

SIA

SARs IN ACTION
MAGAZINE



UKFIU
UK Financial Intelligence Unit

Virtual Squatting Cell

Page 15

Professional Enablers

Cross System Professional Enablers Strategy

Page 3



The Links Between Fraud and Other Serious and Organised Crime Threats

Page 9



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



Message from the head of the UKFIU



Vince O'Brien Deputy Director

Hello and welcome to the 27th issue of the UKFIU's magazine SARs in Action.

In this issue we take a closer look at professional enablers as the National Economic Crime Centre introduces the recently launched cross system professional

enablers strategy, establishing a new framework to respond to the threat and setting out specific actions the system will take to combat it.

Also included in this issue are case studies involving professional enablers and the services they offered to enable criminality and how SAR intelligence assisted law enforcement investigations in these cases.

We look at the NCA National Assessment Centre's analysis on the links between fraud and other serious organised crime threats, which shows that fraud remains the most common crime type in England and Wales, accounting for an estimated 38% of crime in the year (ending September 2023). It has been estimated that fraud against individuals in England and Wales costs society about £6.8 billion per year, with cybercrime playing a key role in facilitating fraud.

This is followed by HMRC's guidance for Art Market Participants on The Money Laundering Regulations.

And finally, we introduce the virtual squatting cell commissioned by the Fraud Public Private Threat Group and look at the work of the cell to identify this activity carried out by fraudsters and other economic crime suspects.

➔ Who is the magazine aimed at?

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

➔ Contents

Cross System Professional Enablers Strategy	3
Case Studies	8
The Links Between Fraud and Other Serious and Organised Crime Threats	9
Art Market Participants and Money Laundering Regulations	13
Virtual Squatting Cell	15

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

CROSS SYSTEM PROFESSIONAL ENABLERS STRATEGY

The UK published its second Economic Crime Plan in 2023 setting out a series of strategic objectives to transform the public and private sector's response to economic crime.

The cross system strategy to tackle professional enablers is a core commitment within this plan and has been developed by the National Economic Crime Centre (NECC), and the Office for Professional Body AML Supervision (OPBAS) in close partnership with HM Government, supervisory bodies, law enforcement, the Crown Prosecution Service and private sector.

The aim of this strategy is to galvanise a whole system response to deliver a step-change in reducing the threat posed by professional enablers.



What is a professional enabler?

The financial and professional services are gatekeepers to the UK economy and play a critical role in the prevention and detection of economic crime. The public expects them to uphold the highest levels of trust and integrity, and prevent criminal activity entering the system.

The majority of firms invest heavily in ensuring their services are not used for criminal purposes, however, professional enablers have the ability to tarnish the reputation of our financial and professional services sectors and undermine the UK as a global centre for legitimate finance and investment.

A professional enabler is defined as *“an individual or organisation that is providing professional services that enables criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations.”*¹

Professional enablers can impact the following sectors amongst others:



Banks



Money Service Businesses



Legal Sector



Accountancy



Estate Agents



TCSPs



Art Market Participants

¹Economic Crime Plan 2

Why has the UK established a strategy?

The professional enabler threat is complex and is driving serious and organised crime at a regional, national and international level. A professional enabler can play a critical role in the efforts of corrupt elites and Organised Crime Groups to conceal the origin and destination of the proceeds of crime and corruption.

The UK needs to implement a multi-faceted response that prevents, disrupts and prosecutes professional enablers whilst implementing initiatives to build resilience in the financial and professional services sectors.

The cross system strategy established a new framework which will focus and reinvigorate the response to professional enablers and sets out the specific actions the system will take.



By bringing the whole system together to work in partnership we can...



Maximise the knowledge, skills and capabilities available across the system



Protect the financial and professional services from criminal exploitation



Make the UK a hostile place for professional enablers

STRATEGY

VISION

Our vision is to deliver a world-leading response to professional enablers, which sets the bar for international standards and maximises the combined knowledge and capabilities of the whole system. We will build a culture where law enforcement, supervisors, prosecutors and the private sector work together to enhance collective understanding, make better use of powers and intervention tools, and develop joint disruption strategies.

OBJECTIVES

The strategy focuses on developing the whole system approach in order to:

1. Create an enhanced sectoral level understanding of the threat
2. Ensure quality information is shared between law enforcement and supervisors
3. Strengthen and co-ordinate the capabilities of the whole system
4. Prevent enabling activity through supervision
5. Achieve long-lasting disruptive impact against the threat
6. Be a world-leader on the response to professional enablers

The strategy sets out our priority actions to drive a fundamental change in approach to tackling professional enablers

Pillar 1: Threat understanding

We will develop a detailed, sectoral-level understanding and fill intelligence gaps through enhanced exploitation of data.

Pillar 2: Information and intelligence sharing

We will ensure effective legal gateways and processes are in place and encourage proactive and reciprocal sharing of information between law enforcement and supervisors.

Pillar 3: System coordination

We will ensure effective legal gateways and processes are in place and encourage proactive and reciprocal sharing of information between law enforcement and supervisors.

Pillar 4: Protecting financial and professional services

We will ensure effective legal gateways and processes are in place and encourage proactive and reciprocal sharing of information between law enforcement and supervisors.

Pillar 5: Delivering impactful disruptions

We will develop joint operating models using the full range of civil and criminal powers and supervisory interventions to disrupt enabling activity. We will ensure cases reach positive outcomes.

Pillar 6: Driving an international response

We will drive the international response, prioritising engagement with key jurisdictions and sharing lessons learnt to continually enhance best practice.



“In April 2024 we launched the strategy at an event at the FCA offices, bringing together a fantastic group of law enforcement agencies, supervisors, government bodies and academics committed to its delivery. We know the majority of financial and professional services providers work hard to prevent money laundering. This strategy is about tackling the enabling minority, committing to strengthening information sharing between law enforcement and supervisors, and better equipping both the public and privates sectors with the information and tools they need to take action.”

Alice Boulton, Illicit Finance Lead, National Economic Crime Centre, NCA

NECC

NATIONAL ECONOMIC CRIME CENTRE

“Reducing money laundering requires a whole system approach, working in isolation just plays into the hands of money launderers looking to exploit weak links. OPBAS is pleased to co-lead this important strategy, working with statutory supervisors, law enforcement partners and PBS-supervised sectors to combat the threat of professional enablers and build resilience across the system.”

Melanie Knight, Head of OPBAS

OPBAS

OFFICE FOR PROFESSIONAL BODY AML SUPERVISION
FINANCIAL CONDUCT AUTHORITY


“The Solicitors Regulation Authority were pleased to work with the NECC and other partners in the development of the Professional Enablers Cross-System Strategy, and were grateful to have been asked to speak at the launch event. The SRA is committed to working with all of its partners in tackling the issues identified through the Strategy

Christopher Hall, Intelligence Manager, Solicitors Regulation Authority




Solicitors Regulation Authority

PROFESSIONAL ENABLER CASE STUDIES



A reporter had concerns regarding the deposit of high volumes of cash to a professional business account over a period of several months. This led to the reporter conducting an internal investigation, suspecting tax evasion. The cash deposits, totalling over £300,000, were inconsistent with the nature of this professional business, and had been transferred in quick succession to linked subjects. The reporter conducted further Customer Due Diligence checks and decided to end their relationship with the professional business and linked subjects, submitting SARs on its suspicion and a DAML SAR to return the deposits in the business account. The UKFIU disseminated the DAML SAR intelligence, allowing a law enforcement agency (LEA) to pursue an investigation on the origin of these funds. These SARs provided vital information that allowed the LEA to uncover properties being used in the illegal drug supply chain. The investigation is ongoing.



A reporter held concerns their customer's business account activity was indicative of money laundering activity. Large value funds were being paid into a business account that were not consistent with the business profile and included payments from firms unrelated to the business. The reporter wanted to exit the relationship and submitted a DAML SAR to return over £200,000 to the business. The UKFIU refused the DAML and shared the intelligence with the relevant LEA prompting an investigation into the business. The LEA successfully obtained an Account Freezing Order (AFO) against the business account for the full amount. While court proceedings continued, a second reporter submitted a DAML SAR in relation to a business account linked to the same business citing similar concerns. Thanks in part to these DAML SARs, the LEA's investigation uncovered the business' links to organised immigration crime (OIC), resulting in another LEA revoking the business' licence and cutting the business' ability to partake in OIC, anywhere in the UK. The AFO was contested but a forfeiture order was granted with funds successfully forfeited. Details of the investigation were shared with LEA partners to begin further investigations.

THE LINKS BETWEEN FRAUD AND OTHER SERIOUS AND ORGANISED CRIME THREATS

National Assessment Centre (NAC)
National Crime Agency (NCA)



Fraud remains the most common crime type in England and Wales, accounting for an estimated 38% of crime in the year ending September 2023.¹ It has been estimated that fraud against individuals in England and Wales costs society about £6.8 billion per year.² Fraud is most directly linked to Serious Organised Crime (SOC) threats where fraudulently obtained cash is spent, or where it serves to increase the scale and sophistication of fraud operations.

Cybercrime plays a key role in facilitating fraud. Initial access and compromise, online marketplaces, and victim engagement platforms are key pillars of cyber-enabled fraud. The use of network intrusion, compromised login credentials, and hacked social media accounts directly enable a range of frauds, such as unauthorised banking fraud, investment fraud, and payment diversion fraud (PDF).



Links between compromised data and fraud

Compromised data directly enables unauthorised bank fraud including card not present (CNP) fraud, which is likely the most common fraud experienced in the UK. About 2 million incidents of CNP fraud are reported each year and there is a wide and established market for sensitive information. Payment card data, bank details, and account credentials are all available for sale on the clear, deep, and dark webs, enabling offenders to carry out CNP fraud at minimal cost. The UK's introduction of two factor authentication for e-commerce in 2022 likely decreased the scale of CNP fraud reports, but some offenders are still able to bypass this.

DARK WEB

¹ [Crime Survey for England and Wales \(CSEW\): year ending September 2023](#)

² [Home Office; Fraud Factsheet](#)



Compromised data is also one method offenders can use to takeover social media accounts, which can subsequently be used in investment fraud, ticket fraud, and online shopping fraud. Action Fraud data indicates that compromised accounts are being used to upload fake images advertising high profits from fraudulent cryptocurrency schemes to the original account holder's friends and family. Additionally, hacked accounts are used to commit online shopping fraud and ticket fraud, often using the identity of a trusted seller. An emerging method involves compromised accounts used to broadcast deepfake videos of well-known figures endorsing fraudulent schemes.

Online marketplaces highly likely provide the easiest way to acquire compromised data, lowering the barrier of entry to commit fraud. For example, the Genesis marketplace enabled the exchange of compromised data, often between users who lacked the technical expertise or capability to acquire it themselves.

Offenders are likely to exploit compromised data and engage in offensive cybercrime campaigns as this activity can be monetised via fraud. The UK is one of many countries targeted by criminals for obtaining this data. According to one industry cybersecurity report, Europe had the highest number of data breaches of any region in the world.

Links between business email compromise and payment diversion fraud (PDF)

PDF involves fraud offenders convincing the victim to change details of a direct debit, standing order, or bank transfer by pretending to be an organisation or colleague to which they make regular payments. Business email compromise (BEC), where criminals gain illicit access to victim email systems, is often a precursor to PDF.

Offenders often use sophisticated cyber-dependent methods to enable BEC. Account credentials can be acquired through the use of malware, via the compromise of a legitimate email account. Remote access trojans and information stealers are also often deployed as a malicious attachment in a phishing email, enabling the offender to capture credentials or control keyboards, thereby compromising the target account.

Cybercrime-as-a-service (CaaS) providers highly likely facilitate the means to target victim networks for fraud offenders.³



³ CaaS is a model in which cybercriminals provide various cybercrime services to other individuals or groups, typically for financial gain.

Modern Slavery and Human Trafficking (MSHT) in South East Asia

It is almost certain that a proportion of hybrid romance-investment fraud against UK victims is linked to overseas MSHT.⁴ Large compounds in South East Asia are used to carry out sophisticated fraud campaigns against victims globally, often staffed by workers held against their will.

Organised Crime Groups (OCGs) target potential victims from countries in South East Asia, South Asia, and East Africa via adverts on social media sites detailing high-paid sales and marketing jobs. The potential victims are typically multi-lingual, highly likely to help expand the number of communities the OCG can defraud. The use of translation software and large language models to target victims in countries not represented by potential victims has also been reported.



OCGs use debt bondage to control victims by entirely or partially covering the cost of travel to the compounds. This debt ensures the OCG can coerce the victim into committing frauds for an extended period of time. Fines are also arbitrarily imposed by the OCG for minor infractions, increasing the debt to be repaid.

Each individual is set a defined quota detailing the number of people they need to defraud and the amount of money they need to generate. Failure to meet these targets can result in punishments.

The number of compounds and the people working within them is increasing. This is highly likely because it offers OCGs an organised and efficient method to defraud victims across the globe at scale. In Q3 2023, the UN noted that the compounds continue to expand in size and operation.

It is almost certain that fraud accounts for a small proportion of the UK MSHT threat, and a range of different methods have been identified linking potential MSHT to fraud.

⁴ Also known as 'pig butchering', this fraud refers to the process of luring victims into digital relationships to build their trust, before convincing them to invest in a fraudulent investment scheme.



One method identified involves offenders targeting potential victims on the basis of vulnerabilities, such as age and substance misuse, and using them to commit frauds across the country. In one case, the head of a UK-based gang was convicted of modern slavery offences after exploiting teenage girls to commit refund fraud against high street stores.⁵

UK-based MSHT offenders have also been involved in opening bank accounts used in money mule activity. In one case, MSHT victims had bank accounts opened in their name by their traffickers. The accounts were then sold onwards to launder the proceeds of other crimes.

Intimate Image Blackmail for Financial Gain (IIBFG)

IIBFG is where an intimate image of a victim is obtained to blackmail victims.⁶ IIBFG is known to occur during or after a romance fraud, though the known scale is low. The low number of cases identified is likely because of differences in the way IIBFG and romance fraud is carried out. Whereas a romance fraud prioritises time and communication to deceive the victim into believing they are in a genuine relationship, IIBFG is characterised by highly sexualised conversations with the sole purpose of eventually extorting the victim. Romance fraud offenders benefit from prolonging the relationship as long as possible so that further requests for money can be made.



⁵ Refund fraud is where fake barcodes are placed on items to pay a significantly cheaper price, before later requesting a refund at the full price.

⁶ Often referred to as 'sextortion' in the media.

ART MARKET PARTICIPANTS AND MONEY LAUNDERING REGULATIONS

Economic Crime

HMRC

The Money Laundering Regulations (MLRs) exist to prevent money laundering and terrorist or proliferation financing. As an Art Market Participant (AMP), you need to understand the risks that the business may face under the MLRs. These risks should be detailed in the business risk assessment (RA), and how the business deals with the identified risks are explained in their policies, controls and procedure (PCP) documents.

HMRC has found that some AMPs do not understand the risks within their sector correctly. This results in their RAs not being complete to the required standard, flowing through to their PCPs being inadequate. In several cases, customer due diligence (CDD) fails due to insufficient checks.

We have seen some AMPs holding good quality RAs and PCPs. Though some businesses do not follow their own procedures and are only carrying out minimal checks for CDD.

By engaging with businesses who have failed CDD, we understand a common reason for the insufficient checks is that the AMP has known their customer for many years. They feel there is no need to carry out full checks, or only carry out minimal checks.



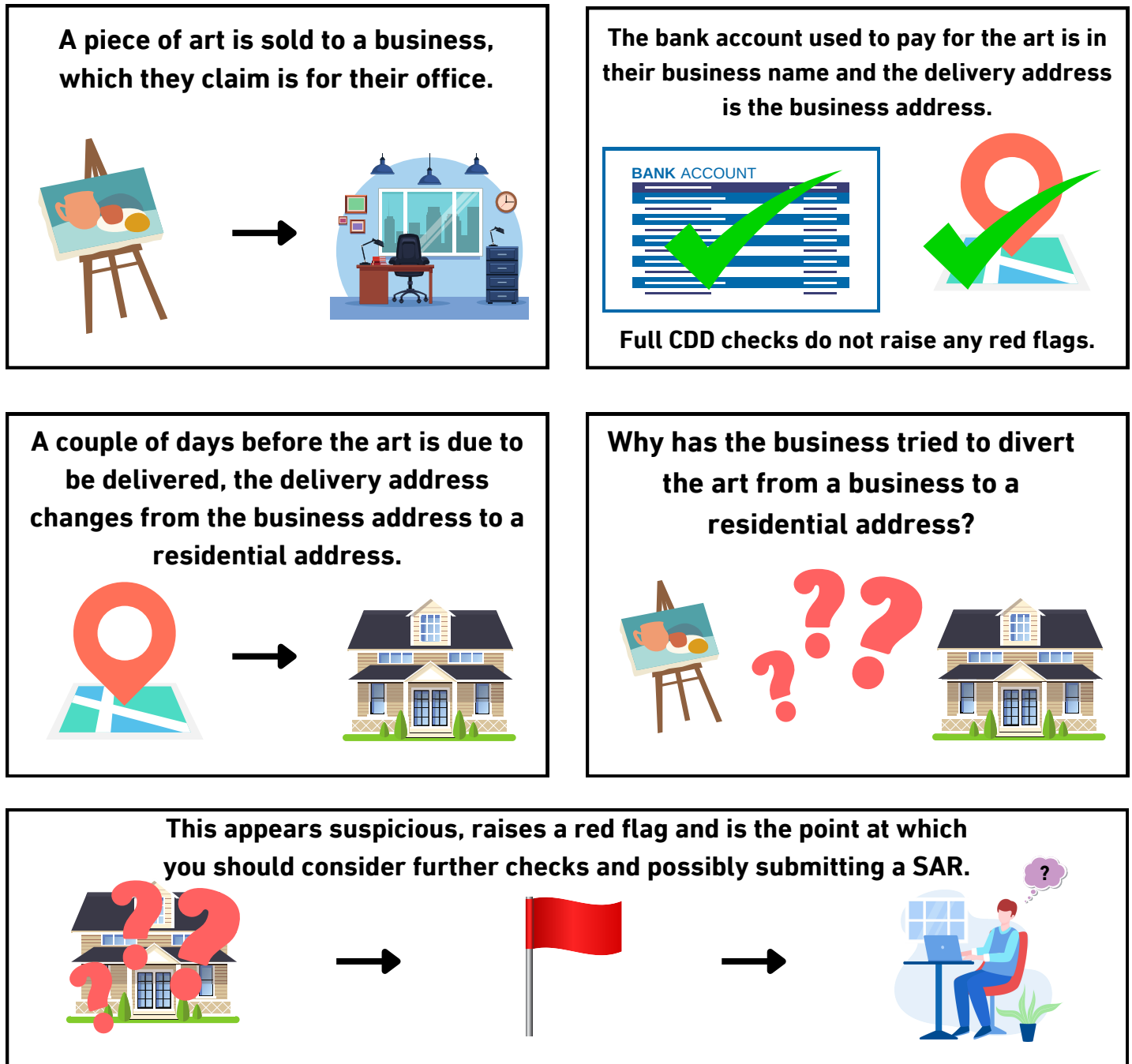
Regardless how well you believe to know a person, or whether you have traded with someone over a long period, they could still be subject to bribes, especially during financial difficulties, or they could have generally been involved in some form of illicit finance activity that you were unaware of.

For this reason, we advise that for all customers, an adverse media check and sanctions check should be carried out. If a customer has something to hide, the internet will often bring up details of this. Where you identify red flags which then lead to reasonable grounds for suspicion, you are legally required to submit a Suspicious Activity Report (SAR). This would protect you, your business, or organisation from the risk of prosecution, and the UK's financial institutions from the risk of money laundering and terrorist financing.

AMPs should also check these basic questions when transacting with their customers:

- Is the customer name the same as the name on the bank account. If not, why it is different?
- Is the delivery address the same as the customer billing address?

If there is an unsatisfactory answer to the questions above, then you should consider a SAR. You may need to consider a SAR partway through a transaction, see the illustration below.



HMRC have provided a range of webinars and YouTube videos to explain various aspects of the MLRs. See our videos on [risk assessment](#) and [identifying and reporting suspicious activity](#), which also covers NCA's [new SAR online portal system](#).

VIRTUAL SQUATTING CELL

ICAEW and NECC Fraud Threat Leadership Virtual Squatting Cell Co-Chairs

The Fraud Public Private Threat Group (PPTG) commissioned a time-limited cell to look at virtual squatting.



Virtual Squatting



A term used to describe activity by fraudsters, and other economic crime suspects, who attempt to create legitimacy to their activities, or evade investigation, by registering addresses of serviced offices, accountants, and law firms, where there has in fact been no agreement or contract to do this.

The purpose of the cell was to identify false information supplied to Companies House which can allow these criminals to access financial products, or other benefits, and subsequently create opportunities to disrupt them.

The cell, co-chaired by the NECC Fraud Threat Leadership Team and the AML Supervisory Team at the Institute of Chartered Accountants in England and Wales (ICAEW), was supported by the Public Private Partnerships team under the Joint Money Laundering Intelligence Taskforce (JMLIT)+ model.

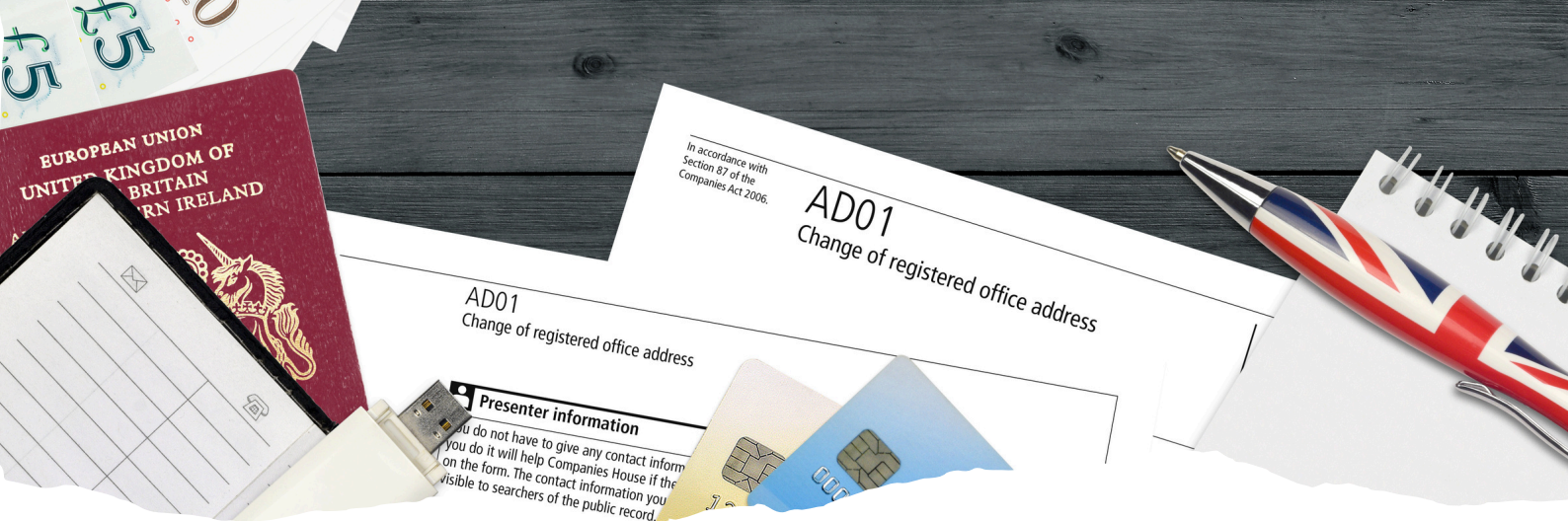


Tackling financial crime together

The cell first met in September 2023, where participants agreed the definition of 'virtual squatting' to ensure all cell members were aligned. Overall, engagement was strong and positive, with good discussions around potential activity and analysis; sharing of information and potential avenues of investigation; sharing of contacts and colleagues to further investigation work; and sharing of case studies, known virtual squatters and companies involved.

In particular, engagement was strong within both public and private sectors, with public sectors looking to analyse bulk data available to them and private sectors providing good case studies and explanations of how they encounter virtual squatting in day-to-day activities.



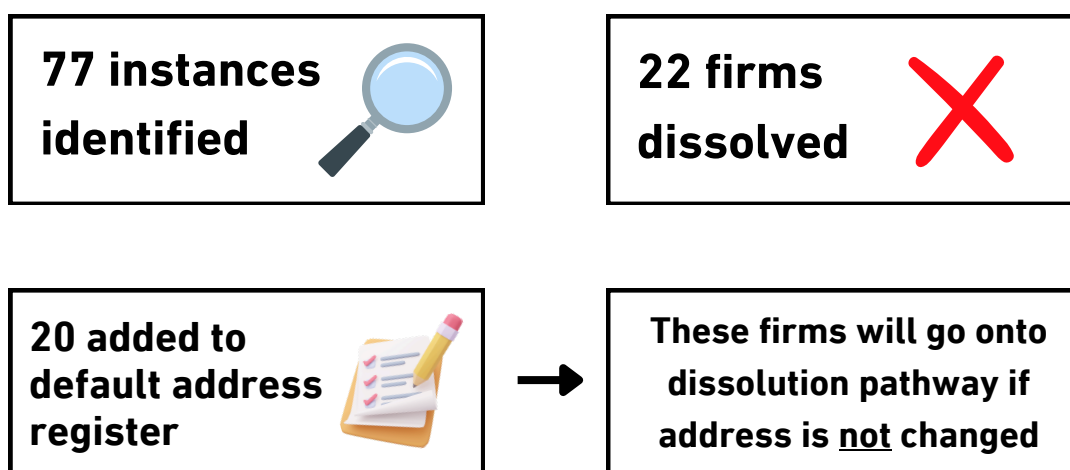


Monthly meetings, with high attendance and commitment from all cell members, helped maintain momentum and key cell outputs were:

- ▶ The development of an Amber Alert, circulated to all JMLIT+ members.
- ▶ The identification of 77 instances of virtual squatting by four cell members.

The Amber Alert was produced in conjunction with both the public and private sectors who made positive contributions and suggested amendments. It explained what virtual squatting is, described typologies and case studies as well as identifying risk factors and red flags. It provided information to the regulated sectors on how to protect themselves and suitable reporting routes if a virtual squatter is identified.

Of the 77 instances identified, Companies House dissolved 22 firms adding a further 20 onto its default address register. Should the businesses not change their registered office within a specified timeframe, these will be put on the dissolution pathway. Companies House also identified a further 10 squatters which are no longer using the addresses they initially registered.



If you identify activity which may be indicative of the activity detailed in this report, and there is a proceed of crime, you may wish to make a Suspicious Activity Report (SAR). If you decide to make a report in this way, you should adopt the usual mechanism for doing so. It will help our analysis if you would include **XXJMLXX** within the text and the reference **0742-NECC** for this alert within the relevant field on the NCA SAR Portal.

SIA

SARs IN ACTION

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



UKFIU

UK Financial Intelligence Unit



Episode 19

AVAILABLE HERE

THE UKFIU PODCAST

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

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



Updates can also be found on our LinkedIn page and on X (formerly Twitter) at [NCA_UKFIU](https://twitter.com/NCA_UKFIU).

