20 DECEMBER

# Economic crime quarterly

Q4 2023

Welcome to the December edition of the Economic Crime Newsletter - our last of 2023.

Since our last newsletter was published, the Economic Crime and Corporate Transparency Act has received Royal Assent. The Act marks a significant milestone in ensuring the UK's economy remains a leading place for businesses to grow and prosper. Its powers will allow UK authorities to proactively target organised criminals who would seek to abuse the UK's open economy, and allow law enforcement agencies to seize, freeze and recover cryptoassets. Selected businesses will now be able to share relevant customer information for the purposes of preventing, detecting and investigating economic crime. Companies House reform will improve transparency over UK companies, representing the most sizeable reforms to the UK's framework for registering companies for 180 years.

We would like to thank you for your engagement in the policy development of the measures and throughout the passage of the Bill through Parliament. We look forward to continuing to work with you as we implement these measures.

We are also underway in delivering the two major economic crime plans published this year: the second Economic Crime Plan and the Fraud Strategy. 17 of the 52 actions in the Fraud Strategy are now complete, including the recent agreement of the Online Fraud Charter - keep reading for more information on this. Fraud has reduced by 13% compared to last year, demonstrating progress on the Government's commitment to block scams at source and protect people's hard earned cash.

We look forward to continuing to deliver on the commitments set out in these plans next year, as well as setting out our plans to continue tackling bribery and corruption in our forthcoming Anti-Corruption Strategy. Thank you again for all your work and engagement this year, and we look forward to our continued partnership to tackle economic crime in 2024.

## Newsletter Highlights

**If you wish to discuss this newsletter in more detail or contribute to the next issue, please contact us at HOECSET@homeoffice.gov.uk. Please do feel free to share this newsletter across your network**

DECEMBER 2023

# Criminal Justice Bill introduced to Parliament

The government has introduced its third Bill in three years to tackle economic crime. The Criminal Justice Bill was introduced to Parliament on 14 November, had its second reading on 28 November and began Committee Stage on 12 December.

The Bill, which covers a range of government priorities, represents the next stage in our mission to strengthen Economic Crime legislation. It builds on the recently enacted Economic Crime (Transparency and Enforcement) Act 2022 and the Economic Crime Corporate Transparency Act 2023, by introducing measures to better protect the UK public against criminals who operate at a local and national level.

The Economic Crime measures within the Bill are:

## 1 Reform of the confiscation regime

To address concerns regarding the complexity and enforcement of the regime, the Bill will streamline court processes; provide for realistic and enforceable confiscation orders; prioritise victims' interests; and optimise the enforcement of confiscation orders.

## 2 Full reform of the identification doctrine

The Economic Crime Corporate Transparency Act 2023 modernised this principle to make it easier to convict corporates for economic crime offences. The Criminal Justice Bill enables a corporate body or partnership to be held criminally liable where a senior manager commits non-economic crime related offences while acting within the actual or apparent authority granted by the organisation.

## 3 Suspended funds

The Bill enables the creation of a voluntary Suspended Accounts Scheme (with detail to be set out through regulations), that will allow the financial sector to transfer monies equivalent to the balances of accounts that they hold suspended on suspicion of criminality to government. This follows on from the Targeted Engagement Exercise earlier this year.

## 4 SIM farms

The Bill creates a new offence banning the possession and supply of “SIM farms” which are used by criminals to send thousands of scam texts at once, with exceptions for legitimate uses.

## 5 Domain name and IP address suspension

The Bill enables law enforcement to block access to domain names and IP addresses when they are being used to conduct criminal activities. Being able to suspend access can prevent harm to individuals, such as through fraud and unauthorised access to systems, as well as protecting against botnets that may adversely impact the operation of thousands of devices.

These reforms support the objectives set out in the Economic Crime Plan 2 and Fraud Strategy, namely to:

- reduce money laundering and recover more criminal assets; and
- cut fraud while restoring faith in the public sector response.

You can view the Bill online here. We have also published a series of factsheets which contain helpful information on the economic crime measures within the Bill, which can be found here.

**If you have any questions on the Bill or would like to discuss the measures further, please get in touch with Tom Bell at tom.bell38@homeoffice.gov.uk.**

DECEMBER 2023

# Online Fraud Charter published

On the 30 November, the Online Fraud Charter was launched at an event in Lancaster House. One-by-one each signatory tech firm signed the Charter, reaffirming their commitment to tackle online fraud, with the Home Secretary putting his name to paper on behalf of the Government.

> Fraud is now the most common crime in the UK, with online scammers targeting the most vulnerable in society.
>
> For the first time, we are beginning to see a drop in fraud cases, but we must do more.
>
> By joining forces with these tech giants we will continue to crack down on fraudsters, making sure they have nowhere to hide online.

**Prime Minister, Rishi Sunak**

> The Online Fraud Charter is a big step forward in our efforts to protect the public from sophisticated, adaptable and highly organised criminals.
>
> An agreement of this kind has never been done on this scale before and I am exceptionally pleased to see tech firms working with us to turn the tide against fraudsters.

**Home Secretary, James Cleverly**

Following a Summer and Autumn of negotiations, the Charter is a document containing detailed commitments that some of the biggest tech platforms and services in the world will adopt. It is split into several areas of detailed commitments: blocking, reporting, takedowns, advertising, law enforcement, intelligence sharing, transparency, comms, and horizon scanning.

In practice, what this means is that companies have agreed to work on:

**Filtering out and removing frauds**

- Deploying systems so users do not face fraud in the first place
- Offering simple reporting mechanisms for users and taking immediate action on fraudulent content

**Making sure people are who they say they are**

- Greater verification of users from marketplace sellers to dating app users
- Enhanced measures to verify adverts and advertisers

**Raising awareness for users and victims**

- Alerts and advice at the point of first contact
- Collaboration on the government’s National Fraud Campaign

**Collaboration with law enforcement**

- Dedicated reporting routes for law enforcement and trusted third parties
- Strengthened relationships to respond to law enforcement requests

Measures in the Charter will be completed within 6 months from publication. The Security Minister, through the Joint Fraud Taskforce, will be monitoring progress and holding firms to account.

**Signatories include:**

amazon ebay facebook Google
Instagram LinkedIn Match Group Microsoft
Snap Inc. TikTok X YouTube
techUK FOR WHAT COMES NEXT HM Government

> I’ve long called for regulation and law changes to make these big tech firms step up to the plate and deny these scammers the oxygen of publicity. So I am pleased at the signing of this voluntary agreement, which is adopting many of the scam ad protection measures we’ve been calling for – such as 2 click reporting, and advertiser and site destination verification.

**Martin Lewis, founder of MoneySavingExpert.com**

DECEMBER 2023

# Government launches Independent Review of Disclosure and Fraud

As part of the Fraud Strategy, the government committed to improving the law enforcement response to investigating and prosecuting fraud. Delivering on this promise, the Independent Review of Disclosure and Fraud Offences was launched on 12 October and Chair of the Review, Jonathan Fisher KC PhD, was appointed.

As the proportion of online-enabled fraud has increased, so have the challenges facing investigators and prosecutors. One significant challenge is the already large and continually increasing volume of digital material that fraud and other complex crime cases generate.

As a result, significant time and resource is required to undertake an investigation and bring a prosecution to court. The Review will consider how the disclosure regime is working in a digital age and if fraud offences, which fall under the provisions of the Fraud Act 2006, meet the challenges of modern fraud.

The Review is split into two parts:

01 **Part one: Disclosure**

This will focus on the disclosure regime, exploring ways in which this can be modernised for all crime types.

This will report in Summer 2024.

02 **Part two: Fraud offences**

This part of the review will be focused on fraud offences. This will consider the challenges facing the investigation and prosecution of fraud and if offences and penalties still fit the crime.

This will report in Spring 2025.

**The Independent Review Secretariat can be contacted at disclosureandfraudreview@homeoffice.gov.uk.**

### Review Chair: Jonathan Fisher KC PhD

Jonathan is a leading King's Counsel in financial crime, proceeds of crime, fraud (civil and criminal) and tax cases and has been a visiting professor in practice at the London School Of Economics since 2006.

He holds a PhD which was awarded by the LSE following his research into money laundering cases and the relationship between the obligation to report suspicious activity and corporate right.

### Engagement approach

As Chair, Jonathan is engaging with a wide range of interested parties to inform the Review. This includes investigators, prosecutors, and defence professionals, and the judiciary where appropriate.

Two advisory panels are also being established:

1. **A Practitioners Panel**. Members will include leading prosecution and defence representatives, former law commissioners and academics.
2. **A Representatives Panel**, that will bring together the expertise of organisations, that uphold the disclosure regime, across the criminal justice system and the representative bodies for the legal profession.

An update on the Review's engagement approach was published on gov.uk.

DECEMBER 2023

# New Anti-Fraud Champion appointed

Simon Fell MP has been appointed as the Prime Minister's new Anti-Fraud Champion.

The Anti-Fraud Champion, which is a voluntary position, is responsible for driving collaboration between the government, law enforcement and the private sector to help block fraud.

Key areas of engagement include the banking, tech and telecoms sectors. A central part of Mr Fell's role will also be to oversee the implementation of the Online Fraud Charter.

Mr Fell has assumed the position from Anthony Browne MP, who has assumed a ministerial post at the Department for Transport.

> I'm delighted to accept this position. Fraud is an insidious crime that is too common and which profoundly harms those affected.
>
> We have to turn the tide, and I look forward to working with Ministers, industry, law enforcement, and civil society to strengthen our response and better protect society from this crime.
>
> This was my bread and butter before entering Parliament, and I can't wait to bring my experience to bear in better protecting the public.

**About Simon Fell MP**

Mr Fell has been the Member of Parliament for Barrow and Furness since 2019. Before being elected, he worked for Cifas, an industry leader in fraud prevention, for 9 years. He most recently served as its Director for External Affairs.

# Fraud discussed at AI Summit

As part of the AI Safety Summit, we held a Fraud Event in partnership with the Royal United Services Institute (RUSI). Sir David Lidington opened the event, followed by a speech from the Security Minister who formally announced the UK's ambition to host a Home Secretary Chaired Global Fraud Summit in London next March. The Summit will bring together the UKs strategic partners (5EYES, G7 + Singapore) as well as law enforcement partners to agree a co-ordinated action plan to dismantle fraud networks.

HSBC and Google presented a joint "AI for good" show and tell on their collaborative approach to deploying AI which has increased detections from two to four fold and improved HSBC's operational efficiency and customer experience.

Anthony Browne MP, while still in his role as the Anti-Fraud Champion, then hosted an interactive panel and wider room discussion on the AI enabled fraud risks, mitigations and opportunities. The panel included the Security Minister; Ben Donaldson OBE, Managing Director for Economic Crime at UK Finance; Adrian Searle, Director of the National Economic Crime Centre; Javahir Askari, Digital Regulation Policy Manager at techUK; Dr Vasileios Karagiannopoulos, Co-Director of the Cybercrime and Economic Crime Research Centre at the University of Portsmouth; and Kathryn Wetmore, Senior Research Fellow at RUSI's Centre for Financial Crime and Security Studies.

The discussion recognised the potential threats of AI enabled fraud, but was balanced by optimism and a desire to see greater collaboration and information sharing across sectors and borders to meet that challenge and drive the use of AI in taking on the fraudsters and protecting the public.

# Deepfakes and Synthetic Media: techUK and members taking steps to tackle misinformation and fraud

The surge in synthetic media and deepfake technology, while presenting new possibilities, has ushered in challenges in combatting misinformation and fraud. techUK, at the forefront of technology innovation, is actively leading initiatives to both develop synthetic media tools for constructive purposes and counter the malicious use of AI-generated content.

## Understanding Synthetic Media and Deepfakes

Synthetic Media, an umbrella term for AI-generated content, spans video, image, text, and voice. Deepfakes, a specific subset, manipulate visual or auditory information, creating convincing but fraudulent content. Pioneering technology by techUK members has led to advancements in detecting manipulated videos and developing innovative solutions.

## Benefits of Synthetic Media

Synthetic media offers diverse positive implications, from creative expression to applications in advertising, entertainment, healthcare, and education. Notably, techUK members contribute to the entertainment industry's use of CGI and enable AI-driven synthetic media for advertising initiatives.

## Risks Posed by Deepfakes

However, the rapid progress in generative AI has fuelled the proliferation of hyper-realistic deepfakes, posing risks in the form of disinformation, impersonation, and fraud. The number of deepfake videos online has surged, with 51.1% of online misinformation originating from manipulated images in Q1 of 2023. The threats extend from privacy concerns to reputational damage and trust erosion in media.

With major elections on the horizon, the potential for deepfakes to sway public opinion and spread misinformation intensifies. TechUK member Logically.ai is actively addressing political deepfakes, offering tools for fact-checking and combating fake news online. In the business realm, deepfakes pose risks of reputational damage and assist criminals in fraud schemes.

## Mitigating Deepfake Risks

To counter these risks, companies must invest in robust AI detection tools, employee training, and authentication mechanisms. Legislation, such as the Online Safety Act, is a step forward, but the evolving technology demands real-time strategies. techUK members, spanning start-ups to industry leaders, actively collaborate to share insights and promote deepfake detection and content provenance.

# Deepfakes and Synthetic Media (cont)

Members are developing advanced tools based on biological signals, phoneme-viseme mismatches, facial movements, and recurrent convolutional models. Collaboration with media outlets for watermarking authentic content and public awareness initiatives are also essential in the generative AI space.

Companies like X, Google, and Intel are taking proactive steps. X labels posts containing synthetic media and expands its Community Notes tool to tackle deepfakes. Google focuses on detecting synthetic audio and employs watermarking and metadata techniques. Intel, leveraging AI expertise, also launched a real-time Deepfake Detector with a 96% accuracy rate.

**The Future of Synthetic Media**

As AI technology advances exponentially, we must then ensure that any legal or policy responses strike a balance between harnessing AI's immense potential for societal progress while ensuring that safeguards are in place to counter its misuse. techUK emphasizes responsible AI advancement, safeguarding against misuse. techUK conduct a workstream on the use of deepfakes and synthetic media and will be working closely alongside members to address this issue through the Online Fraud Working Group.

**If you'd like to find out more about techUK's work on fraud and deepfakes and how to get involved, please contact: javahir.askari@techuk.org**

# Tackling the misuse of Registered Addresses

Section 105 of the Economic Crime (Corporate Transparency) Act 2023 ('ECCTA') makes a change that will be welcomed by Accountancy and other professional service firms throughout the UK. This provision permits the Secretary of State to introduce regulations which will permit the Registrar to make changes to the Registered Address of a company, if it appears that is not an appropriate address – that is, one which can be used to contact the company.

When this provision comes into effect, it will significantly reduce the risk that the public may be lulled into a sense of security by fraudulent companies. Currently it can take several months and considerable effort to remove a company from the address registered with Companies House. This should make the process quicker and easier. Particularly when this is combined with the powers to force a company to change its name.

A real-life example: one accounting firm identified that a company was using its address as the registered office address without authorisation. The company had a name that was almost identical to that of an FCA regulated investment firm, but had no connection to the legitimate regulated firm. This took a number of months to resolve – in the meantime, the risk of the public being misled and defrauded was a significant concern.

These new administrative powers and the ability to flag potential concerns on the register will be a big step forward in making life more challenging for fraudsters.

**Written by Angela Foyle, BDO**

DECEMBER 2023

# Cross-system strategy to tackle professional enablers

The UK's second Economic Crime Plan was published in March 2023 with broad intentions to reduce economic crime, protect national security and support the UK's legitimate economy. The National Economic Crime Centre (NECC) has led on one of its core commitments, to develop and implement a cross-system strategy to tackle the threat of professional enablers.

The financial and professional services are key gatekeepers to the UK economy and play a critical role in the prevention and detection of economic crime. We know that the majority of regulated firms and practitioners offering these services invest heavily in ensuring they comply with Anti-Money Laundering obligations. They build compliance teams to detect potential money laundering and prevent the exploitation of their services to facilitate that criminal activity. However, professional enablers have tarnished the reputation of these sectors. This in turn undermines the UK's reputation as a global centre for legitimate finance and investment, erodes public trust in the professions, and drives serious and organised crime at a local, regional and national level.

> A professional enabler is defined in the Economic Crime Plan 2 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*"

Throughout 2023 the NECC consulted widely with private and public sector partners across the system to understand the challenges and barriers in our collective efforts to reduce the threat from professional enablers. Through this engagement we have identified six key areas where the UK could enhance its response to professional enablers. These six areas form the foundation of our strategy, and act as the core pillars under which we will drive the response across the system. They are:

01 **Pillar 1: Threat Understanding**
To enhance our understanding and create a strong evidence base of the current and emerging threat at a sectoral level through the effective tasking and prioritisation of research into intelligence gaps.

02 **Pillar 2: Information and Intelligence Sharing**
To equip the system with the information it requires by increasing the quantity and quality of information sharing between law enforcement, supervisory bodies and the private sector.

03 **Pillar 3: System Coordination**
To strengthen and co-ordinate the knowledge, resource and capabilities of the whole system to drive a holistic response to the threat.

04 **Pillar 4: Protection of the Financial and Professional Services**
To prevent enabling activity through effective supervision by supporting firms to protect themselves against exploitation in economic crime and increase compliance with regulatory obligations and professional standards.

05 **Pillar 5: Deliver Impactful Disruptions**
To increase long-lasting disruptive impact against the threat, we will develop joint operating models using the full range of civil and criminal powers, and supervisory interventions.

06 **Pillar 6: Drive the International Response**
To be a world-leader on the response to professional enablers by developing our partnership working with other jurisdictions, utilising international engagement to share lessons learnt and continually enhance best practice.

The NECC has developed the cross-system strategy with partners including HM Government departments, supervisory bodies, the Crown Prosecution Service and the private sector. We have collectively committed to key performance indicators and milestones to ensure effective delivery under strategy pillars.

Our mission is to deliver a step-change in the UK's response to the professional enabler threat and enshrining a no tolerance culture towards professional enabler activity in the UK.

To find out more, please contact Alice Boulton
alice.boulton@nca.gov.uk

# HMRC host first Trade-Based Money Laundering Summit

HMRC hosted the first of its kind Trade-Based Money Laundering Summit in London on the 18-20 September.

The Summit aimed to bring together experts from across the globe. We welcomed approximately 200 delegates from the public and private sector – both domestic and international – with guest speakers from the United Arab Emirates, Australia, The United States, Canada, United Nations and the Asian Development Bank.

It focused on three key areas:

1. **Capability and engagement**, to ensure we have the right people with the right skills, technological and legislative support to target TBML
2. **Intelligence and data**, to discuss how to make better use of data and knowledge to improve the overall intelligence picture
3. **Operations**, to allow the sharing of operational insight and expertise.

The final Summit session was a Call to Action, with delegates committing to exploring opportunities for domestic public private partnership initiatives to work across borders and sharing intelligence on common commodities exploited to support increased targeting and disruption of TBML networks.

HMRC's ongoing performance delivery on TBML, on behalf of system partners, will be reported via the ECP2 reporting framework into the Economic Crime Delivery Board and Strategic Boards.

**To find out more about HMRC's work on TBML, contact Shyla Mohanadas shylaja.mohanadas@hmrc.gov.uk and tbml.threatsteam@hmrc.gov.uk**

> Trade Based Money Laundering is:
> **The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins"**
>
> - Financial Action Task Force

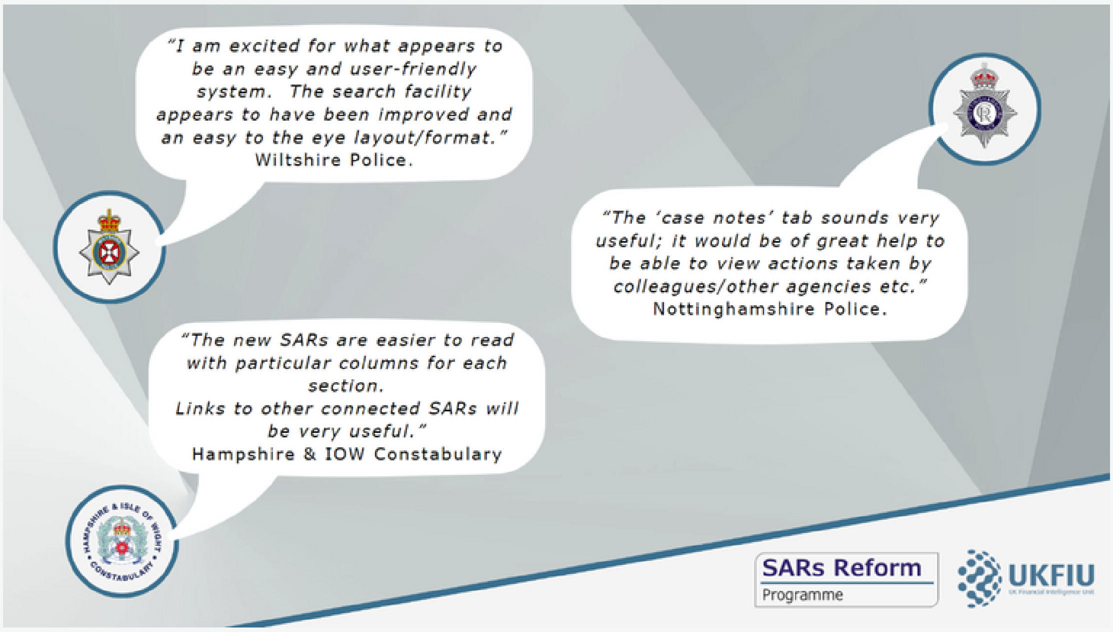
Criminals are adept at laundering their dirty money, often perverting technological advancements to spin increasingly complex webs to hide their illicit gains. Trade-Based Money Laundering (TBML) – the exploitation of the trade system to 'clean' dirty money - is a major driver of the £1.4 trillion that is laundered globally every year. In the UK alone, it is estimated that billions are laundered annually through exploitation of the trade system.

This is why we have included it as a named threat in the second Economic Crime Plan. It is a global problem which is notoriously complex and difficult to identify. By its very nature, it touches on a wide range of stakeholders, sectors and jurisdictions. It also shares risk indicators with other money laundering methodologies or criminality such as illicit commodity smuggling or abuse of corporate structures.

# SARs Digital Service Development

In the recent SOCEX Economic Crime Conference, the Programme team shared initial designs of the next release of the SARs Digital Service, impacting Law Enforcement and Government agencies across the UK. A large number of attendees were shown what the new service is expected to look like when it beings to be rolled out in 2024.

Product owner, Mike Hindes, has also hosted a series of walkthroughs with members across the 77 Law Enforcement and Government partners. This has helped us gather valuable feedback and insights, including the below.



*"I am excited for what appears to be an easy and user-friendly system. The search facility appears to have been improved and an easy to the eye layout/format."*
Wiltshire Police.

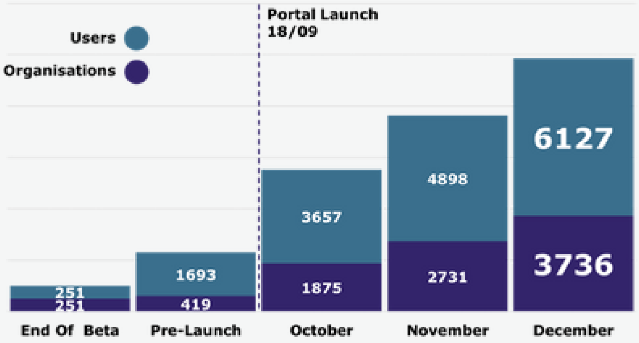
*"The 'case notes' tab sounds very useful; it would be of great help to be able to view actions taken by colleagues/other agencies etc."*
Nottinghamshire Police.

*"The new SARs are easier to read with particular columns for each section.*
*Links to other connected SARs will be very useful."*
Hampshire & IOW Constabulary

The Programme will continue to engage and request feedback from the wider SAR community in early 2024. Plans include sharing wireframe walkthroughs and providing access to a test environment, for users to interact with a dummy version of the system to provide feedback.

## SAR Reporting Route Growth

Since the SAR Portal was launched to the public in September 2023, over **6000** users from **4000** organisations are now submitting SARs though the new SAR Portal. This has resulted in more than **50,000 submissions**, all with an enhanced data structure and additional fields.



Users of the SAR Portal have called it user friendly and easy to use, and the changes made are helping provide Law Enforcement and Government colleagues with more information that can be used to trace, investigate and prosecute criminal activity.

Several prominent reporters from a range of reporting sectors have provided feedback about their experiences using the SAR Portal, with many highlighting the ease of registering and submitting SARs. This feedback has been used to identify and drive a number of improvements aimed at enhancing and streamlining the overall user experience.

The SAR Portal now accounts for **60%** of all submitted SARs compared to the legacy SAR Online System, which is due for final decommissioning in early 2024. In preparation, it is recommended that all remaining SAR Online users register for the SAR Portal and begin using it as their sole reporting route from now on.

**For questions on the SARs Digital Service, please contact SARsITTransformation@nca.gov.uk**
**For questions on the SAR Portal and other reporting routes, its UKFIUEngagement@nca.gov.uk**

# Law Society and Bar Council continue working with government on supporting the sanctions regime

The Law Society of England and Wales and Bar Council sanctions compliance experts published a joint note on the sanctions 'control' test in light of the Court of Appeal judgment in NBT v Mints [2023] EWCA Civ 1132.

The identification of who is subject to UK sanctions regimes – in particular the targeted asset freeze prohibition – is of fundamental importance to the operation of those regimes, to legal certainty and to the credibility of the UK as a major international sanctions jurisdiction. There is currently an extreme degree of uncertainty on this key issue.

As acknowledged by the UK government, the Court of Appeal judgment highlighted one aspect of uncertainty that it could be a given that President Putin and other ministers have been designated and Russia is a command economy. The test might mean that every company in Russia should be treated as subject to UK sanctions on the hypothesis that the President could ultimately control all of those companies.

This uncertainty is causing significant problems, which is particularly serious given potential criminal liability and strict civil liability. For example, lawyers need to know if they are acting for a company subject to an asset freeze.

Whilst the joint Law Society and Bar Council note was prepared before the High Court's judgment in Litasco SA v Der Mond Oil and Gas Africa SA [2023] EWHC 2866 (Comm) and the publication of the government guidance on ownership and control: public officials and control, which provide some additional guidance relevant to the assessment of control issues, the substantial uncertainty highlighted in the note still remains.

Given the Court of Appeal's judgment on the wide breadth of the control test, it is difficult to see how guidance will provide the necessary clarity and ultimately amendment to the regulations will be needed to deliver the requisite legal certainty.

Guidance is a stop-gap measure and, in reality, if the problem is to be addressed legislative change is needed.

The Law Society remains committed to supporting the government's ongoing aim of responding with strong and effective sanctions against Russia's illegal war on Ukraine. Working closely with the Bar Council, we are continuing to actively engage with the Office of Financial Sanctions Implementation and other stakeholders offering ongoing assistance in reducing uncertainty and developing a framework that provides greater clarity.

**Written by Nick Emmerson**
**President of the Law Society of England and Wales**

DECEMBER. 2023

# FORWARD LOOK

| | |
|---|---|
| Christmas Recess | Christmas recess: **19 December - 8 January** |
| Public Private Steering Group | PPSG to be held on **27 February** |
| Global Fraud Summit | Hosted in London on **11-12 March** |

**If you wish to discuss this newsletter in more detail or contribute to the next issue, please contact us at HOECSET@homeoffice.gov.uk**
**Please do feel free to share this newsletter across your network**