NCA
National Crime Agency

SARs IN ACTION

Issue 4 - March 2020

@NCA_UKFIU

www.nca.gov.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

In this fourth issue of the UKFIU magazine we focus on the world of financial technologies (fintech) and virtual assets: what they are, how they work and the subsequent complexities faced by law enforcement.

We also shine the spotlight on the important work being done by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) which aims to bolster the UK's anti-money laundering (AML) supervisory regime.

The complexities surrounding Defence Against Money Laundering (DAML) SARs submitted in relation to potential suicide risks, and the areas in which the UKFIU finds itself providing operational support as a result, is also examined particularly in relation to our priorities.

As per previous issues, there is also plenty inside this edition on the UKFIU's engagement with partners, particularly our international counterparts, and also information on three new SAR working groups which the UKFIU has hosted recently, catering for Payment Service Providers, E-money, Fincrime, Fintech Financial Services; cryptocurrency and challenger banks (see the previous magazine issue for more on the latter sector).

CONTENTS

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**

Previous issues 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 IT Transformation - update from the project team

What is the SARs IT Transformation project?
The project will transform the SARs IT systems used by key stakeholders. It is one work stream within the Home Office-led SARs Programme which aims to reform the SARs regime. It will support the Programme in achieving key outcomes of protecting the regulated sector from exploitation for money laundering and terrorist financing and provide improved capabilities for targeted disruptions.

What is the structure of the project?
The project has been split into six stages. Stage 1 related to internal NCA infrastructure while stage 2 provides the UKFIU with a new tactical search tool. Stages 3 to 6 cover the majority of work for the project and will deliver: a single solution for law enforcement end users, developing a new online reporting portal, providing the UKFIU with a transformed SARs system, and replacing the bulk SARs reporting system.

What have we done so far?
We completed stage 1 last year and have nearly finished stage 2. We have undertaken significant amounts of design and development work. We also started a series of engagement sessions with partner law enforcement agencies (LEAs), held change impact assessments and commenced development of a training package. High level technical design work and engagement has also started on stages 4, 5 and 6.

What's going to happen in 2020?
We will do a first stage 3 release of the new LEA end user system in February. This will mainly be a technical proof of concept with LEA users involved in testing. Following this, we aim to do a second and third release during the summer. For stages 4, 5 and 6, we will finish the high level designs, followed by two releases for the stage 4 online reporting system - also expected during the summer. In addition, the team will start development work on stages 5 and 6 in the spring. The team will keep you informed of progress of this exciting project on a regular basis.

UKFIU ENGAGEMENT

Closer working with Pakistan colleagues

In October 2019 the Head of the UKFIU, accompanied by the NCA's International Corruption Unit and the NCA International Team, visited the Pakistan Financial Intelligence Unit, the Federal Monitoring Unit (FMU) in Karachi, following on from the signing of a Memorandum of Understanding in London in 2019. The FIUs agreed to focus on international corrupt money flows and to undertake joint analysis. There were meetings with Pakistan LEAs, regulators and the private sector to discuss the introduction of a public–private information exchange in Pakistan. It is hoped that this new relationship with the FMU will allow for the proactive identification of illicit money flows between the two countries to complement reactive asset recovery work.

Manila conference

In November 2019 UKFIU senior manager Martin Cox presented at the fifth counter terrorism funding summit in Manila. Martin spoke about a joint project the UKFIU is leading on with the Australian and Philippines FIUs around financial flows associated with online child exploitation streaming (see last issue for details).

Liaison with Argentinian and Kosovan FIUs

In September 2019 the UKFIU hosted the chair of the Egmont Group (the coordinating body for the international group of FIUs) and president of the Argentinian FIU, Mariano Federici, in London. The UKFIU presented on analytical work, IT and international engagement. On a separate occasion the UKFIU also delivered a presentation on the unit's functions and domestic and international engagement to representatives of the Kosovan FIU, Kosovan prosecutors and LEA representatives.

UKFIU involvement in slavery and trafficking workshops

In September 2019 the UKFIU supported modern slavery and human trafficking (MSHT) workshops targeting SAR reporters from the legal and accountancy sectors, as well as legal and accountancy supervisors. The workshop focused on raising awareness of MSHT, consultation on developing red flag indicators and a plan to communicate key MSHT SAR messages throughout the legal and accountancy AML community.

UKFIU ENGAGEMENT

New SAR working groups hosted by UKFIU

During the winter the UKFIU hosted a number of new SAR working groups. The very first challenger bank and cryptocurrency groups were formed during November 2019, and in January 2020 the first meeting of the Payment Service Providers, E-money, Fincrime, Fintech Financial Services group was held. The groups were attended by representatives who regularly submit SARs and DAMLs. All the attendees agreed operating protocols which aim to help the continuous improvement of SARs quality. The groups have the ambition to help the UKFIU make the SARs regime as effective and as efficient as possible and elected chairpersons to encourage the sharing of good AML practices. Discussions were also held on indicators of suspicion for virtual asset service providers. The UKFIU outlined the key features of the 2019 SARs Annual Report and provided key SAR guidance updates.

RBS Edinburgh visit

In October 2019, as part of its regular engagement with the banking sector, the UKFIU visited RBS at its Edinburgh office. Over two days UKFIU officers made numerous presentations to RBS staff involved in the SAR process. Guidance and best practice was shared regarding making good quality SARs and DAMLs.

Feedback was very complimentary of the UKFIU's input and the delivery of the *SARs in Action* magazine was very well received. Ainslie Pettie, Deputy Nominated Officer in the FIU at RBS, said: "the sessions were great and hugely informative for our investigative staff."

Charities event with partners

In October 2019 the UKFIU supported a joint National Terrorist Finance Intelligence Unit (NTFIU)/Charity Commission event to inform charities operating in high risk areas of risks posed by terrorist groups known to use charities to finance and support terrorist activities, in order to improve understanding and risk management within the charity sector. The UKFIU occupied an all-day stall where it informed attendees of the UKFIU's work and made them aware of the SARs regime as a potential reporting mechanism when they suspect potential terrorist finance while conducting their charitable work.

UKFIU presence at counter fraud forum

In October 2019 the UKFIU attended the Counter Fraud Banking Forum organised by HMRC. The UKFIU sat on a panel to help address questions relating to tax evasion SARs. Also in discussion were red flag indicators for organised labour fraud, payroll company fraud and mini umbrella companies exploiting VAT and employment allowances. The intention is to share those indicators with other SAR sectors to help shape their construction of reasons for suspicion in their SARs. HMRC is using DAMLs to help inform their tactics to recover stolen money.

A digital presence

Law enforcement needs to respond and adapt to the changing risks and opportunities of the digital world. In line with the National Police Chief Council 2025 vision on this, the UKFIU is preparing to adapt and promote its online presence.

To do so the UKFIU will look to include more digital tools such as a UKFIU app, webinars, podcasts and a social media presence. This will contribute to delivering a smarter approach to fighting crime, in line with the NCA's priorities of reducing harm and protecting the integrity of the UK economy.

The podcasts initiative will look at building a series of themes on specific subjects relating to SARs; the UKFIU app will focus on improving the quality of SARs, providing a step-by-step guide on how to submit SARs with links to guidance, regulators, advice. In essence a one stop shop for users to view SAR related content.

Due to popular feedback from previous webinar events we are developing tools to allow regular sessions of such events, geared specifically towards certain sectors, themes and UKFIU products. These will allow users and the UKFIU to have live engagements at their desks and the ability to playback the webinars to capture any points previously missed.

The UKFIU are in the developmental stages of researching these digital tools and there will be future updates once we are further down the implementation stage.

Suicide and SARs
An operational response

Suicide affects families, friends, colleagues and communities and can have lasting effects on those left behind. For every suicide, there are many others who attempt it. The World Health Organisation identifies risk-factors associated with suicide as mental health disorders, particularly depression, and alcohol related disorders. Other risks can manifest impulsively, often in crisis, with a breakdown in the ability to deal with life stresses, including chronic pain, illness, relationship and financial problems.

In some of these potential suicide risks, particularly financial problems and life-limiting health scenarios, the UKFIU finds itself providing operational support across a range of linked issues. Two areas of consideration are DAML SARs and the arranging of payments to facilitate end of life clinic services overseas.

The submission of a DAML SAR triggers 'the initial notice period'; this effectively freezes a subject's ability to access funds for up to seven working days. The UKFIU is often contacted by reporters seeking operational support to help deal with situations where members of the public threaten to commit suicide as a result of an initial freeze. This can develop quickly, with subjects communicating threats to the reporter by phone or online. Whilst a simple interpretation could be that any threat to commit suicide may be interpreted as a form of emotional blackmail to release the freeze, in reality, the potential risk is all too real.

The UKFIU's priority is to assess the reporter's information using the National Decision Making Model, ensuring that immediate steps to mitigate harm to the subject, the reporter and the general public are expedited and ensuring an emergency response by law enforcement is instigated where appropriate.

The UKFIU was approached where a client with a life-limiting condition asked a bank to arrange payments on their behalf to an end-of-life clinic overseas. The reporter raised that by authorising the payment, would the bank become involved in assisting a suicide or inadvertently committing a criminal offence?

Whilst committing suicide or attempting to is not a criminal offence, encouraging or assisting someone to commit or attempt suicide is (e.g. encouraging a suicide may include online trolling or bullying resulting in suicide). In the bank/client scenario, the keeping or recording of any conversations, communications or discussions would be a helpful starting point to help understand the nature of the request made. It may also be prudent to escalate or inform your legal department.

The Crown Prosecution Service has a policy for prosecutors regarding cases of encouraging or assisting suicide. The Director of Public Prosecutions is required to provide guidance, outlining the facts/circumstances that would be taken into account in deciding whether to consent to a prosecution. This guidance would help inform legal departments in terms of the legal landscape in this area.

If a client has asked you to make a payment to an end-of-life clinic overseas then you should flag this to your legal department with background information volunteered by the client. Where you believe someone's life may be in imminent danger or that a danger is posed to others you should always first consider an immediate response from the emergency services.

OPBAS

Kate Carpenter
Senior Associate
Office for Professional Body Anti-Money Laundering Supervision (OPBAS)
OPBAS@fca.org.uk

The OPBAS at the Financial Conduct Authority (FCA) exists to strengthen the UK's AML supervisory regime and ensure professional body supervisors (PBSs) provide consistently high standards of AML supervision.

OPBAS supervises 25 legal and accountancy PBSs and has two key objectives:

- To improve the consistency of PBS AML supervision.
- To facilitate collaboration and increase information and intelligence sharing between PBSs, statutory AML supervisors (HMRC, the FCA and the Gambling Commission) and LEAs.

To deliver our second objective we established two new Intelligence Sharing Expert Working Groups (ISEWGs) with the National Economic Crime Centre (NECC). The ISEWGs are loosely based on the existing Joint Money Laundering Intelligence Taskforce (JMLIT) model used by the banks and are globally pioneering in public-private intelligence sharing forums for the legal and accountancy professions. There is an ISEWG for each sector with members consisting of PBSs, NECC, HMRC, the FCA and OPBAS. Both ISEWGs have agreed published Terms of Reference.

The ISEWGs have two distinct functions: strategic and tactical. The strategic element involves discussion and consideration by all members on the high-level threats and emerging risks for their sector. Members give anonymised real-life case examples of where they have found a specific money laundering risk identified from their supervisory work, along with mitigating actions. The strategic sessions have also seen the development of a drafting group of volunteer PBS members who receive JMLIT alerts and redraft them to make them relevant to their sector.

The tactical element is a confidential disclosure meeting between members, under the relevant legal gateways, relating to a live investigation. To participate in an ISEWG tactical session, members have agreed to be security vetted and have secure email addresses for correspondence. As part of the terms of reference, members also commit to feeding back anonymously to the wider membership in the next strategic session on any overarching themes from tactical sessions. This enables a better understanding of inherent money laundering threats to their sector.

The ISEWGs have been in operation for just over a year and have delivered a significant improvement in the collaborative working relationships, engagement and trust between PBSs, statutory AML supervisors and law enforcement. One of the main benefits from the ISEWGs has been a more consistent flow of high-quality information and intelligence sharing in both sectors and increased SARs reporting. We expect the impact of the ISEWGs to continue to grow throughout 2020 as the work of the groups is adopted by and embedded in the member organisations.

Comments from ISEWG members

"The tactical intelligence sharing aspect of the ISEWG is extremely beneficial; it allows us to have meaningful conversations with law enforcement to understand the investigation and provide relevant information"
Wesley Walsh, Manager, AML (Association of Certified Chartered Accountants)

"HMRC is pleased to be part of the ISEWGs. The groups directly contribute to how we tackle illicit finance in the UK, creating a way for AML supervisors to have a continuous conversation about risk trends and more detailed disclosure about those that pose an increased threat of money laundering or terrorist financing"
Louise McDonald, Assistant Director, Illicit Finances Policy (HMRC)

"The ISEWGs have led to improved engagement with the regulated and/or supervisory sector. The NECC's Enabler Practitioner Group is now able to exchange relevant information on overlapping priorities with vetted staff from professional bodies. This is resulting in relevant referrals from the regulated sector to the NECC which may lead to potential disruptions"
Kevin Soobrayen, Threat Lead for Money Laundering, Bribery and Corruption (NECC)

"The Legal Sector Affinity Group (LSAG) welcomes the creation of the ISEWGs to support our members' supervision by improving information sharing with law enforcement"
Ian Messer, Chair of the LSAG

ISEWG
INTELLIGENCE SHARING EXPERT WORKING GROUPS

Modulr

Mike Venn
Head of Risk & Compliance for Modulr

Modulr are a payments service for businesses, regulated as an electronic money institution with the FCA

The world of crypto remains an area of significant commercial opportunity in terms of value generated from investments as well as a future mechanism to trade and make payments (often described as a value transfer). However, the perceived complexity associated with it can bring misunderstandings of the risks but also opportunities for criminals to exploit. In recognising its increasing importance and movement into the mainstream there have been developments in the regulatory frameworks that govern it, significantly the 5th Money Laundering Directive (5MLD), reflected in the FCA regulatory guidance which came into effect in January 2020.

Globally it comes as no surprise that the jurisdictions operating under more effective regulatory frameworks are assessed as having a lower level of risk associated with crypto firms operating and based there. The introduction of these requirements in the UK pushes crypto payment service providers to adopt similar standards and controls as their non-crypto counterparts.

Modulr's move into the market is at an early stage so our approach continues to evolve through experience and partnering with businesses that have capabilities and expertise. However, many of the actions we take remain consistent in how we on-board any new customer, assessing their understanding of risk and how they have developed a control environment to mitigate these risks.

Working closely with our sales and development teams to ensure we also understand the commercial rationale and how this links to our product continues to be a key area of insight. A particular challenge can be collaborating with businesses that are newly formed and therefore have limited information or operating history to assess against.

As part of this these businesses are also often looking to innovate and evolve their model which means we need to maintain open lines of communication to ensure that our understanding of the business and associated risks is in place. The movement towards greater regulation is positive in this sense with a clear opportunity to assess crypto businesses plans to assess and comply with the relevant regulatory frameworks. Whilst a positive first step, inevitably regulation will need to develop and evolve to reflect the experiences of the market.

More generally research and analysis has been undertaken in an attempt to ascertain the level of criminality associated with crypto – there remains a general perception that crypto is regularly being used to drive organised crime and terrorism but there is limited evidence to support this. Elliptic (a tech and consultancy provider in the crypto/AML space) has published articles and undertaken analysis on the subject and the risk.

Whilst recognising that more is needed to be done, they point to the fact that when considering the value of crypto being processed on the dark web to the value of $829m, this equates to 0.5% of the value of crypto. A pattern that also appears to be continuing is that the majority of crypto is used more as an investment than to acquire things at this time, limiting the volume of this type of activity.

What isn't disputed is that many of the traditional criminal opportunities can be adapted and applied to the crypto environment, with criminals exploiting confusion, complexity and uncertainty. This is particularly the case in relation to 'investment scams' with a number of high-profile cases being reported and investigated recently.

Ironically, until crypto becomes more mainstream, particularly as a payment tool, the opportunities to use it to support wide scale money laundering or terrorist financing remains limited. Unstable valuations as well as data security risks (as well as the need to use technology to manage, which can become more traceable) continue to be reasons that both illicit and legitimate fund holders are cautious. Key areas of concern remain the opportunities for sanctions evasion or the wide scale adoption of the sector by nation states; the opportunity to use this at scale remains hypothetical but continues to be high on the agenda of those assessing the risks associated with crypto.

Selecting the right parameters in terms of cryptocurrency/exchanges and controls can ensure that crypto is aligned in terms of risk with other payment strategies and a significant improvement on cash. Privacy and concealment remain the goal of those looking to abuse the system. Many of the tools now in place introduce high levels of traceability that mitigate this and can act as a key deterrent. Risk assessment of exchanges and currencies particularly in relation to privacy is key for businesses operating in this area.

Blockchain technology is essentially the mechanism that enables the exchange of crypto assets in a secure way. Blockchain is also a form of Distributed Ledger Technologies (DLT - a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time), and it is through this that monitoring drives greater transparency and investigative opportunities.

Its use is primarily as an investment strategy, buying it in the hope that it will increase in value as its use and demand increases. The exploitation of this as a mechanism for criminality will in many respects be linked to its adoption as a mainstream currency, with more stable value and greater security.

FinTech Scotland

Nicola Anderson
Strategic Development Director

FinTech Scotland has been established to secure Scotland as a top global fintech centre, bringing together Scotland's financial sector, public sector, consumer groups, academia and innovators to enable collaboration and encourage economic/social changes.

New technologies enable greater flexibility and are helping create new platforms that are becoming mainstream for Millennials and Generation Z.

This change is also prevalent in financial services. New technologies are transforming this industry. Online banking introduced 24-7 access to banking services and 2019 statistics show that approximately 75% of the UK population regularly banks online. Further analysis shows that 64% of individuals between 15-34 access banking services via their smartphone.

The growing opportunities offered by new technologies in financial services have led to the development of a vibrant 'fintech' movement, with reports suggesting that there are over 1,600 fintech firms in the UK; estimates suggest this will more than double by 2030.

'Fintech' – shorthand for 'financial technology' – is a broad term, but one that can generally be understood to mean technology utilised to create new ways of providing financial services. The emergence of digital-only banks and the way that traditional banking institutions have promoted their own online/app-based banking processes, highlights the extent to which fintech is a part of current customers' banking experience.

Open Banking

Regulation has played an important role in the changing landscape of financial services. Open Banking, a government led change through the work of the Competition and Markets Authority (CMA), seeks to drive change and competition in the retail banking sector.

The change has enabled an appropriate framework for authorised third parties to access information from consumers' current accounts. Access is granted with the consumer's consent and has enabled innovators to develop a range of fintech solutions that provide consumers with a greater insight and broader range of products.

Many believe that Open Banking and the ability to access this type of current account data has the ability to significantly change the way people engage with money. Open Banking Ltd, established by the CMA to deliver Open Banking, describes it as "the future of money, where [customers are] in control."

Open Banking works through Application Programme Interface (API) software. API allows connectivity between banks and other third parties such as personal finance management apps to access the customer's current account, after the customer has granted permission and consent to access the data.

Following consented access fintechs use data analytics and machine learning to analyse income and expenditure to provide accurate and specific insights. Among other things this analysis can also be used in assessing affordability for a loan or mortgage, to helping improve approaches to budgeting, providing insights on the use of cash, debit card and contactless payments.

Fintechs are working with this type of data/analysis to address questions such as proving online/digital identity, over-indebtedness and problem debt, changing circumstances and spending behaviours. This has the potential to significantly change financial services and address difficult and complex issues such as Know Your Customer (KYC), AML, efficient transaction monitoring and financial inclusion.

Fintech and the growing capabilities around information sharing will help address some of the recommendations set out by the Financial Action Task Force (FATF). This is an emerging market and starting to identify as 'RegTech' – technology that can help regulatory oversight and compliance.

Cryptoassets

Cryptoassets is the broad term used to describe cryptocurrencies (e.g. Bitcoin) or other digital value tokens. They are digital or virtual and are supported by DLT, a database that records assets (information), run over a distributed network operating across different locations and networks. DLT's aim is to offer transparency.

The UK Government established a Cryptoassets Taskforce in 2018; the Taskforce published its final report in October 2018, including the underlying technology, the associated risks, potential benefits and a way forward with respect to regulation in the UK.

The report sets out three broad types of cryptoassets and typical uses which help establish a framework for considering the impact, potential risks and need for regulation. The Taskforce outlined the need for action to mitigate the risks for consumer harm, prevent the use of cryptoassets for illicit activity and guard against threats to financial stability that could emerge.

From January 2020 the FCA will be the UK supervisor for cryptoasset businesses in respect of AML and counter terrorist financing, under amended Money Laundering Regulations (MLRs). The FCA has specified a range of cryptoasset activities captured under the new regime and businesses conducting these activities will be required to comply with the MLRs.

The businesses include existing financial institutions that offer the option to convert cryptoassets to fiat (government issued currency) or accept cryptoassets as collateral against a loan or purchase. The regime will also apply to new businesses and developing business models such as peer-to-peer providers, digital wallet providers offering crypto services such as exchange or custodian services, cryptoasset ATMs and issuers of cryptoassets. The FCA has signposted firms to existing resources to help build an understanding of managing financial crime risks.

A law enforcement overview

Craig Gleeson
Senior Officer
National Economic Crime Centre (NECC)

The regulation of cryptocurrencies is developing at pace as, across the world, authorities react to the emerging threat posed by criminals using new payment methods to conceal and launder the proceeds of their crimes.

The new 5MLD regulations coming into effect in January 2020 aim to tackle the risks linked to cryptocurrencies and bring exchange platforms and custodian wallet providers within its scope. These two categories will soon become 'reporting entities' under the new legislation. This means they will be required to conduct strong customer due diligence (CDD) much like traditional financial institutions and report suspicious transactions to the competent financial intelligence unit.

Craig Gleeson of the NCA's NECC provided an insight into some of the potential consequences of these changes in AML and counter-terrorist financing (CTF) legislation from a law enforcement perspective.

"For law enforcement, exchanges are the point of attack," said Craig. "Strong CDD and KYC checks will help officers further their investigations and detect and pursue the criminals using Virtual Asset Service Providers (VASPs) to conceal and launder the proceeds of their crimes. It may well also result in some individuals being deterred from applying for accounts in the first instance and/or an increase in the number of accounts being refused."

While the introduction of the new regulations may seem like a necessary and logical evolution of AML/CTF requirements, and in theory they will introduce consistency and set a standard for KYC and CDD checks, the increased transparency of the players involved and the transactions may further push criminals to interact with entities less likely to comply with the regulations.

"There is likely to be a dramatic increase in the detection and reporting of suspicious activity when exchanges and wallet providers become regulated. Since they will be required to implement robust CDD and transaction monitoring, the new reporting entities will be better placed to identify and investigate concerns and potential suspicious activity. As they identify more risks and suspicions, it is to be expected that they will submit more SARs," said Craig.

The main criminal use of cryptocurrencies is as a method of payment for illicit commodities and services online, particularly on the dark web. The media has, however, highlighted the lack of anonymity in such transactions and there has been a growing uptake and development of privacy-focused cryptocurrencies.

"Dark web marketplaces have diversified to accept payment in cryptocurrencies," Craig explained. "These privacy-focused cryptocurrencies use encryption technology to prevent law enforcement from monitoring and tracing transactions, and criminals are increasingly aware of the need to use mixing and tumbling services to anonymise transactions. The use of privacy cryptocurrencies has been observed in ransomware attacks where payment was demanded in one crypocurrency then exchanged for another, preventing the funds from being traced."

Child Sexual Abuse and Exploitation (CSAE) websites on the dark web have been seen offering CSAE material for payment in cryptocurrency. This is also observed with other high-risk commodities available on dark web marketplaces such as firearms.

An increase in cryptocurrency use to facilitate criminal activity outside of online marketplaces is being observed, however, as traditional crime is adapting to embrace cryptocurrencies. In several recent kidnap cases, ransom has been demanded in cryptocurrency, one of these involving a demand for €9m.

The ease with which global transactions can be carried out with cryptocurrency facilitates the exchange of goods and services between criminals operating in different countries and jurisdictions, and this applies to criminals operating both on and offline wishing to transact anonymously with each other.

Coinbase

Iggy Azad
Senior Investigator

Coinbase is a digital currency exchange founded in 2012, predominantly based in California but with offices in Europe. Coinbase brokers the exchange of currencies such as Bitcoin and Ethereum as well as other cryptocurrencies, offering their customers a variety of products in which to buy, sell and send cryptocurrency. It also offers trading accounts to professionals as well as the storage of crypto assets and payment processing in cryptocurrency.

Staff at Coinbase are required to be aware of the money laundering regulations and other industry wide regulations due to Coinbase being fully regulated in the US; as such, all staff, irrespective of their location, must undertake AML training, especially as being a global company means that staff may work on projects across jurisdictions. This enables them to be vigilante to potential criminality such as fraud and money laundering. They are also trained on a wide range of areas from the processes of setting up accounts, case studies (from real life scenarios provided and a multitude of different cases from money laundering to the dark web), AML training and SARs. Staff regularly attend conferences and reach appropriate industry levels required for commercial and corporate lending and politically exposed person training.

"The systems that we have in place, such as the inbuilt transaction monitoring system (TMS), allow us to monitor every transaction on every account," said Iggy.

"There is a setup of alerts which monitor keywords we have set up, such as references to the darknet, blacklisted addresses and sanctioned countries. Once alerted these are reviewed and investigated further if required.

"As well as having staff trained to process cryptocurrency and to review transactions and irregularities, Coinbase needs to be aware of its customers signing up to our packages. In addition to having legitimate customers or those requiring our services, there are also obviously those who wish to potentially commit fraud or money laundering. On signing up with us the customer must provide photo ID, proof of address and a date of birth, plus further checks are done on government websites as well as using text and photo matches."

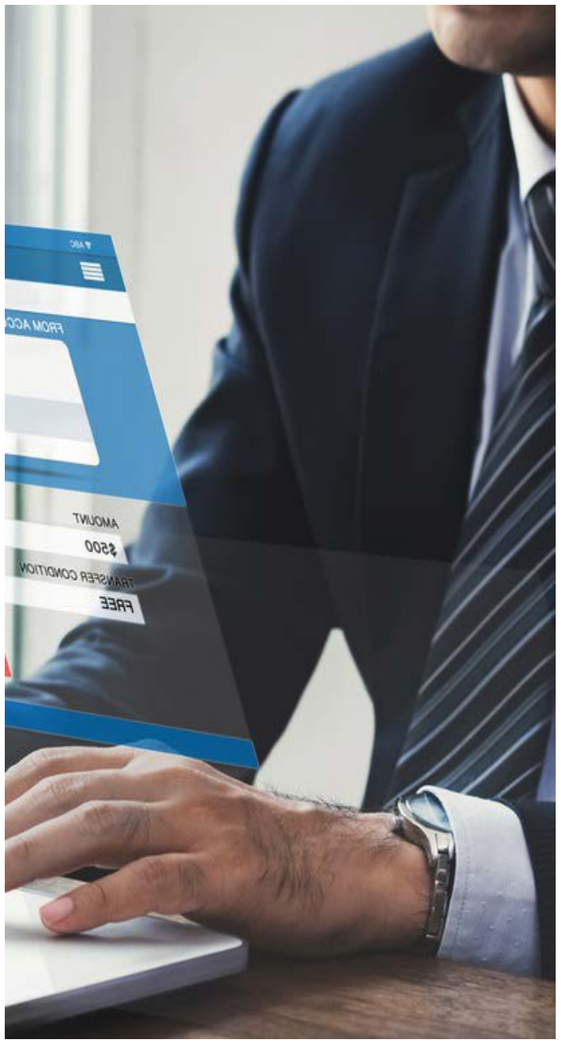
One of the key areas of criminality identified by Iggy is money mules, where teenagers (who are recruited via social media groups and chat messaging groups and may be vulnerable to such approaches) within certain postcodes are being duped/bullied/groomed into opening accounts by criminals for money laundering purposes.

The systems that Coinbase has in place can spot such trends via its KYC processes which can identify teenagers creating accounts which enables Coinbase to ask further questions and to do more background checks.

"Another big area of concern relating to key trends is social engineering," said Iggy. "This is where customers are being scammed into signing up to what they believe are cryptocurrency providers, believing them to be genuine websites, so that they are tricked into inputting their details. In actual fact the criminals behind the websites are stealing their details and using these for identity theft and for creating accounts in their names for money laundering. This is not immediately identifiable as genuine customers are creating accounts. The victims need to call their banks immediately to stop transactions."

With these systems and processes in place, as well as staff training, Coinbase looks to combat any irregular transactions and potential fraudulent accounts. This includes CDD in which extra checks, such as phone calls to new customers, are used to further verify details. The keyword alerts that are identified by the system are investigated by staff, where transactions are reviewed and additional questions can be raised regarding the funds. Accounts can be potentially frozen/closed dependent on the situation. This then enables Coinbase to prepare an internal SAR which is then reviewed before submission to the NCA.

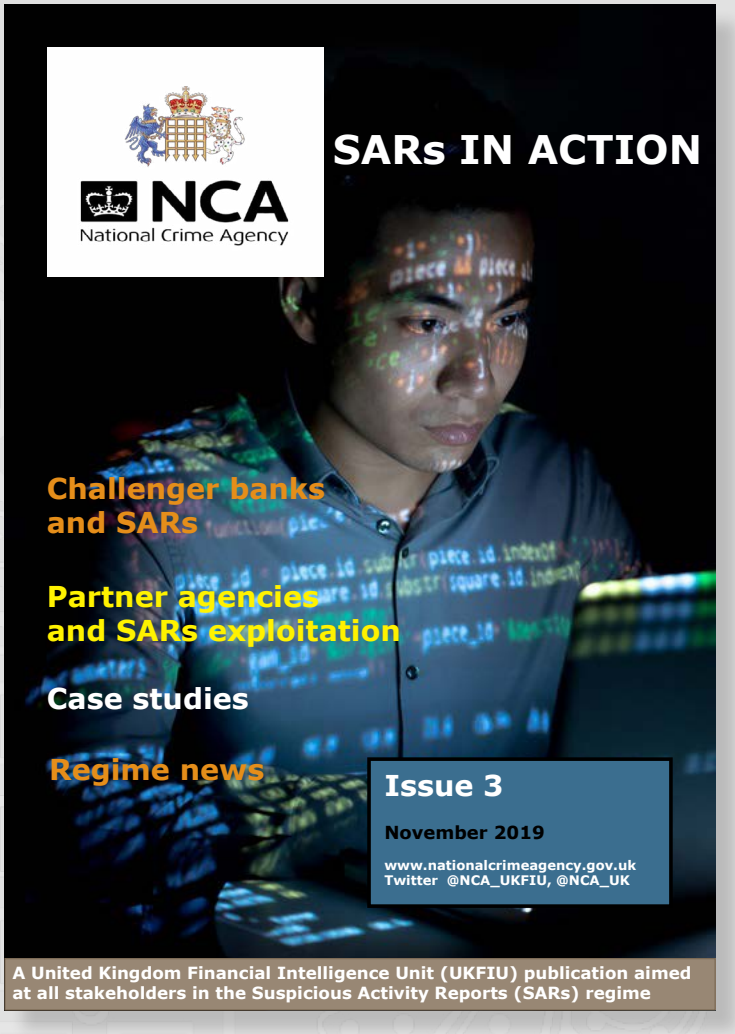
"The new 5MLD regulations came into effect in January 2020 and we are making sure we are fully prepared for this," said Iggy. "5MLD will require all customers whether crypto-to-crypto, fiat-to-crypto or custodial wallet only, to complete full KYC and identity verification. Currently we require all customers who have access to fiat payment methods, to complete full KYC and identity verification. Therefore, this requirement is being rolled out to our customers. So apart from a few administration changes this should not impact on our business too heavily."

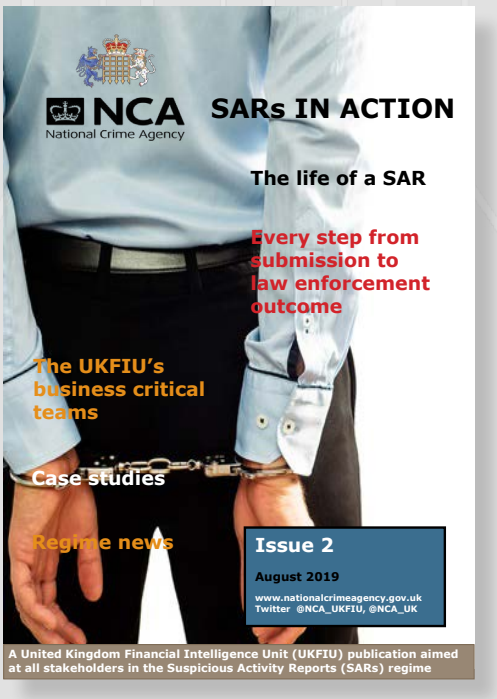


Missed an issue?

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