Issue 35

SIA

SARs IN ACTION MAGAZINE

UKFIU
UK Financial Intelligence Unit

CRYPTO DREAM SCAM NIGHTMARE

Cautioning against the threat of crypto investment fraud

PAYMENT DIVERSION FRAUD

UKFIU supports campaign to highlight the risks to victims

ASK THE UKFIU:

How do I update the main point of contact on the SAR portal?

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

NCA
National Crime Agency

Message from the Head of the UKFIU

Vince O'Brien
Deputy Director

Hello and welcome to Issue 35 of the UKFIU's magazine, SARs in Action.

This issue begins with two articles explaining how criminals are using the mask of professional services to scam individuals and businesses.

In the first article we look at how the UKFIU have supported a campaign highlighting the risk of payment diversion fraud in property sales, where victims are losing an average of £82,000.

The second article highlights the risks of company impersonation fraud and how fraudsters attempt to gain credibility by misusing well-known accountancy brand names.

The 'Crypto Dream Scam Nightmare' campaign from the National Economic Crime Centre highlights another growing fraud threat - crypto investment fraud (CIF) – a crime that costs the UK public millions of pounds every year.

Included in this issue is an update on the UK Presidency led panel discussion from the recent CARIN Steering Group meetings.

We feature a contribution from a housing association group financial crime manager on the escalating threat of money laundering to social housing and why action is needed to combat this.

To conclude this issue we answer a reporter's question, who asks the UKFIU how to update the main point of contact on the SAR portal and two case studies displaying how SAR intelligence continues to support law enforcement officers in the pursuit against financial crime.

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

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.

Payment Diversion Fraud in Property Sales

National Economic Crime Centre (NECC) Fraud and The Law Society

UKFIU have been supporting NECC Fraud and The Law Society in a campaign aimed at solicitors and conveyancers that highlights the risks of payment diversion fraud (PDF) in property transactions, a crime that costs the public millions every year. The activity is delivered with the Home Office's national '*Stop! Think Fraud*' campaign.

UKFIU, NECC Fraud and a conveyancing solicitor have collaborated to produce an episode in the UKFIU podcast series, focusing on PDF in the legal sector. The podcast addresses the scale of the threat, common methodologies, the role of social engineering, the type of criminals involved and future trends. To listen to the podcast, click here.

PDF during property sales involves criminals intercepting and redirecting legitimate property purchase funds by impersonating solicitors, estate agents or buyers through fraudulent contact. The aim is to manipulate victims into transferring house deposit funds and/or the balance of purchase to the fraudsters instead of their legitimate destination.

Figures released by Report Fraud reveal that from April 2024 to March 2025, there were 143 reports of this type of payment diversion fraud, with **victims losing an average of £82,000**. Of these victims, 32% were aged 40-49, and 27% were 30-39, making the average age of victims significantly lower than for many fraud types.

143 reports

APRIL 2024 - MARCH 2025

The campaign provides solicitors and conveyancers with practical guidance on identifying and preventing this fraud including:

CHECK

by calling before you transfer your money, as emails can be intercepted or diverted

TEST

the account is genuine by sending a small sum to the account details provided and ensure it has been received correctly

NEVER

transfer money until you are satisfied the details are correct

An information sheet was sent to 165,000 property solicitors and conveyancer members of the Law Society.

To date, our LinkedIn campaign has delivered over 1,500,000 impressions reaching 442,000 solicitors and conveyancers, and the press release was picked up by national and local outlets, as well as property focused media.

PDF is a high harm fraud for which we have a dedicated strategy and action plan to mitigate the threat from this fraud type. This work directly aligns with this plan in preventing and protecting people against becoming victims of PDF.

To find out more about Payment Diversion Fraud, download the info-sheet from the NCA website here.

Company Impersonation Fraud

BEWARE!

One of our SARs In Action readers reached out to the UKFIU recently to highlight an important topic, company impersonation fraud. The UKFIU highlighted the topic in a social media alert posted in January and have included a case example of the reader's experience as an article in this edition of SARs In Action. This article draws on an experience from the accountancy sector, but remains relevant to all professional services providers.

For many years, fraudsters have sought to gain credibility for their scams by misusing well-known accountancy brand names. Examples include using professional service firm addresses as a registered office for suspect companies without permission, faking audit reports and filing these with financial statements at Companies House. Furthermore, fraudsters are known to use logos and names of accountants on investment prospectuses to give the impression that the firm had provided assurance about the claims made about the projected returns and/or existence of the assets backing the "investment product".

Case Example

One such fraud that our reader identified targeted the victims of a previous cryptoasset scam. The fraudsters set up a domain which allowed them to create both a website and email addresses which used a variation of the name, and the real logo, of a large accounting firm.

Before the legitimate firm could have the domain taken down, the criminals sent emails to the victims of the earlier scam which stated that:

- The forensic team of the accounting firm had been carrying out an investigation into the earlier fraud;
- That they had traced the funds stolen to cryptoasset wallets which they, the accounting firm, now controlled;
- They believed that the recipient of the email was entitled to some of the funds held in the wallet; and
- The recipient should complete a client questionnaire (providing name, address, bank details and other personal information) using the link to the fake firm's website in the email.

This email was followed up by telephone calls, indicating that the individual needed to act quickly if they were to get their share of the funds. It is understood that some were told that once they signed up, they would have to pay a contribution to the costs of the investigation so far.

What actions are required?

Whenever anyone receives an unexpected email from an accounting firm, the "Take Five" rules apply just as much as in any other case.

- **Do not** feel pressurised by the sense of urgency in the email and emphasised by any follow up calls.
- Contact the firm directly by **independently searching** for its website which should provide contact details and will be able to confirm whether the individual who has emailed or called works for the firm and whether the email is genuine.
- All fraud should be reported to Report Fraud via https://www.reportfraud.police.uk/ providing as much detail as possible.

If an accounting firm becomes aware of the misuse of its name in this way, there are several steps it should consider.

Whether to make a suspicious activity report

A suspicious activity report may be required if the reporter has information which could identify a person in possession of proceeds of crime, or the location of such funds. For example, if the firm is aware that the individual has made a payment to the fraudsters and it has the recipient bank account details or any other details which may assist in tracking the funds or the fraudsters.

Alert the public

The firm should consider whether to publish an alert on its website warning about potential fraudulent misuse of its name, providing key details of any misuse it is currently aware of.

Taking down the website and related domains

Where possible, the firm should take action to have the fraudulent domain taken down. This may require the use of a specialist provider. Once the original domain is removed you may find that fraudsters set up further websites using slight variances in domain names and suffixes (e.g. .com, .co.uk etc), but removing these fake addresses as you find them can act as a disruption to the criminals.

UKFIU Reminder

SARs are solely for reporting knowledge or suspicion of money laundering under the Proceeds of Crime Act 2002 (POCA), or belief or suspicion relating to terrorist financing under the Terrorism Act 2000 (TACT). The SAR regime is **not** a route to report crime, including any predicate offences to the suspected money laundering which is why the fraud element should be reported to Report Fraud too. Any SAR filing should clearly establish the laundering of the proceeds of fraud).

The UKFIU would like to thank the contributor of this case example for their input into this article. If you would like to contribute an article to the SARs In Action, please get in touch with our Digital Media Team at UKFIUFeedback@nca.gov.uk. Articles that we feature should have a relevance to **illicit finance and SARs**, and where possible, should include a helpful **"call to action"** so that out readership can apply the learning to their own firm or institution.

Crypto Dream Scam Nightmare

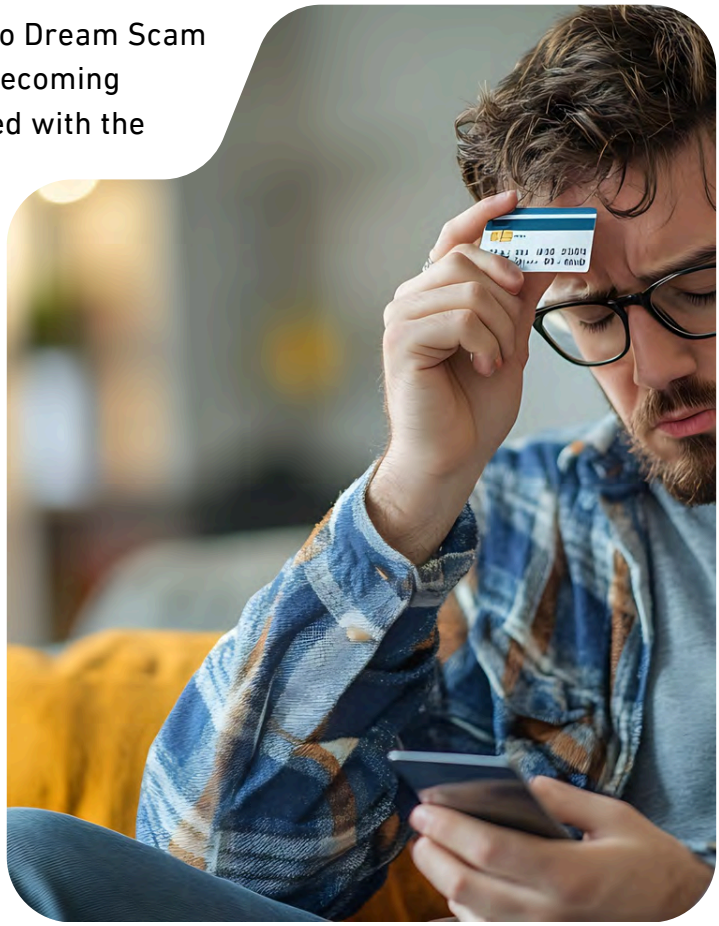
National Economic Crime Centre
National Crime Agency

In November 2025 the NECC launched a PROTECT campaign to highlight the threat of **crypto investment fraud (CIF)** – a crime that costs the UK public millions of pounds every year.

NECC
NATIONAL ECONOMIC CRIME CENTRE

CIF illicit actors target members of the public by introducing them to fake cryptocurrency trading platforms, where they are encouraged to send thousands of pounds as an investment. Victims are deceived into thinking their money is growing, but the truth is their funds have been stolen by fraudsters.

The campaign introduces the strapline 'Crypto Dream Scam Nightmare' to address how the optimism of becoming involved in crypto investing is quickly replaced with the harsh reality of losing thousands of pounds.



A series of short videos were produced, cautioning the public about the threat, and advising them to research thoroughly before sending any money. The videos signposted victims to the Financial Conduct Authority Firm Checker tool to check the legitimacy of a platform, and highlighted the importance of reporting CIF to the police via Action Fraud (now Report Fraud).

1 An info sheet (available here) was created using victim data analysis and advice from crypto experts, identifying ten tips to help spot this fraud before any money is lost.

2 Work is ongoing with Virtual Asset Service Providers (VASPs) and Crypto UK to identify further opportunities to share the media and protect the public from the threat.

3 Videos were shared on NECC LinkedIn and NCA social media, as well as targeted ads on YouTube and google, specifically aimed at the highest victim demographic: males aged 25-64. This resulted in over 12.6 million impressions of the campaign videos within 4 weeks of launch.

> **Laura Scoble, NECC Illicit Finance Threat Lead** said: "I am very proud of what we achieved under the comms campaign. Having met with victims and hearing first- hand the impact this threat had on their lives – not only financially but psychologically too – underscored the need for clear, educational messaging to prevent others from falling victim. Having the support of public and private partners via the Public Private Crypto Forum (PPCF) ensured the comms reached a huge audience online."

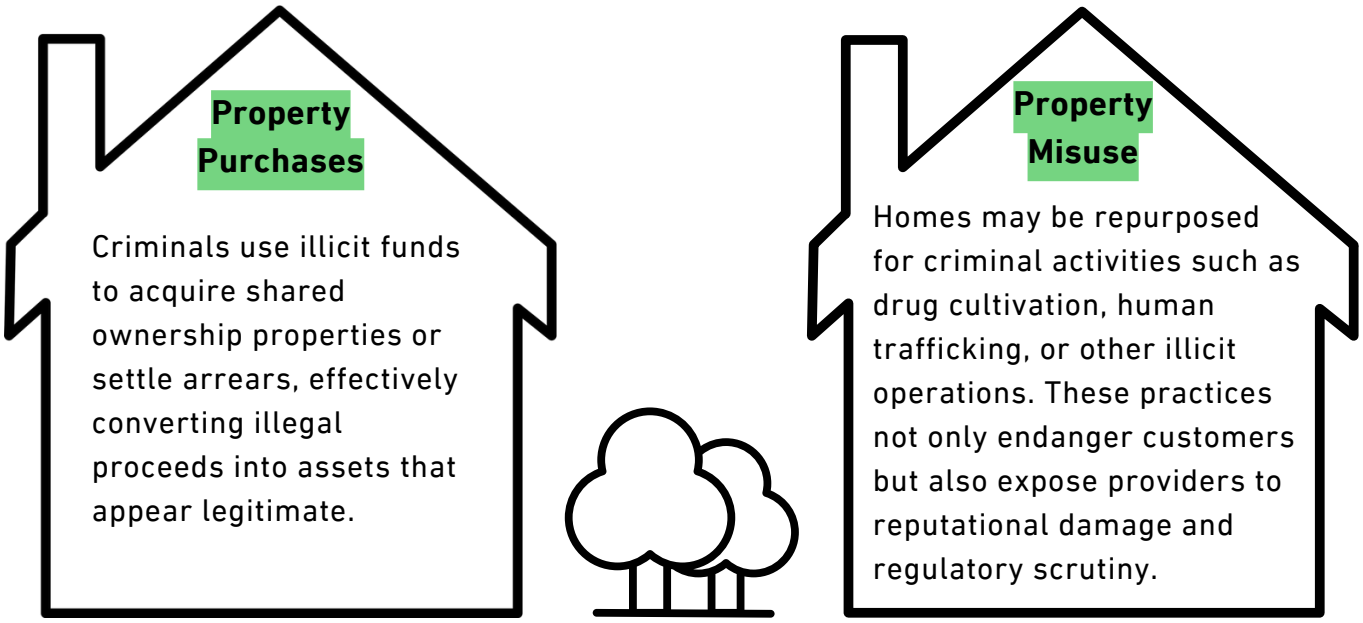
Money Laundering in Social Housing

Housing Association Group Financial Crime and Insurance Manager

Social housing providers play a critical role in supporting communities, **yet they face growing exposure to financial crime,** particularly money laundering. This risk is often underestimated within the sector, leaving housing associations vulnerable to exploitation by organised crime groups. Failure to address these threats can result in severe legal, financial, and reputational consequences.

How Criminals Exploit the Social Housing Sector

Money laundering within social housing typically occurs through everyday processes that may appear legitimate.



Such exploitation may go undetected within the sector.

Role of Professional Enablers

Solicitors, accountants, and estate agents can inadvertently, or deliberately facilitate money laundering by failing to conduct adequate due diligence. Common lapses include neglecting to verify the source of funds or ignoring suspicious payment patterns. These failures breach the Money Laundering Regulations (MLRs) and the Proceeds of Crime Act 2002, creating liability for both enablers and housing associations. The consequences include regulatory penalties, criminal prosecution, and significant reputational harm.

If a reporter submits a SAR where the suspicion involves professionals or others in the financial sector who are providing a service which is potentially willingly or unwillingly enabling money laundering, then the reporter should select the relevant glossary code in the UKFIU SAR Portal (XXPRFXX). Please see UKFIU guidance for further information.

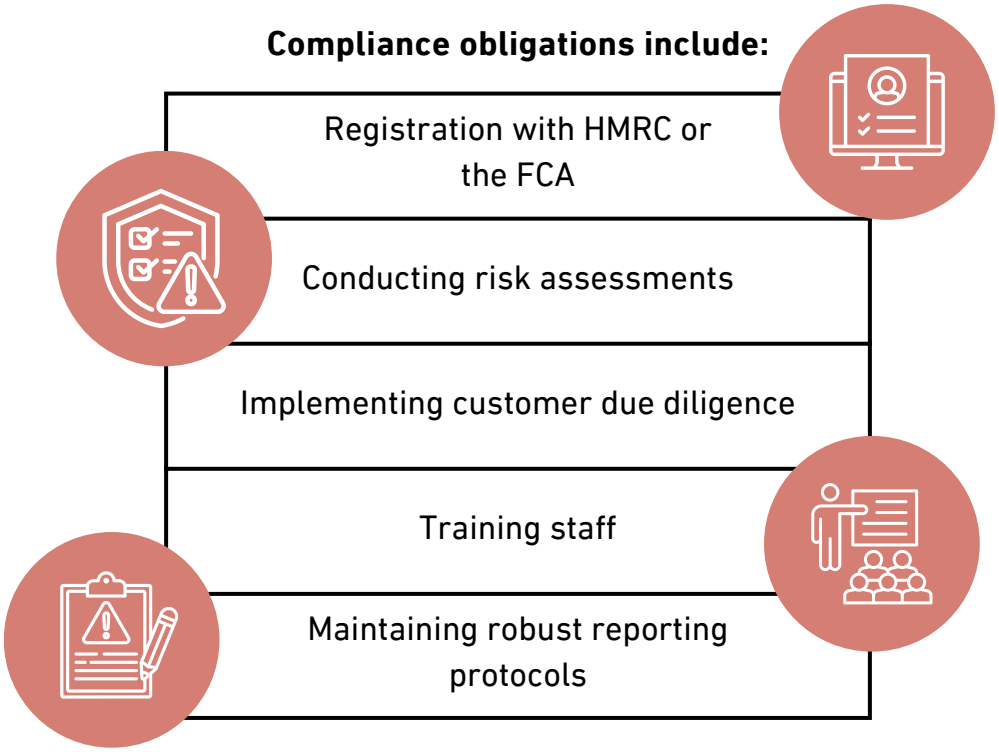
SARs in the Social Housing Sector

While the UK sees record volumes of Suspicious Activity Reports (SARs), **housing associations submit very few**. This may highlight the need for stronger internal controls and awareness within the sector.

Why Housing Associations are Regulated

Housing providers fall under the MLRs for specific activities, including:

- **Estate Agency Work:** Acting in shared ownership resales or property transactions.
- **Credit Services:** Offering loans, arrears management, or debt advice.



Why Action is Urgent in the Social Housing Sector

Financial crime is evolving rapidly, with criminals exploiting regulatory gaps and operational weaknesses. For housing associations, robust anti-money laundering (AML) compliance is essential to:

- Protect customers and communities.
- Safeguard organisational reputation.
- Support national efforts to combat economic crime.

Embedding a risk-based approach, strengthening governance, and investing in staff training are critical steps toward resilience.

Money laundering poses a real and escalating threat to social housing. By prioritising compliance, enhancing internal controls, and fostering a culture of vigilance, housing associations can mitigate risk, uphold their legal obligations, and maintain public trust.

International co-operation through CARIN

The Camden Asset Recovery Inter-agency Network (CARIN) is an informal network of law enforcement and judicial practitioners working in the field of asset tracing, freezing, seizure, and confiscation. Over 60 jurisdictions are registered as members of CARIN, with representatives assisting each other on the identification and, ultimately, confiscation of assets associated to criminals or obtained via criminal means.

CARIN continued to demonstrate its effectiveness over the last year, utilising and further strengthening relationships across its membership and with the regional Asset Recovery Inter-agency Networks (ARINs). The United Kingdom assumed the CARIN Presidency in 2025, following a successful handover from our French colleagues in a year that celebrated the 20th anniversary of CARIN.

The 2025 Steering Group meetings were held in EU countries, providing members with the opportunity to gain enhanced knowledge of the powers of Asset Recovery Offices, Prosecutors, and Financial Intelligence Units within those jurisdictions. In October, over 160 participants attended the CARIN annual general meeting representing members of CARIN, 9 ARINs, and partner organisations including Eurojust and the European Public Prosecutor's Office (EPPO). The UK Presidency led panel discussions on effective CARIN co-operation and non-conviction based asset recovery and facilitated asset recovery workshops with CARIN members.

To learn more about international co-operation through CARIN, including the UK Presidency and the role of the UKFIU and Crown Prosecution Service, we highly recommend UKFIU podcast listeners tune into episode 25.

Ask the UKFIU:
How to update the main point of contact on the SAR portal

UKFIU Reporter Engagement Team

Dear UKFIU,

We recently had a change of money laundering reporting officer (MLRO) at ABC Capital, and I've been tasked with updating the main point of contact on the SAR Portal. Is there a simple way to update the main contact details?

This is a great question — and a situation that comes up often. The SAR Portal allows users to update personal and organisational contact information via the 'Account Settings' section in the top right of the SAR Portal home page.

All personal details can be amended, with the exception of the email address used to register your account. This is the primary point of security.

If you wish to update your registered email address, you will need to:

1. Invite your new email address as a new user via your organisation's SAR Portal account
2. Complete the registration process for that new user account

Once successfully registered as a new user, you can either:

- Log into the old account and select 'Remove account' under Account Settings,

or

- Log into the new account and select 'Remove user' next to the relevant account under the 'Manage users' section.

All users linked to an organisation's SAR Portal account can update the main point of contact details for that organisation.

This includes:

- Name
- Email address
- Phone number

This can be done via the 'Account Settings' and 'Manage users' tabs. The ability to change this information is in place to help organisations keep their MLRO or nominated contact details up to date, especially for receiving DAML and DATF-related communications without interruption.

The UKFIU recommends organisations use a shared inbox for the relevant AML compliance team as their main contact email, as well as a mobile telephone number for the MLRO or Nominated Officer (or other staff member able to action defence refusals and receive communications out of normal office hours).

UKFIU
UK Financial Intelligence Unit

SARs Case Studies

A business account exhibited suspicious activity as it was primarily funded by card merchant credits which were rapidly dispersed to third parties, alongside structured debits from the account. The business had a limited online and physical presence and showed signs of a shell company, using legitimate card merchants to launder illicit funds. The reporter became suspicious and submitted a Defence Against Money Laundering (DAML) to the UKFIU.

The business was linked to multiple other business accounts, through shared addresses and transactional activity, including genuine trading activity and the rapid dispersal of large credits. The UKFIU disseminated the intelligence to a law enforcement agency (LEA) already investigating a linked business (exhibiting similar activity) and both DAMLs were refused by the UKFIU, triggering an investigation by the LEA. An Account Freezing Order (AFO) was secured against the business' account balance in excess of £115,000. Enquiries are ongoing.

Concerns were raised by a reporter after multiple business accounts linked to the same business address showed rapid movements of funds, including same-day payments, alongside inconsistent business information. Further enquiries made by the reporter highlighted a poor online presence and discrepancies in the registered address of the businesses, prompting the submission of a DAML. The UKFIU refused the DAML request and disseminated the intelligence to an LEA. Enquiries made by the LEA confirmed that the businesses were likely shell or fake entities, and that an individual listed as a director had their identity fraudulently used without their knowledge. An AFO was granted, securing over £100,000 whilst LEA enquiries continue. The DAML enabled officers to safeguard the victim's identity, protect the funds and disrupt criminal activity.

SIA

SARs IN ACTION

UKFIU
UK Financial Intelligence Unit

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

Episode 27

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 at NCA_UKFIU.