operating licence. The profits from an illegal lottery may also be considered criminal property under POCA and therefore the operator may have committed a money laundering offence. It is not an offence to participate in an illegal lottery.

XXVAXX - 'virtual assets' is an all-encompassing term including virtual currencies, cryptocurrencies and digital currencies, but also covers that fact that anything can be tokenised as an asset and transferred on a blockchain or other digital peer-to-peer format. The use of virtual assets/virtual currencies/cryptocurrencies/digital currencies is not illegal. This code relates to where there is a suspicion that virtual assets are being used to facilitate money laundering. The visibility of virtual assets in isolation should not automatically suggest that a SAR is required.

Previous issues of the magazine are available from the NCA website

www.nationalcrimeagency.gov.uk


NCA SARs IN ACTION
National Crime Agency

The life of a SAR


Every step from submission to law enforcement outcome

The UKFIU's business critical teams

Case studies

Regime news

Issue 2
August 2019
www.nationalcrimeagency.gov.uk
Twitter @NCA_UKFIU, @NCA_UK


NCA SARs IN ACTION
National Crime Agency

Safeguarding the vulnerable

Exploiting SARs intelligence to protect those most at risk

Key questions for law enforcement and reporters

Case studies

UKFIU news

Issue 1
March 2019
www.nationalcrimeagency.gov.uk
Twitter @NCA_UKFIU, @NCA_UK

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

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