House of Commons

Treasury Committee

Economic Crime: responses to the Committee's Eleventh Report

Eighth Special Report of Session 2021–22

Ordered by the House of Commons to be printed 25 April 2022

HC 1261
Published on 28 April 2022
by authority of the House of Commons

The Treasury Committee

The Treasury Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of HM Treasury, HM Revenue and Customs and associated public bodies.

Current Membership

Mel Stride MP (Chair) *(Conservative, Central Devon)*

Rushanara Ali MP *(Labour, Bethnal Green and Bow)*

Harriett Baldwin MP *(Conservative, West Worcestershire)*

Anthony Browne MP *(Conservative, South Cambridgeshire)*

Gareth Davies MP *(Conservative, Grantham and Stamford)*

Dame Angela Eagle MP *(Labour, Wallasey)*

Emma Hardy MP (*Labour, Kingston upon Hull West and Hessle*)

Kevin Hollinrake MP *(Conservative, Thirsk and Malton)*

Julie Marson MP *(Conservative, Hertford and Stortford)*

Siobhain McDonagh MP (*Labour, Mitcham and Morden*)

Alison Thewliss MP *(Scottish National Party, Glasgow Central*)

Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/treascom/ and in print by Order of the House.

Committee staff

The current staff of the Committee are Morenike Alamu (Committee Operations Officer), Rachel Edwards (on secondment from the Bank of England), Kenneth Fox (Clerk), Dan Lee (Senior Economist), Adam McGee (Senior Media and Communications Officer), Aruni Muthumala (Senior Economist), Moyo Oyelade (on secondment from the Bank of England), Charlotte Swift (Second Clerk), Ben Thompson (on secondment from the National Audit Office), Sam Upton (on secondment from the Financial Conduct Authority), Adam Wales (Chief Policy Adviser), Maciej Wenerski (Committee Operations Manager), and Marcus Wilton (Senior Economist).

Contacts

All correspondence should be addressed to the Clerk of the Treasury Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5769; the Committee's email address is treascom@parliament.uk.

You can follow the Committee on Twitter using @commonstreasury.

Eighth Special Report

The Treasury Committee published its Eleventh Report of Session 2021–22, *Economic crime* (HC 145), on 21 April 2022. Responses have been received from HM Treasury, the Financial Conduct Authority, and the Payment Systems Regulator. Those responses are appended to this Report.

Appendix 1: response from HM Treasury

Government response to the conclusions and recommendations of the Treasury Select Committee report on 'Economic Crime':

The government has considered and is grateful for the Treasury Select Committee's report titled 'Economic Crime', published on 2 February 2022.

The report's conclusions and recommendations are appreciated. The government wishes to provide the Treasury Select Committee with a clear and detailed understanding of the public and private sector's shared response to economic crime.

The importance of actions the government has taken to fight economic crime have only been heightened in light of the Russian invasion of Ukraine on 24 February. In response to the invasion, as well as significantly expanding and strengthening our sanctions regime, the government has accelerated the delivery of several key measures designed to tackle illicit finance. It has also announced a comprehensive package of further reforms, including additional primary legislation to be introduced in the Third Session of this Parliament. These measures will enhance our ability to tackle economic crime and make it harder for international illicit finance to enter the UK.

This paper sets out the government's response to each of the Committee's conclusions and recommendations. The Committee's text is in bold, and the government's response is in plain text. Paragraph numbers refer to corresponding paragraphs in the Committee's report.

The growth in economic crime, and the Government's response

The growth in economic crime and fraud is constantly evolving and poses a challenge to Government. There is no "silver bullet" solution. Government must work across departments, regulatory bodies, and law enforcement agencies to address all aspects of the problem. A plan to co-ordinate this work, such as the existing Economic Crime Plan, is a sensible approach. However, it can only work if there is extensive co-ordination at all levels, from Ministers to those on the ground who are enforcing the law. This might be simpler if a single Government Department or agency had responsibility for all policy aspects. (Paragraph 33)

We are as unhappy as the Minister is with progress so far in tackling economic crime, and we welcome his frankness about the progress made. We acknowledge that there is a lot of activity going on across Government, by regulators and crime-fighting agencies, to tackle economic crime; but fraud and economic crime have continued to rise at an alarming rate. Work being done by Government is still not enough and not urgent

enough to stem the rise, let alone start to bring it under control. (Paragraph 34)

The Government should give this work a far higher priority. Economic crime harms consumers and businesses, damages the reputation of the UK as a pre-eminent financial centre and, as the NCA says, threatens national security. (Paragraph 35)

The government takes the threat of economic crime extremely seriously and has developed robust processes to ensure an effective and coordinated response. This involves departments across government, regulatory and enforcement agencies, and the private sector, reflecting the wide-ranging impacts of economic crime and the need for a comprehensive response in partnership with the private sector. The broad range of stakeholders involved in the policy, supervisory and operational response to economic crime means a robust governance structure is required.

The Home Office and HM Treasury lead the policy response to economic crime for government and are responsible for coordinating the public-private Economic Crime Plan.[1] It is right that these two departments jointly lead the government's response, to support system leadership that fully considers the long-term ramifications of decisions that impact both the UK's prosperity and security.

The establishment of the National Economic Crime Centre (NECC) was an important step taken by the government. Hosted in the NCA it sets and leads the threat response to economic crime, ensuring the wide range of stakeholders are focused on the agreed strategic priorities where the system, collectively, can have the most impact on the threat.

The Economic Crime Plan's delivery and effectiveness is shaped and monitored through shared, regular, ministerial governance with cross-sectoral private sector members through the Economic Crime Strategy Board. This senior forum sets the strategic priorities for the UK's response to economic crime. Below it, a number of other coordination and information-sharing forums meet regularly to review progress and ensure coordination of priorities across government on operational and transformational policy programmes. For example, the Economic Crime Delivery Board drives forward the development of economic crime policies, assesses the implementation of key reforms and brings together key departments and agencies.

Russia's invasion of Ukraine has only increased the importance and urgency with which the government will pursue our economic crime agenda. The UK has already imposed the most severe package of financial sanctions in history in response to Russia's unprovoked and illegal invasion of Ukraine. Working with private sector and international partners, the government will continue to make it far more difficult for oligarchs and businesses to operate in an illicit manner outside their own borders.

Further swift steps have been taken by the government on economic crime since the Committee's report was published. Most notably, the government passed the Economic Crime (Transparency and Enforcement) Act on 15 March.[2] This will:

- Introduce a Register of Overseas Entities Beneficial Ownership of UK property to tackle foreign criminals using UK property to launder money.

1 Economic Crime (Transparency and Enforcement) Act 2022 (legislation.gov.uk)
2 Economic Crime (Transparency and Enforcement) Act 2022 (legislation.gov.uk)

- Reform the UK's Unexplained Wealth Orders regime, to remove key barriers faced by law enforcement and help target more corrupt elites.
- Strengthen the Treasury's ability to take action against financial sanctions breaches.
- Enable Ministers to impose sanctions quicker and in concert with the UK's allies.

Noting the Committee's comments regarding the pace of delivery, the government would also highlight that the NCA has rapidly established a 'Combatting Kleptocracy Cell'. This will target the most egregious corrupt elites and their enablers through their assets hidden in the UK, including through criminal sanctions enforcement.

The government has also published details of upcoming legislation planned for introduction in the Third Session.[3] Measures will include reform of Companies House, reforms to prevent abuse of limited partnerships, new powers to seize and recover illicit cryptoassets, and reforms to give businesses more confidence to share information on suspected money laundering.

Turning to fraud, the government and law enforcement agencies relaunched the Joint Fraud Taskforce last year to clampdown on criminals through new partnerships across government and the private sector. The government, alongside the National Cyber Security Centre (NCSC), has also established a new Suspicious Email Reporting Service, which has led to the public submitting over 10 million suspicious emails. Since the takedown service launched in April 2020, over 76,000 online scams have been removed across 139,000 URLs. An additional proactive programme carried out by NCSC in partnership with the NECC and industry partners has led to the removal of over four million pieces of online criminal infrastructure used in fraud and cyber crime.

Tackling fraud requires a unified and co-ordinated response from government, law enforcement and the private sector to better protect the public and businesses from fraud, reduce the impact of fraud on victims, and increase the disruption and prosecution of fraudsters. As part of its commitment to this agenda, this year the government will be publishing its 10-year Fraud Strategy to address the threat of fraud. It will set out how government will work with industry to remove the vulnerabilities that fraudsters exploit, with intelligence agencies to shut down fraudulent infrastructure, with law enforcement to identify and bring the most harmful offenders to justice, and with all partners to ensure that the public have the advice and support they need.

We intend to continue using and refining these well-established governance structures to coordinate progress and maintain this momentum to strengthen the UK's response to the serious risks economic crime poses. The upcoming publication of the Fraud Strategy and second Economic Crime Plan later this year will set out more detail on our priorities.

The Economic Crime Plan is for the period 2019 to 2022, and this year there is an opportunity for the Government to review how well the Plan has operated, its strengths, and its failings. It should be adapted as necessary and renewed for a further three years. We expect that the Government will use the opportunity to push harder and act faster to reduce fraud and economic crime across a range of policy areas. (Paragraph 36)

3 https://www.gov.uk/government/publications/corporate-transparency-and-register-reform

We recommend that the Government considers whether the governance of the Economic Crime Plan has been effective and also whether having such a wide range of departments with responsibilities in this field is the best way to tackle a problem like economic crime. The Government should consider whether policy responsibility should be centralised in a single Government department. The Government should move to a strategy for combatting fraud which focuses on outcomes, not processes. Its explicit target should be to reduce substantially the level of fraud. (Paragraph 37)

Fraud and economic crime are complex and multifaceted issues that touch upon much of the economy and manifest in many different ways. A single departmental approach would, in the government's view, undermine our efforts to tackle holistically the challenge that economic crime presents. That is why the government established the NECC and published the Economic Crime Plan. It is intended to facilitate progress through coordinated partnership-working between the public and private sectors.

One such partnership, the NECC's Joint Money Laundering Intelligence Taskforce (JMLIT+) is a world-leading model of best practice. The JMLIT+ model, which has been expanded and strengthened over the last 18 months, enables tactical and strategic intelligence sharing between the public and private sectors, enabling them to tackle serious and organised crime more effectively, support high priority operations, and manage financial risk across the system.

As mentioned above, the Economic Crime Plan is monitored at the most senior levels of government. It provides a collective articulation of actions the UK is taking to tackle economic crime. The private and public sectors are making measurable progress in delivering the Economic Crime Plan and are on course to deliver 49 of the 52 actions set out in the Plan. At the most recent Economic Crime Strategic Board this progress was summarised and welcomed across the private and public sector.

This action-driven approach to the Economic Crime Plan has resulted in substantial improvements in the UK's overall response to economic crime. The Plan prioritised risk areas by addressing gaps identified by the Financial Action Task Force's (FATF) Mutual Evaluation Report assessment.[4] The FATF is the international standard-setter for measures to tackle money laundering and terrorist financing. For example, the Economic Crime Plan committed the UK to update its Money Laundering Regulations. This has closed vulnerabilities in our system and brought new sectors within scope of the requirements.[5] The Economic Crime Plan has also led to the publication of a White Paper setting out the government's plans for Companies House reform.[6] These proposals have been widely supported and the package of reforms—thanks to this coordinated approach—will be put forward as legislation in the Third Session. They will ensure Companies House plays a larger role in combatting economic crime.

Delivery of the actions from the first Economic Crime Plan has played an important role in the UK's fight against economic crime. However, the threat posed by economic crime is constantly evolving. Therefore, at the most recent Economic Crime Strategic Board the Home Office and HM Treasury proposed a second iteration of the Plan. We share the Treasury Select Committee's view that the government's approach should be informed by

4 MUTUAL EVALUATION OF THE UNITED KINGDOM (fatf-gafi.org)
5 The Money Laundering and Terrorist Financing (Amendment) Regulations 2022 (legislation.gov.uk)
6 Corporate transparency and register reform - GOV.UK (www.gov.uk)

the analysis of measurable outcomes.

This shift in focus will help to ensure that the private and public sectors' energies are well-targeted towards addressing fraud, as well as high-end and cash-based money laundering. During the development of the Economic Crime Plan 2.0 the government will evaluate the strengths and weaknesses of the first iteration of the Economic Crime Plan. This assessment will help ensure the next iteration of the Plan is effective as possible.

Spending on economic crime needs to be sufficient to meet the challenge. The Economic Crime Levy is intended to bring in a useful amount of additional funding to support the fight against economic crime. We welcome the design of the Levy, as it is simple and excludes the vast majority of regulated businesses. However, spending on anti-money laundering should match the need and should not be limited by the yield of the Levy alone. (Paragraph 47)

We welcome the Government's undertaking to be accountable for spending the money raised by the Economic Crime Levy in the way in which it is intended. We recommend that the Government publishes an annual account of its spending on economic crime, including an account of how the yield from the Economic Crime Levy has been spent, and an evaluation of its effectiveness. (Paragraph 48)

The government recognises the need for increased spending to tackle economic crime. That is why we have legislated for a new Economic Crime (Anti-Money Laundering) Levy which will raise around £100 million per year to help fund anti-money laundering measures.[7]

In line with the principle of transparency set out by the Levy consultation document, the government intends to remain accountable for the spending of the money raised by publishing an annual report on the levy, in addition to a more wide-ranging review of the levy by the end of 2027. These mechanisms will provide transparency to industry and levy payers on how the policy is performing, including how the money is being spent.

The Levy, combined with funding announced at last year's Spending Review, collectively represents a package of around £400 million to tackle economic crime until 2025. For example, the government is delivering reforms set out in the Economic Crime Plan with approximately £100m to be spent on tackling fraud specifically.

Among other measures, this investment is intended to deliver Suspicious Activity Reports (SARs) reform and support efforts to tackle illicit finance. This investment will increase intelligence capabilities in the National Crime Agency (NCA) and the national security community to identify and disrupt the most harmful criminals and serious organised criminal gangs. It will also establish a new fraud investigative function in the NCA. We are also increasing law enforcement investigative capacity in the City of London Police, as national lead force for fraud, and in Regional Organised Crime Units across England and Wales.

The government also recognises the importance of delivering Companies House reform. HM Treasury has therefore provided BEIS with £63 million over the Spending Review period to facilitate reforms. This funding will ensure that the Economic Crime (Transparency and Enforcement) Act, and the legislation being introduced in the Third

7 Economic Crime (Anti-Money Laundering) Levy - GOV.UK (www.gov.uk)

Session, can be operationalised as quickly as possible.

In addition, £5.4 million of Official Development Assistance (ODA) funding has been allocated across the Spending Review period to support the work of HM Treasury's Illicit Finance Technical Assistance Unit. It will also provide additional support to the work of the FATF and FATF-Style Regional Bodies. This funding will help to tackle international illicit finance by strengthening the implementation of the FATF Standards in ODA-eligible countries, in concert with partners.

We recommend that the Government provides a breakdown of how the additional funding allocated to the Home Office in the Spending Review for fighting economic crime will be spent, and how much of that funding will reach crime-fighting agencies. The financial resources being brought to bear on the problem are fragmented and modest when compared to the losses attributed to fraudulent activity. Given the scale of the problem and the speed at which it is growing, we remain to be convinced that this extra resource will enable a sufficient response in the absence of a substantial reform of the anti-fraud infrastructure. (Paragraph 49)

The government has developed a sustainable funding model that demonstrates its commitment to tackling economic crime. As aforementioned, the combination of last year's Spending Review settlement and private sector contributions through the Economic Crime (Anti Money Laundering) levy will provide economic crime funding totalling around £400 million over the Spending Review period.

Law enforcement activity on economic crime is conducted by a number of organisations, some of which, like the Serious Fraud Office, are narrowly focussed on this issue whereas others, such as territorial policing, work on the full range of crime types. This structure means that it is challenging to track the exact total of how much is being spent by the public sector to tackle economic crime specifically. Public-private partnerships, such as the NECC, are also helping to provide resources for coordinating a national response to economic crime. In addition to core funding, under the Asset Recovery Incentivisation Scheme law enforcement agencies also receive a proportion of the assets recovered under the Proceeds of Crime Act (2002) which can be used to fund future asset recovery work, as well as wider crime reduction projects.[8]

While exact allocations for the Spending Review period are not yet determined, around £100 million has been allocated to tackling fraud by the Home Office up until 2025. The focus of this spending will be on the law enforcement response and replacing the current Action Fraud system with a new Fraud and Cyber Reporting Analysis Service. For economic crime, investment will be focused on continuing to deliver the Suspicious Activity Reporting and Illicit Finance programmes, investing in teams and technology to recover criminal assets, as well as investing in new fraud and anti-money laundering capabilities. Specific allocations are subject to internal departmental allocations processes for each financial year.

This funding will also support the second iteration of the Economic Crime Plan, which will set out the outcomes the private and public sector are working towards and how we intend to measure the impact of investment.

8 Asset Recovery Action Plan (accessible version) - GOV.UK (www.gov.uk)

The number of agencies responsible for fighting economic crime and fraud is bewildering. Each of the enforcement agencies has other crime-fighting or regulatory objectives, and although the joint working co-ordinated by for example the National Economic Crime Centre is welcome, there is a bigger question about whether there should be a single law enforcement agency with clear responsibilities and objectives to fight economic crime. We recommend that the Government seriously considers this issue as part of a review of the Economic Crime Plan. (Paragraph 56)

The government believes that a multi-agency approach is the right way to fight economic crime and fraud. It enables us to differentiate between different crime types. For instance, fraud within the public sector requires a different response to fraud committed by individuals or businesses. Similarly, some forms of fraud are minor and localised and therefore requires a local response. Collaboration between agencies enables the UK to deploy relevant expertise and resources in a targeted and specific manner. The government has taken important steps to ensure effective coordination, most notably through the NECC, which sets the strategic priorities for the system's response to economic crime and tasks the UK's law enforcement response.

In this role the NECC has brought together agencies and intelligence in a way that has been integral to several areas of successful enforcement activity. The NECC has helped facilitate a number of interventions to prevent, prepare, and protect against economic crime, and to pursue those responsible for it, including through targeted communications on emergent threats.

The NECC's capabilities were displayed in work to improve government's collective knowledge of the company formation system, as well as the risks associated with the Trust and Company Service Provider (TCSP) sector through joint working with the NCA's National Assessment Centre, HMRC, and private sector partners. Several intelligence assessments have now been produced on these issues, contributing to the increase of the risk level applied to the TCSP sector in the 2020 National Risk Assessment from MEDIUM to HIGH.

The NECC's approach to assessing economic crime threats and how they are changing is imperative to ensuring capabilities and resources are focused on the highest priority threats causing or likely to cause most harm. This consolidated view of economic crime threats was vitally important in pulling together and coordinating our response to, for example, economic crime related to Covid-19 across 2020 and 2021.

The UK Financial Intelligence Unit (FIU), an operationally independent arm of the NECC within the NCA, has the national responsibility for receiving, analysing, associated decision-making and disseminating Suspicious Activity Reports (SARs), and makes all SARs available to appropriately trained officers in law enforcement agencies and other approved bodies for their own analysis and investigations (with the exception of SARs in certain sensitive categories). It is important to note that the UK SARs regime takes an 'all-crimes' approach—any suspicions of money laundering or financing of terrorism must be reported to the FIU.

The FIU works in close partnership with other key international organisations. For instance, the FIU is an active member of the international Egmont Group of Financial Intelligence Units, set up to improve cooperation in the fight against money laundering and the financing of terrorism.

The NECC also hosts the Proceeds of Crime Centre and the Expert Laundering Evidence cadre which provides impartial expert evidence to courts hearing money laundering cases throughout the UK, so that the courts can better understand complex money laundering methodologies, and an interpretation of evidence.

It is through this ability to coordinate that the NECC can facilitate interventions to prevent, prepare, protect against economic crime, and to pursue those responsible for it, including through targeted communications on emergent threats. We believe that the NECC operates effectively in its role, and that whilst there could be benefits from unifying law enforcement within a simple department, the size and scope of the new body would likely by unwieldy and ineffective in delivering operational outcomes.

Law enforcement agencies themselves appear to note the mismatch between the scale of the problem and the response. Given the harm involved in economic crime, whether directly affecting consumers or not, the Government must consider why it seems not to be a priority for law enforcement, and how it can ensure it becomes one. The Government must ensure that law enforcement agencies are appropriately resourced to tackle the scale of the problem. (Paragraph 57)

Economic crime is a priority for law enforcement agencies, and the government is committed to ensuring enforcement can continue to make the UK an even more hostile place for illicit finance and economic crime.

The sustainable funding model the government has developed is intended to ensure enforcement agencies are able to crack down on dirty money and financial exploitation, to protect the UK's security and prosperity. Through increased investment of £400m over the SR period, prioritisation across agencies and legislative changes the government is tackling the problem of economic crime head on.

Supporting this, the government has introduced powers for law enforcement agencies to seize the proceeds of crime and deny criminals and corrupt elites' access to their assets. It has also enhanced its ability to sanction individuals through the Global Anti-Corruption Sanctions Regulations.[9] These sanctions freeze the assets of the designated individuals and make it a criminal offence for anyone to make funds or economic resources available to them. The new dedicated Kleptocracy cell in the NCA will also target sanctions evasion and corrupt assets hidden in the UK.

We are also increasing law enforcement investigative capacity in the City of London Police, as national lead force for fraud, and in Regional Organised Crime Units across England and Wales.

Since 2014 an average of 1,778 prosecutions and 1,174 convictions have been undertaken annually for standalone money laundering cases or where money laundering is the principal offence. Taking into consideration all cases involving asset recovery (not just money laundering) agencies have recovered over £1.3 billion since 2015/16 using the

9 The Global Anti-Corruption Sanctions Regulations 2021 (legislation.gov.uk)

Proceeds of Crime Act powers. In the financial year 2020/21, £219 million was recovered in the proceeds of crime in England and Wales, Northern Ireland, and those with no recorded jurisdiction.

We recommend that, in its response to this Report, the Government sets out the legislation which is being worked upon across Government and that is relevant to addressing economic crime and provides an assessment of the measures that might be required to be brought in through an Economic Crime Bill, the timescales for this, and why it has chosen not to bring forward such a bill at this time. (Paragraph 61)

Since the committee published its report, the government has made several announcements about future legislation. A summary of key legislative activity is provided below.

The Economic Crime (Transparency and Enforcement) Act

In response to Russia's invasion of Ukraine the government urgently brought forward the Economic Crime (Transparency and Enforcement) Act to crack down further on dirty money and corrupt elites in the UK. The Act passed through Parliament on an expedited basis to receive Royal Assent on 15 March.

This Act introduces a new register which will require anonymous foreign owners of UK property to reveal their real identity, ensuring that they can't hide behind secretive chains of shell companies. In an amendment to the draft legislation, the act also now requires reporting of trustees, beneficiaries, settlors and protectors of trusts and trust like structures that run offshore companies that own UK property through the register. The legislation will level the playing field with property owned by UK companies, who already need to disclose their beneficial owners to Companies House.

The Act will also enable Unexplained Wealth Orders (UWOs) to be sought against property held in trust and other complex ownership structures such as opaque foundations. It also removes key barriers to the use of UWOs by increasing time available to law enforcement to review material provided in response to a UWO and reforming cost rules to protect law enforcement incurring substantial legal costs following an adverse ruling.

Reforms made through the Act to section 146(1) of the Policing and Crime Act 2017 will change the basis on which HM Treasury can impose a monetary penalty for a breach of financial sanctions. There will no longer be a need for the Treasury to prove that those who breach financial sanctions knew or had reasonable cause to suspect that they were doing so. Amending the current civil legal test will strengthen the Office of Financial Sanctions Implementation (OFSI's) ability to take appropriate enforcement action against companies that fail to ensure they are not dealing with sanctioned individuals or entities. This change to the civil legal test will bring the provisions for financial sanctions closer to those for the import and export of arms and that used by US sanctions enforcement. The government believes that a strict liability test accompanied by guidance best allows for robust enforcement of financial sanctions whilst also allowing OFSI to take into consideration a wide range of factors, including self-disclosure, proportionality, public interest, and steps taken by companies and individuals to ensure they do not breach financial sanctions.

The Act will allow the government to move faster when sanctioning oligarchs and businesses, as well as intensifying its sanctions enforcement. The Act will allow the UK to align more rapidly with the individual designations imposed by our closest allies via an urgent designation procedure. It also simplifies the legal tests for the UK's own designations, allowing the government to act more quickly and make changes to further facilitate the designations of groups of individuals.

The forthcoming economic crime-focused Bill

The government has meanwhile published details of further legislation that is planned in the Third Session of this Parliament. This legislation will deliver fundamental reform of Companies House, enhanced information sharing powers to give businesses more confidence to share information on suspected money laundering, and new powers to seize crypto assets from criminals, as the proceeds of crime are increasingly held in the form of cryptoassets. These powers are designed to clamp down further on money laundering and illicit finance.

While the government is preparing the Economic Crime and Corporate Transparency Bill at pace, more time is needed as it will feature substantial changes to UK company and partnership law, which we need to get right.

The reforms to Companies House amount to the largest change to the UK's system of setting up and operating companies since the companies' register was created over 170 years ago. The Corporate Transparency and Register Reform White Paper published on 28 February provides considerably more detail on the way the reforms will operate, and it will help the UK's business community, law enforcement agencies and all stakeholders to start to prepare for the changes to come.[10]

The White Paper sets out, for the first time, the new statutory function for the Registrar to maintain the integrity of the register of Companies. Company agents from overseas will no longer be able to create companies in the UK on behalf of foreign criminals or secretive oligarchs and new proposals will void the appointment of directors of UK companies who are disqualified, undischarged bankrupts or sanctioned under the Sanctions and Anti-Money Laundering Act 2018.

The upcoming primary legislation will also feature the widest changes to limited partnership law since 1907. It is vital that the UK maintains ease of doing business for legitimate commerce and avoids a chilling effect on inward investment. These reforms will affect every incorporated business in the country, and it was right that the government consulted on them extensively. Similarly, new powers which will enable the seizure and recovery of crypto assets are complex. It is vital that the reforms are not rushed.

The Online Safety Bill

More widely, on 9 March, the government announced a new standalone duty requiring firms to tackle fraudulent advertising as part of the Online Safety Bill. For the first time, companies will have to proactively tackle these advertisements. The duty will apply to user-to-user services that have the highest reach such as Facebook, and to search functions like Google. This will include the biggest publishers of online adverts.

10 Corporate Transparency and Register Reform White Paper (publishing.service.gov.uk)

More detail on the Online Safety Bill is set out later in this document.

Changes to the Money Laundering Regulations

Further to upcoming primary legislation, HM Treasury will be making necessary updates to the Money Laundering Regulations (MLRs) through secondary legislation in a 2022 Statutory Instrument. The government is also carrying out a broader review of the MLRs and the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) regulations this year.

HM Treasury published a consultation document on the proposed Statutory Instrument in July 2021 and engaged with key stakeholders on the changes we intend to make to the MLRs, in a series of engagement sessions throughout Autumn 2021. Feedback gathered from industry, supervisors and the broader public will help to better inform the final Statutory Instrument, which is due to be laid in 2022.

This will be followed by the broader review of the MLRs, which will shape the direction of the UK's anti-money laundering (AML) regime for the coming years.

It is vital that AML regulation keeps pace with technology, so that no part of our financial system becomes a place where criminals can evade checks and controls. This is why the Statutory Instrument will include measures to extend the FATF Recommendation 16—known as the "travel rule"—for cryptoasset firms. This change will require information on the identity of the originator and beneficiary of a transfer of funds or assets is sent and recorded by the firms making the transfer. The Statutory Instrument will also make other discrete, mature changes to strengthen and clarify how the regime operates.

HM Treasury also laid a Statutory Instrument amending the MLRs, which was made in February 2022. This made minor changes to the provisions relating to HMRC's Trust Registration Service (TRS)—which requires trustees of UK express trusts, and non-UK express trusts with certain links to the UK such as the acquisition of UK property to register details of their beneficial ownership—to ensure that trustees have sufficient time to register and made changes to the types of trusts required to register.

HM Treasury updated its list of high risk third countries to ensure this continues to mirror countries identified by the FATF as having strategic deficiencies in their anti-money laundering and counter terrorist financing regimes. The most recent update was made via secondary legislation on 28 March 2022, ensuring the UK financial system continues to remain protected from those jurisdictions which have poor money laundering and terrorist financing controls, and that the UK remains in line with international standards to combat money laundering and terrorist financing.

Online Economic Crime

We agree with the Joint Committee that the Draft Online Safety Bill should be amended so as to include fraud offences in the list of "relevant offences" in Clause 41(4) of the Bill. Fraudulent content should be designated as "priority illegal content", thereby requiring online firms to be proactive rather than reactive in removing it from their platforms. These steps would place greater responsibility on online companies to prevent their platforms from being used to promote financial fraud, something of

which these online firms are capable. (Paragraph 74)

We reiterate our strong belief that the Government should include measures to address fraud via online advertising in the Online Safety Bill, in the interests of preventing further harm to customers being offered fraudulent financial products. (Paragraph 94)

The government introduced the Online Safety Bill[11] on 17 March 2022, shortly after announcing that fraud and money laundering offences would be included as priority illegal content. This means that regulated companies will have to take strong action in ensuring their users are protected from this harmful user-generated content. This will extend beyond just swifter removal of materials; firms will now have to proactively implement measures to prevent fraud on their services. This will combat some of the most harmful fraud types, such as romance and investment scams, as well as driving down enabling crimes such as the recruitment and use of money mules.

Following detailed evidence provided at the Joint Committee on the Draft Online Safety Bill and comprehensive feedback from our partners, the government amended the Bill to include a fraudulent advertising duty requiring the largest and most popular social media platforms and search engines to prevent paid-for fraudulent adverts appearing on their services.

Ofcom will set out further details on what platforms must do in codes of practice. This may include measures such as checking the identity of those who wish to publish advertisements and ensuring that financial promotions are only made by firms authorised by the Financial Conduct Authority (FCA).

The Government should consider whether online platforms and social media companies should be required to do Know Your Customer checks on their advertisers, to make it more difficult for fraudsters to promote themselves. We welcome the steps taken by certain online firms to take a clearer line in facilitating access to their platforms only for financial promotions placed by entities which are authorised by the FCA. We urge other online companies which have not made such commitments to follow suit. (Paragraph 95)

Ofcom will be producing codes of practice to outline the application of the new fraudulent advertising duty. Measures could include verification checks by the regulated company ahead of entering a business arrangement with a potential advertiser and ensuring that financial promotions are only made by firms authorised by the FCA.

Following the UK's exit from the European Union, the government made changes to the financial promotions regime. This has led to Google putting in place a new policy to ensure only authorised firms or firms with promotions approved by an FCA authorised firm can advertise financial services products through their platform. Other platforms have committed to put in place similar policies in the future.

The Government should not allow online companies to ignore legislation designed to protect consumers from harm. The Government should ensure that financial services advertising regulations apply also to online companies, and that the FCA has the necessary powers to effectively enforce the regulations. (Paragraph 96)

11 Online Safety Bill publications - Parliamentary Bills - UK Parliament

It is not appropriate that online companies should profit both from paid-for advertising for financial products and from warnings issued on their platforms by the Financial Conduct Authority (FCA) about those advertisements. We urge all online companies to work constructively with the FCA and to follow Google's example by giving advertisement credits to the FCA for the future. We also expect them to refund money that has been spent in the past by the FCA. (Paragraph 97)

On 9 March, the government announced a new standalone duty requiring firms to tackle fraudulent advertising as part of the Online Safety Bill. For the first time, companies will have to proactively tackle these ads, instead of potentially benefiting financially from paid-for fraudulent advertising. The government will be working with Ofcom, who will be producing codes of practice to outline the application of the duty. We expect online companies to do their utmost to tackle fraudulent advertising, including verification checks by the regulated company ahead of entering a business arrangement with a potential advertiser; proactive inspection measures to ensure the safety of the advert; and controls to ensure that fraudulent adverts are speedily removed.

Separate to the new fraudulent advertising duty, the FCA already has a range of supervisory and enforcement powers available to enforce financial promotion rules on the internet. To promote a financial product, a firm must either be authorised by the FCA or have its advertisement approved by an FCA-authorised firm. This means that authorised firms must not approve the content of a financial promotion unless they are satisfied that the promotion meets the FCA's rules.

Where a financial promotion fails to comply with the FCA's rules, the FCA already had a wide range of powers to deal with this, including to require the withdrawal of the promotion.

Financial adverts hosted on online platforms now need to be communicated or approved by an FCA authorised person. As mentioned above, the government brought this about through a change to the financial promotion regime following our exit from the EU. The changes mean online platforms can no longer rely on an exemption to the financial promotions' regime for their paid for advertising.

Following this change, and after significant engagement between the FCA and government, Google announced a new Financial Services Verification policy to ensure only FCA authorised firms or firms with promotions approved by an FCA authorised firm can advertise financial services products on Google. Other platforms have committed to put in place similar policies.[12]

We recognise that placing a responsibility on online companies to reimburse consumers who are victims of online fraud could rapidly transform their approach to fraud. Any move to force online firms to compensate victims of fraud should not be to the detriment of the outcomes for consumers already achieved through the compensation banks and other financial institutions pay. The consumer should see no loss of speed or amount in repayment. (Paragraph 101)

12 Major technology companies step up efforts to tackle financial fraud and scam adverts (techuk.org)

We recommend that the Government seriously consider whether online companies should be required to contribute compensation when fraud is conducted using their platforms. (Paragraph 102)

Every company owes it to their customer to protect them from fraud and support them when they have fallen victim. Consumer safety should be the core guiding principle at the heart of every business model. We are working closely with technology companies and partners in law enforcement and civil society to consider every possible option to support victims of online fraud and to mitigate the harm that they have experienced.

The Joint Committee on the Draft Online Safety Bill concluded that self-regulation of online platforms had failed. It is true that there have been many failings, and it is right that action should now be taken to place more responsibility on online firms to prevent harm from fraud and other economic crimes which their platforms and services have facilitated. However, the formation of the Online Fraud Steering Group is evidence that co-operative working between the private and public sectors can help improve outcomes and compliance. A number of online companies also showed in their evidence to us that they are taking a more constructive approach to co-operation with law enforcement agencies. (Paragraph 103)

We welcome the setting up of the Online Fraud Steering Group, and we encourage all online companies to work constructively with Government agencies and the wider public sector to fight online scams and fraud. The Government is correct to recognise in this area, as in the Economic Crime Plan more generally, that a public-private partnership approach is needed. (Paragraph 104)

The Government should build on these foundations when it updates the Economic Crime Plan. But it should also ensure that regulators and law enforcement agencies have the powers they need to ensure that online companies provide them with information and comply with regulatory requirements. (Paragraph 105)

The government welcomes the Committee's support of the establishment of the Online Fraud Steering Group and its sub-groups. We look forward to seeing the products of this partnership, both in developing the collective understanding of the threat and new actions to counter it.

The public-private partnership is essential in tackling fraud, and it is vital that the technology sector and online companies play their part. That is why in October 2021, the Home Office relaunched the Joint Fraud Taskforce, chaired by the Security Minister. The Joint Fraud Taskforce has an extended membership, including representation from the technology and online sectors for the first time.

The Online Safety Bill represents a new, game-changing regulatory regime overseeing the online and tech sectors. The expectation under this Bill is that all regulated companies comply with the codes of practice being led by Ofcom and do all they can to protect their users from harm. The bill outlines the penalties for breaching this regulation including substantial financial penalties.

The Home Office is also intending to launch a technology and online sector charter with industry. This will include private and public actions that will drive down fraud in these sectors. This follows the publication of a series of voluntary charters with the retail banking, telecommunications, and accountancy sectors in October 2021.

The Government will consider all opportunities, including legislation, to ensure that the public are kept safe from these terrible crimes and that law enforcement have the powers needed to bring those who commit them to justice.

Authorised Push Payment Fraud

The work of the Payment Systems Regulator to improve the Contingent Reimbursement Model Code is welcome, as is the Government's confirmation that it will introduce any necessary legislation to that end. Together, these steps will help improve consumer outcomes and reduce fraud. (Paragraph 116)

However, the pace of change has been very slow against a background of growing fraud, which should have prompted greater urgency. The super-complaint was made in 2016, and the previous Treasury Committee called for the Contingent Reimbursement Model Code to be made mandatory in 2019. Since then, nearly three years have passed, during which time authorised push payment fraud has increased, causing significant harm. The Payment Systems Regulator's 'Call for views' was published in February 2021 and, although there is now a clear intention to make reimbursement mandatory, another year has been lost. (Paragraph 117)

We recommend that the Government urgently legislates to give the Payment Systems Regulator (PSR) powers to make reimbursement mandatory, and that the PSR then take rapid action to protect consumers. We recommend that the PSR and Treasury accelerate their consultation processes to enable quicker implementation of measures to protect consumers from fraud. (Paragraph 118)

We recognise and share the Committee's concerns regarding payments fraud. The government is committed to tackling fraud within payment networks and recognises the actions of the financial services industry to help tackle Authorised Push Payment fraud.

The government has recognised the actions of the financial services industry to reduce Authorised Push Payment fraud, including investment in anti-fraud capabilities, the creation of a voluntary reimbursement Code, and the implementation of initiatives such as Confirmation of Payee. However, there is more that needs to be done to prevent these scams, and to ensure that victims are not left paying for fraud through no fault of their own.

The government therefore welcomed the publication of the Payment Systems Regulator's Consultation on further measures to counter Authorised Push Payment scams on 18 November. In developing their approach to Authorised Push Payment scam reimbursement, the Payment Systems Regulator identified a barrier in the Payment Services Regulations 2017 preventing it from using its existing regulatory powers to introduce mandatory Authorised Push Payment scam reimbursement for scams which occur over Faster Payments. As such, in November 2021 the Economic Secretary stated that the Government would legislate at the earliest opportunity to address these barriers

to regulatory action on Authorised Push Payment fraud.

We welcome the introduction of the Confirmation of Payee service in 2019, as recommended by our predecessor Committee. We also welcome the work the Payment Systems Regulator is doing to broaden its scope through the introduction of Phase 2, extending and enhancing the service. (Paragraph 123)

We recommend that the PSR supplies a report to our Committee on progress in the implementation of Phase 2 by the end of 2022. (Paragraph 124)

Improving data-sharing between banks is one of the measures which the PSR is implementing as part of its reform of the CRM Code. The Treasury should be ready to bring forward any legislation which is needed to enable this, and the PSR should ensure that banks act quickly in putting in place the necessary changes. (Paragraph 125)

The government welcomes the steps being taken by the Payment Systems Regulator to reduce fraud, including the widening of Confirmation of Payee and the Consultation on Authorised Push Payment scams, which includes data-sharing proposals. Although HM Treasury does not currently foresee the need for enabling legislation in relation to the Payment Systems Regulator's data sharing proposals, we continue to work closely with the Payment Systems Regulator across its anti-fraud agenda.

The Payment Systems Regulator intends to issue its own response to the recommendations directed towards it by the Committee.

Anti-money laundering

The National Crime Agency is right to focus on Suspicious Activity Reports as a priority, and we welcome the much-needed investment in new IT systems and the plans for increasing staff and analytical capacity. The SARs reform programme is likely to improve anti-money laundering systems and the ability of law enforcement agencies to handle large numbers of SARs quickly and effectively, to make full use of them in the fight against economic crime and organised crime more generally. (Paragraph 141)

It is, however, disappointing that the SARs reform programme is not yet complete and that no timetable or target date for its completion has been published. A timeline showing when the SARs reform programme milestones are expected to be met, and an annual progress report on the programme, should be provided to this Committee. (Paragraph 142)

But the SARs reform programme is not an end in itself—it can only deliver change if the law enforcement agencies have the ongoing capacity and funding to tackle the criminal activity indicated by SARs. Responsibility lies with the Government to make available all the resources needed by the Home Office, regulators, and crime-fighting agencies if they are to have any meaningful impact on criminal activity indicated by SARs. (Paragraph 143)

Milestones for SARs Reform delivery were published by the government in the Economic Crime Plan Statement of Progress (May 2021).[13] The reform programme is performing well, with a number of core components of the programme now complete.

The SARs Reform Programme is at the heart of improving the performance of the Anti-Money Laundering (AML) system. SARs intelligence is a critical tool in our ability to identify, disrupt and recover the hundreds of millions of pounds which underpins the most serious and organised crime in the UK. Through the increased investment over the SR period, funding will be provided to ensure changes being implemented by the programme, such as maintaining the new SARs digital service and the increased staffing levels in the UKFIU and ROCUs are delivered. This will enable the SARs Reform Programme to help the AML regulated sector prevent money laundering and disrupt more criminality through SARs intelligence.

The SARs Reform Programme focusses on three key areas of change, with good progress being made across each:

1. **Uplifting staffing***:* to increase capacity within law enforcement to analyse and act on SARs intelligence. This includes 75 additional officers in the UKFIU which will almost double capacity. 45 of these officers are already in post and the milestone for recruiting the remaining 30 is the end of FY 2022/23. The programme has also provided more than 20 new financial investigators in the Regional Organised Crime Units (ROCUs) dedicated to SARs analysis. These new staff are already delivering operational results from SARs intelligence including the recovery of criminal assets (£380,000 to date this year, with a further c. £1 million frozen) and identification and arrest of previously unknown Organised Crime Group members.

2. **IT transformation**: a new SARs Digital Service including data analytics, to replace legacy IT implemented more than 20 years ago. The first elements of the new SARs IT systems (Bulk Reporter submission) were delivered in early 2021, to enable organisations that submit large volumes of SARs (bulk reporters) to begin testing the new systems. To ensure consistency of service, de-risk delivery and ensure the protection of the public, the end-to-end SARs Digital Service will be delivered in stages. The new SARs Online Portal and bulk submission method will go live first from summer 2022. This will be followed by further releases, which will replace the current SARs IT used by the UKFIU, Law Enforcement Agencies, and other Government Departments.

3. **Legislation and guidance**: covering improved guidance and better feedback to the private sector who report SARs, and legislative exemptions to Defence Against Money Laundering (DAML) SAR reporting to reduce the volume of ineffective reports. The additional staff in the UKFIU have enabled significantly increased UKFIU feedback and engagement, with 90% of bulk SARs reporters (banks) feeding back that the engagement with NCA on SARs is better than 12 months ago. Changes introduced in 2021 through the Financial Services Bill brought Electronic Money Institutions into scope of existing reporting exemptions, resulting in c.10,000 fewer low value DAMLs this year. Further legislative change that could cut the number of DAMLs by 50%, freeing up staff to focus on high value activity, will be introduced with the second part of the Economic Crime Bill.

13 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf

The effectiveness of SARs might be increased if banks are permitted to share information with the National Crime Agency and other law enforcement agencies before the suspicion threshold required under existing anti-money laundering legislation is reached. (Paragraph 144)

Banks are already permitted to share information with the National Crime Agency before the suspicion threshold required under the Proceeds of Crime Act (2002) is reached, using the gateway provided by Section 7 of the Crime and Courts Act (2013). Disclosures can be made using this gateway without the suspicion threshold having been reached.

Public-private partnership actively led by the NECC within the JMLIT+ model, already takes advantage of this gateway to share information quickly and in a targeted way. As of early 2022, information was being shared activity across a range of subjects including cash-based money laundering, fraud and scams, with the intention of disrupting economic crime, including through prevention. Information received from the private sector is a vital part of producing alerts and intelligence assessments, which help partners close vulnerabilities and prevent criminal activity.

As part of the targeted engagement for the Economic Crime Bill the government consulted on legislation that would facilitate greater information sharing between businesses. The response from industry varied with strong support from the financial sector but mixed appetite from other AML regulated sectors, who questioned the utility in their particular sectors and expressed concerns about the administrative burdens it might place on smaller firms. Utilising the feedback from the consultation, it remains the government's intention, as part of a forthcoming Economic Crime Bill to create the legislative framework that would enable greater information sharing across the private sector for the purposes of preventing and detecting economic crime, whilst protecting the rights of individual customers.

Whilst the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) has made good progress, it is disappointing that nearly four years after it was set up, it is still encountering poor performance from a large proportion of the professional bodies that it supervises. There needs to be a plan to ramp up compliance in this sector, by resourcing OPBAS to do more checks and to allow it to take punitive action against professional body supervisors. (Paragraph 153)

OPBAS's three reports evidence welcome improvements in Professional Body Supervisors' (PBS) technical compliance with the requirements under the Money Laundering Regulations, which has enabled OPBAS to focus more on the effectiveness of their AML supervision. It is on this front that, despite examples of good practice, there are weaknesses and scope for PBSs to make significant improvements.

OPBAS continues to evolve a robust approach to PBS supervision, using a wider range of methods to enrich its understanding of risks and drive more effective supervision by PBSs, and will continue to intervene where PBSs do not make the required progress. OPBAS is independently funded by fees charged to PBSs.

HM Treasury's current review of the Money Laundering Regulations and OPBAS Regulations is assessing the progress that OPBAS has made since its creation and, as part

of the broader assessment of the structure of the UK's supervision regime, will consider if OPBAS's remit and powers remain appropriate. It will also identify opportunities for intensifying OPBAS supervision and the potential for enhanced enforcement powers.

The forthcoming Government review of the regulatory and supervisory regime for anti-money laundering and counter-terrorist financing, expected to conclude by June 2022, needs to address the concerns we have heard in this inquiry about the limited forward steps in compliance that OPBAS has so far secured. The problems which OPBAS identifies are similar to those which our predecessor Committee highlighted in 2019, shortly after OPBAS had been set up. We recommend that the review should not shy away from considering radical reforms, including a move away from the self-regulatory model and the creation of a new supervisory body, potentially independent of the FCA, which takes more direct responsibility for policing professional body compliance with anti-money laundering regulations. The review should also take a hard look at enforcement measures which apply to professional bodies. (Paragraph 154)

The case for a supervisor of supervisors—including statutory supervisors—is still as it was at the time of our report in in 2019. We recommend that this idea should also be considered by the review. (Paragraph 155)

HM Treasury's ongoing review of the MLRs and OPBAS Regulations offers the opportunity for one of the most comprehensive assessments of the UK's anti-money laundering/ counter-terrorist financing (AML/CFT) regime in years. HM Treasury has engaged widely with stakeholders in both the public and private sectors to inform the scope of the Review, including through a call for evidence which ran from July to October 2021.

A key aim of the MLRs Review is to ensure there is effective, responsive AML supervision across the UK's regulated sector. The Call for Evidence asked broad-reaching questions about the structure of the UK's supervision regime. Questions in the Call for Evidence also invited views specifically on the effectiveness and sufficiency of existing enforcement measures.

There have been clear improvements across the UK supervisory regime and PBS compliance with the MLRs, reflected in sector feedback and examples of more robust enforcement. Policy objectives in this area have been largely met, with the need for a focus on overall effectiveness rather than technical compliance moving forward. OPBAS will continue to take action with PBSs when appropriate, to ensure that consistent high standards of compliance are achieved.

The MLR Review is considering the work of OPBAS to drive the consistency and efficiency of PBS supervision, and in parallel to the assessment of the structure of the UK's supervision regime will consider what future remit and powers OPBAS should have. Statutory supervisors (the FCA, HMRC and the Gambling Commission) are public bodies who are directly accountable to Parliament for their work and HM Treasury works closely with all three supervisors on their AML supervision. Any decision on the future model of supervision used by the UK would have significant consequences and must be informed by in-depth analysis and consideration of the implications for the UK's overall efforts to prevent money laundering and terrorist financing.

HM Treasury will respond to Call for Evidence responses and set out next steps in the report on the Review's findings, due to be published in June 2022.

We note the actions taken by HMRC since its previous inquiry to improve its performance in supervising anti-money laundering (AML). However, HMRC's self-assessment of its performance is not truly independent, and we recommend that HMRC finds a way to provide the assurance of independent assessment. (Paragraph 166)

HMRC takes a risk-based approach to the supervision of the 37,000 firms it supervises, using a combination of on-site inspection and desk-based reviews to assess understanding and compliance, and taking robust action where failings are found. Throughout the pandemic, HMRC has continued to detect and address non-compliance, issuing sanctions, including 41 financial penalties and preventing inappropriate businesses from trading, suspending 14 MLR registrations and cancelling 11 others. In addition, HMRC have prevented 235 businesses from trading by refusing their registration.

The individuals who undertake the HMRC self-assessment are appointed from outside the Economic Crime Supervision team in HMRC. They understand their obligation to undertake an impartial review of HMRC's performance and report the assessment's findings, both in a detailed internal review, agreed by HM Treasury, and a published public version. Both OPBAS and HM Treasury are consulted and sighted prior to finalisation of the reports.

HMRC is responsible for anti-money laundering supervision in a number of risky sectors, such as Trust or Company Service Providers (TCSPs). There are signs that HMRC could improve its supervisory performance in that sector and other risky sectors. HMRC should seek to be more proactive in preventing TCSPs facilitating the use of UK companies for money laundering and should aim to drive up significantly the numbers of SARs from that sector. We note that this issue is linked to Companies House reform, which we address in Chapter 7. (Paragraph 167)

The government is very conscious of the risks posed by the abuse of UK companies. Companies can be formed directly with Companies House or through TCSPs supervised by HMRC or professional bodies (such as lawyers and accountants). HMRC supervises less than 10% of UK TCSPs and some HMRC-supervised specialise in selling companies to professional service providers such as lawyers and accountants who then make these companies available to their own clients. As such, a whole system response is required to the risks around TCSPs, including through Companies House reform, and this response addresses the issues rather than focusing on any particular agency.

HM Treasury is co-ordinating a cross-agency Action Plan to tackle the risks posed by abuse of UK companies, including through TCSPs and HMRC are very much committed to playing a part in that work. For this reason, HMRC have intensified their supervision of TCSPs, including through the successful completion of a week of action (in October 2021), which included promoting an updated TCSP risk assessment, hosting an online seminar on risks associated with Registered Office Address services and speaking at three industry conferences, and reviewing those publicly advertising formation services to ensure they were properly supervised.

HMRC also conducted on-site compliance inspections at 90 TCSP premises. In December 2021, HMRC published its latest list of penalties for the non-compliant.[14] This included 3 penalties imposed on TCSPs. The Government intend to continue to focus on supervisory efforts on high-risk activities, including TCSPs.

The government recognises the value of SARs and that the levels of reporting from TCSPs are, on the face of it, low. In large part, this may be due to the fact that businesses self-identify when making a SAR, and they generally do not identify themselves as TCSPs, but instead report under their primary business sector, (e.g. lawyer, accountant, serviced office providers) rather than as a TCSP. The government will continue to focus on this issue.

For its part, HMRC guidance explains the importance of reporting suspicions of money laundering or terrorist financing by filing SARs and this message is reinforced by HMRC webinars and attendance at trade body meetings and conferences, including jointly with the NCA.

HMRC works closely with the NCA's Financial Intelligence Unit on promoting this message, arranging for them to speak at trade conferences and has agreed to jointly host a bespoke webinar on the subject of SARs targeted at TCSPs about the risks they need to be aware of and their reporting obligations when they come across suspicious activity.

To improve TSCPs' understanding of, and compliance with, the Money Laundering Regulations, HMRC works closely with the other TCSP supervisors and has published improved and updated risk information for the sector. HMRC's compliance interventions, guidance, webinars and trade body engagement have helped TCSPs improve their own risk assessments. Whilst the majority of the supervised population wants to be compliant, getting risk assessments right is an area of concern to all supervisors. HMRC will continue to focus on improving these across the sector as good risk assessment is fundamental to TCSPs' overall effectiveness in guarding against criminal exploitation of their services

HMRC addresses the quality of risk assessments right from the point when businesses apply to be supervised. The processes for checking that key TCSP personnel are 'fit and proper' before being allowed to start TCSP activity has been made more rigorous. HMRC's supervision already targets higher risk TCSPs, using a risk- and intelligence-led approach. HMRC TCSP compliance inspection activity has been centred on those assessed as providing higher risk services, supported by a public/private threat assessment (PPTU) project led by the NECC which identified specific higher risk businesses for cross-agency follow-up.

We recommend that HMRC's role as a supervisor is reviewed as part of the HM Treasury review of the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, due by June 2022. That review should also focus on what can be done to improve money laundering compliance by trust or company service providers. (Paragraph 168)

As mentioned in our response to paragraph 154 of the TSC report, HM Treasury is currently conducting a review of the AML supervisory landscape and OPBAS's role

14 https://www.gov.uk/government/publications/businesses-not-complying-with-money-laundering-regulations-in-2018-to-2019/list-of-businesses-for-tax-year-2019-to-2020-that-have-not-complied-with-the-2017-money-laundering-regulations

which will consider the case for changes. Our response to paragraph 167 refers to cross-Government work being led by HMT to address the risks posed by abuse of the TCSP sector.

The new assertive approach by the FCA is welcome. The prosecution of NatWest is a major success, and the Committee congratulates the FCA and everyone in the team working on it. The level of the fine should be a deterrent to others. The question is whether this was an isolated case or whether more prosecutions of banks and financial institutions for money laundering will follow. While that would show effective enforcement, it would also signal that money laundering controls are not working as they should be within the institutions prosecuted. (Paragraph 179)

The FCA successfully prosecuted NatWest for past anti-money laundering controls failings, representing the first prosecution of a bank under the Money Laundering Regulations 2007. This milestone achievement demonstrates the willingness and capability of the FCA to make use of the full range of powers available to it under the MLRs. The government also welcomes NatWest's commitment to strengthening its anti-money laundering controls and procedures since the offences in question.

The significant fine of £264.8 million, imposed by Southwark Crown Court in December 2021, follows other civil penalties imposed directly by the FCA for failures of banks' financial crime controls. For example, the FCA fined Standard Chartered Bank £102.2 million in 2019 and Credit Suisse £147.2 million in 2021.

Landmark cases such as the NatWest prosecution are just part of the broad range of supervisory and enforcement activity undertaken by the FCA. It continues to target activity at the areas of greatest risk, and as of August 2021 had approximately 46 open financial crime investigations into firms and individuals.[15]

We will continue to monitor the de-risking of customers by banks. We recommend that the FCA report annually on numbers of de-risking decisions and on progress to ensure that banks are not unfairly freezing bank accounts and de-risking customers. (Paragraph 186)

Banks and all other financial institutions are required by the MLRs 2017 to apply customer due diligence measures at key stages in a business relationship in order to detect and prevent money laundering. Firms will consider a range of factors as part of this (e.g. nature of the business or its location).

The government continues to work closely with the Joint Money Laundering Steering Group (JMLSG) who publish the anti-money laundering guidance for the financial sector. The JMLSG guidance advises UK firms how to apply the UK's Money Laundering Regulations in a proportionate manner and to act based on the risks presented in each individual case.

The UK Finance (UKF) website hosts an online guide to help businesses prepare when opening or switching to a new current account. The streamlined checklist provides essential details and documents that most businesses will need to open an account.

15 This figure was given by the FCA as part of their response to HM Treasury's annual supervision data collection, which informs the AML/CFT annual supervision report.

Ultimately the decision to exit a banking relationship is a commercial decision for banks, subject to some restrictions to choose with whom they do business. Account exit and freezing is an important and legitimate response to suspicions of money laundering and other economic crime. The government is focused on ensuring that decisions made by banks are proportionate, and that the actions of banks and their customers are informed by clear guidance about what the regulations require.

The FCA collect and publish information from their supervised population on the operation of their financial crime systems and controls, including information on the number of accountants that are exited for financial crime purposes. The FCA does not routinely collect data on firms freezing accounts, but firms are expected to investigate any accounts they freeze in a timely manner and to unfreeze them when appropriate.

Cryptoassets and economic crime

We note the increasing risks around cryptoassets and economic crime. We share the Government's concern about the risk to consumers from the growth in the market for cryptoassets. We welcome the announcement by the Treasury that the Government will legislate to bring advertising of cryptoassets into line with that of other financial services and products, and that the FCA is strengthening financial promotion rules, including those for cryptoassets. (Paragraph 195)

The government notes the committee's support for HM Treasury's recent announcement of its intention to regulate cryptoasset financial promotions. FCA consumer research conducted in 2021 indicated that cryptoasset ownership in the UK has continued to grow, with an estimated 2.3 million people in the UK holding cryptoassets.

As more people decide to invest, it is essential that consumers have access to fair, clear, and not misleading information prior to any purchase. The government's approach to this topic as well as our wider strategy for cryptoasset regulation was set out in the Economic Secretary's keynote speech during Fintech week on 4 April.[16]

On 18 January 2022, the government set out its intention to legislate later this year to bring certain cryptoassets into financial promotion regulation. The measure, and supportive FCA rules, will regulate in-scope cryptoasset financial promotions, requiring them to be fair, clear and not misleading. This is aimed at improving consumers' understanding of the risks and benefits associated with cryptoasset purchases and ensuring that cryptoasset promotions are held to the same high standards as broader financial services products.

The decision to expand the scope of the Financial Promotion Order to capture certain cryptoassets complements broader proposals on cryptoassets and stablecoins set out via the government's consultation on a regulatory framework for stablecoins last year.[17] It also aligns with separate government proposals to strengthen the authorisation process for financial promotions.

16 Keynote Speech by John Glen, Economic Secretary to the Treasury, at the Innovate Finance Global Summit - GOV.UK (www.gov.uk)

17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1047232/Cryptoasset_Financial_Promotions_Response.pdf

The government will also bring forward further legislation to enable cryptoassets to be seized and recovered more quickly as soon as parliamentary time allows. In particular, the creation of a civil forfeiture power which would mitigate the risk posed by those that cannot be prosecuted but use their funds to further criminality.

The work being done by the Advertising Standards Authority to protect consumers from misleading advertisements for cryptoassets is also welcome. The Government should ensure that there is proper consumer protection regulation across the whole cryptoasset industry. (Paragraph 196)

The government believes that it is important that regulation supports innovation in the industry, while protecting consumers from harm. This extends to ensuring that the regulators of our financial system have the right tools to manage those risks.

In 2018 the government launched a cross-authority Cryptoassets Taskforce with the aim of exploring the impact of a rapidly developing cryptoasset market. UK authorities have taken a series of actions to support innovation while mitigating risks to stability and market integrity.

As previously noted, these include confirming an intention to legislate to regulate cryptoasset promotions, ensuring they are fair, clear and not misleading; and consulting on a proposal to ensure cryptoassets known as 'stablecoins' meet the same high standards expected of other payment methods. The government issued its response to this consultation in April 2022, confirming its intention to legislate to this effect.[18]

The FCA and Bank of England have warned that buying cryptoassets involves high risks, and that investors should be prepared to lose all of their money.

The government is carefully considering what, if any, regulation might need to follow as the cryptoasset market grows and evolves in the UK. The government has adopted a staged and proportionate approach to cryptoassets regulation, which is sensitive to risks posed, and responsive to new developments in the market. The Cryptoasset Taskforce will continue to steer the UK's regulatory response to the cryptoasset market.

The Government should set out in the Economic Crime Plan its intention that all cryptoasset firms should be registered for anti-money laundering (AML) purposes. This has not yet been achieved. It is unacceptable that, having introduced AML regulations for cryptoasset firms in 2020, there are so many firms which have not yet been registered. Large numbers have not even applied for registration, and it is not clear what sanction they face. (Paragraph 203)

While we acknowledge the need to ensure that the gateway for registration of cryptoasset firms for anti-money laundering should be a rigorous process, registration has been too slow. It needs to be speeded up, and the Government should work with the FCA to find a solution. The FCA should not extend the deadline for registration again beyond March 2022. If the FCA sees no alternative, it should write to the Committee to explain its position. (Paragraph 204)

18 https://www.gov.uk/government/consultations/uk-regulatory-approach-to-cryptoassets-and-stablecoins-consultation-and-call-for-evidence

If, as we recommend, the Government renews the Economic Crime Plan in 2022, it should consider instituting measures specifically to protect consumers from fraud and scams relating to cryptoassets. (Paragraph 205)

Since January 2020, cryptoasset firms have come within scope of the MLRs and the FCA has been the AML/CFT supervisor for cryptoasset firms. Under the MLRs cryptoasset firms must each conduct a money laundering and terrorist financing risk assessment, implement risk-based systems, policies, controls and procedures, carry out appropriate customer due diligence checks, and report suspicious activities to the authorities.

A robust AML regime for cryptoassets will help to bolster confidence in the UK as a safe and reputable place to start and grow a cryptoasset business. The government recognises the importance of having a robust system and intends to continue maintaining high standards. As the Kalifa review noted, the UK has a hard-won reputation of trust regarding regulation and the rule of law which we must build on.

As such, all cryptoasset exchanges and custodian wallet providers must be registered for anti-money laundering supervision with the FCA, if they are to carry on business in the UK. Since 10th January 2020, all new cryptoasset firms have had to be registered for AML supervision prior to commencing trading. Firms which were trading before this date have had to be registered with the FCA since 10 January 2021.

Due to delays in the processing of applications for registration, a number of firms which were trading prior to 10 January 2020, and which had submitted an application for registration to the FCA by 16 December 2020 were granted temporary registration via the Temporary Registration Regime. This approach has prevented undue disruption to established cryptoasset businesses and their customers, whilst ensuring the FCA are able to assess firms' applications at the appropriate level of detail and with suitable rigor. This has minimised undue disruption to both consumers and firms.

The FCA has concluded its assessment of all firms in the Temporary Registration Regime, which closed on 1 April for all firms but those where it is strictly necessary to continue to have temporary registration. This is necessary where a firm may be making representations to the FCA or may have particular winding-down arrangements. As of 13 April, 5 firms continue to have temporary registration, and all are aware of what is required of them to conclude their application.

It is a criminal offence for a person to provide cryptoasset exchange or custodial wallet services in the UK by way of business without being registered with the FCA. As the supervisor for the cryptoasset sector, the FCA is responsible for policing the regulatory perimeter, and is empowered to bring both civil and criminal enforcement actions against persons who are in breach of this requirement.

The government will bring forward further legislation to enable cryptoassets to be seized and recovered more quickly. In particular, this will include the creation of a civil forfeiture power which would mitigate the risk posed by those who cannot be prosecuted but use their funds to further criminality. The government takes seriously consumer fraud issues relating to cryptoassets, and is closely monitoring developments. It is the government's intention to ensure proportionate action on cryptoassets and potential economic crime risks they are considered as a core theme within the second iteration of the Economic Crime Plan.

Companies and economic crime

We are disappointed that the Government has not yet implemented reform of corporate criminal liability. The previous Committee presented convincing evidence of the need for this in 2019, already two years after the Ministry of Justice had run its consultation in 2017. The decision taken in 2020 to ask the Law Commission to review the law on corporate criminal liability is a sensible step, given the complexity of the law in this area, but it is likely to be years before any change in the law results. We urge the Law Commission to proceed with its review speedily, and we urge the Government to act quickly in bringing forward any legislation flowing from the Law Commission's review. In the meantime, corporate criminals will continue to be able to escape prosecution for economic crimes. (Paragraph 211)

The government intends to engage promptly with the Law Commission on the findings of the review once it has concluded.

It is important that any reforms are proportionate, and evidence based. This is an extremely complex area of the law, and a full assessment will need to be made of the impact of any proposed new offence as well as how it would interact with the existing criminal offences and regulatory regimes for money laundering and other forms of economic crime.

In particular, the introduction of any new failure to prevent or facilitation offence for would need to avoid cutting across existing reforms, including the Senior Managers and Certification Regime.

Reform of Companies House is essential if UK companies are no longer to be used to launder money and conduct economic crime. We welcome the work being done by the Department for Business, Energy, and Industrial Strategy and by Companies House to modernise the legal framework and operations of Companies House. However, the pace of change is slow. The problems with UK company structures were identified by the Government in 2014 in the UK Anti-Corruption Plan. While there have been welcome innovations, such as the People with Significant Control register, on current plans it will have taken over 10 years to improve matters, during which time a large number of UK companies may have been put to criminal use by a wide range of criminals. (Paragraph 230)

The UK is a global leader in beneficial ownership transparency. Last year, under the UK's leadership, all G7 countries committed to strengthening and implementing beneficial ownership registers. The UK is also driving forward ongoing discussions at the FATF to bolster its international standards on company beneficial ownership transparency, to ensure there are no weak links in the global financial system.

The government has brought forward expedited legislation to crack down on dirty money in the UK and corrupt elites. This was introduced to Parliament following Russia's invasion of Ukraine. Further measures will be introduced as part of a wider bill later in the coming months to safeguard and support the UK's open economy, whilst cracking down on people abusing that openness

This legislation will be complemented by the Companies House reforms planned in the Third Session. Companies House reform will bear down on the use of thousands of UK

companies and other corporate structures as vehicles for facilitating international money laundering (including illicit Russian finance), corruption, terrorist financing and illegal arms movements.

Measures to tackle the misuse of Limited Partnerships will increase transparency over Limited Partnerships and force them off the register under specific conditions. Due to outdated legislation, Limited Partnerships have been a particular vehicle of choice for misuse.

These reforms to Companies House and the Register of Overseas Entities Beneficial Ownership will maintain the UK's position as a world leader in corporate transparency. The Register of Overseas Entities Beneficial Ownership is one of the first of its kind in the world. It will enhance our already strong reputation as an honest and trusted place to do business.

Beyond the legislation brought forward this year, the UK made progress year on year since commitments in this area were made. As the committee notes, in 2016 we created a register of beneficial owners for domestic UK companies in 2016 and extended that register to Scottish limited partnerships in 2017. This was followed by a significant reduction in misuse. All the while, the UK has worked with the Crown Dependencies and Overseas Territories to support these reforms.

Waiting until the operational transformation of Companies House is complete risks further delay beyond 2025 if, as with many public sector change and IT projects, unexpected difficulties slow project delivery. Given the urgency of the problem, the Government should seek ways to implement as many reforms as possible sooner, before embedding a full transformation. (Paragraph 231)

The Government should supply us with details of the project milestones for the Companies House transformation programme, together with an annual progress report. (Paragraph 232)

The government published the Corporate Transparency and Register Reform White Paper on the 28 February 2022. The paper provides considerable detail on the way the reforms will operate, helping the UK's business community, law enforcement agencies and stakeholders to start to prepare for the changes to come.

This is a complex area of law; the Companies House reforms amount to the largest change to our system of setting up and operating companies since the companies register was created over 170 years ago. We need to ensure the proposals are effective and work coherently together.

The government intends to introduce the legislation in an Economic Crime Bill later this year. However, the transformation of Companies House is already underway. £20 million is being invested in 2021–22, with a further £63 million announced up to 2024/25 at the most recent Spending Review. Further details regarding these proposals were provided in response to the Committee's recommendations at paragraph 49.

The low costs of company formation, and of other Companies House fees (such as filing fees), present little barrier to those who wish to set up large numbers of companies for dubious purposes. The UK should be charging fees similar to those in other countries,

which would yield significant extra funding for Companies House and for the wider fight against economic crime. An increased cost may also deter some formations, reducing the operational demands on Companies House. Large numbers of registrations of companies place cost burdens on other parts of the public sector, such as HMRC, and on the regulators and law enforcement agencies tackling economic crime. There is a strong case that the cost should reflect the wider burdens on the taxpayer and not just the marginal cost to Companies House. (Paragraph 237)

The Government should significantly increase the costs of company and Limited Liability Partnership incorporation, including Scottish Limited Partnerships, and should review other Companies House fees to bring them closer to international standards. A fee of £100 for company formation would not deter genuine entrepreneurs, and would raise significant additional funding for Companies House and for the fight against economic crime. It would also help compensate for the wider costs on the public sector of large numbers of company formations. (Paragraph 238)

As aforementioned, the government is taking concerted action to prevent the misuse of corporate structures and limited partnerships for illicit purposes. This includes advancing Companies House reforms as well as. measures to reform limited partnerships which will also tighten registration requirements, increase transparency, and modernise legislation crack down on abuse.

The government is open to considering the case for changing fee levels and also recognises the value of Companies House enforcement activity in helping tackle economic crime and ensuring high standards are upheld within the UK's business environment.

Officials across departments are exploring the viability of proposals to ensure compliance with Managing Public Money principles, appropriate legal cover, and assurance that any changes would be value for taxpayer money. It is important that any proposals to change fees are judged against potential impacts on company creations.

We are disappointed that the Registration of Overseas Entities Bill is still awaiting introduction, more than five years after it was promised, and after scrutiny by a Joint Committee. Improving transparency of ownership of UK property is an important step that needs to be taken in order to improve defences against misuse of UK assets and companies by criminals and kleptocrats. (Paragraph 246)

We urge the Government to include a Registration of Overseas Entities Bill in the Queen's Speech for the next Parliamentary session. (Paragraph 247)

The UK continues to be a global leader in beneficial ownership transparency. Thanks to UK leadership, the FATF has agreed an ambitious new global requirement that will require countries to in effect create registers of ultimate ownership of companies, improving transparency of company ownership and preventing abuse of corporate structures, building on the UK's leadership as the first major economy to establish a public register of company ownership.

The Economic Crime (Transparency and Enforcement) Act will introduce the Register of Overseas Entities Beneficial Ownership, requiring anonymous foreign owners of UK property to reveal their real identities, ensuring that they cannot hide behind secretive chains of shell companies. The government is working at pace to ensure these requirements

come into force as soon as practicably possible, now we have received Royal Asset.

The government also brought forward amendments to shorten the deadline for overseas companies holding UK property to register their beneficial owners from 18 months to 6 months, and to require any overseas entity disposing of their property in the period from 28 February and the date of their application to register to provide information about the entity's beneficial ownership immediately before the disposal. These changes will help crack down on money laundering and sanctions evasion through UK property, whilst giving people who hold their property in overseas entities for legitimate reasons appropriate time to comply with the new requirements.

The register will set a new global standard for transparency and enhance the UK's already strong reputation as an honest and trusted place to do business.

Appendix 2: response from the Financial Conduct Authority

Findings of the Treasury Committee Inquiry on Economic Crime

I am writing to you following the Treasury Committee's report, 'Economic Crime', published on 2 February 2022 (the report). We welcomed the opportunity to provide evidence to the Committee's inquiry both in writing and in person and read the resulting report with interest.

As we set out in our written evidence, as the financial services and markets conduct regulator, as well as the money laundering supervisor for the financial sector, we have a crucial role in reducing fraud. Our approach to fraud and scams is based on prevention, the protection of consumers and the pursuit of fraudsters who operate within our perimeter to create a safer financial services sector which consumers have confidence in.

We maintain a coordinated approach involving law enforcement and regulators working with the National Economic Crime Centre (NECC). We work closely through the NECC to share data and intelligence where we identify criminal misconduct, where appropriate using law enforcement gateways to share information We would encourage law enforcement agencies to make more use of the NECC in order to share intelligence with the FCA where they have evidence of fraud which is connected to or enabled by the firms we regulate.

The growth in economic crime, and the Government's response

The number of agencies responsible for fighting economic crime and fraud is bewildering. Each of the enforcement agencies has other crime-fighting or regulatory objectives, and although the joint working co-ordinated by for example the National Economic Crime Centre is welcome, there is a bigger question about whether there should be a single law enforcement agency with clear responsibilities and objectives to fight economic crime. We recommend that the Government seriously considers this issue as part of a review of the Economic Crime Plan. (Paragraph 56)

The question of whether there should be a single law enforcement agency with clear responsibilities and objectives to fight economic crime is a matter for Government. However, as set out in our evidence, we remain of the view that the NECC needs dedicated resourcing so that vital cross-partnership work can happen more effectively.

Online economic crime

We agree with the Joint Committee that the Draft Online Safety Bill should be amended so as to include fraud offences in the list of "relevant offences" in Clause 41(4) of the Bill. Fraudulent content should be designated as "priority illegal content", thereby requiring online firms to be proactive rather than reactive in removing it from their platforms. These steps would place greater responsibility on online companies to prevent their platforms from being used to promote financial fraud, something of which these online firms are capable. (Paragraph 74)

We strongly agree with the Committee. Our written submission to the Online Safety Bill (OSB) Scrutiny Committee set out our hope that to help achieve the Government's stated aim of ensuring the UK is the safest place in the world to be online, the Bill should be amended to:

- Designate content relating to fraud offences as priority illegal content
- Extend the duties in the Bill to cover fraudulent content contained within paid-for advertising

We have therefore welcomed the Government's recent announcements regarding important amendments to the draft Bill. First, that fraud-related offences would indeed be designated as 'priority illegal'. This will mean that instead of platforms only being required to take fraudulent content down after having been alerted to it, now they will need to be proactive and prevent individuals from being exposed to such content. Second, that the OSB will now require the largest platforms to tackle fraudulent paid for advertising. We have been clear about the need for legislation and appreciate the Government's and the Committee's positive engagement o**n** this.

We look forward to working closely with the Government and regulatory partners as the details of the draft Bill are finalised, tabled in Parliament and implemented.

The Government should consider whether online platforms and social media companies should be required to do Know Your Customer checks on their advertisers, to make it more difficult for fraudsters to promote themselves (Paragraph 95).

We welcome the steps taken by certain online firms to take a clearer line in facilitating access to their platforms only for financial promotions placed by entities which are authorised by the FCA. We urge other online companies which have not made such commitments to follow suit. (Paragraph 95)

An authorised firm that approves a financial promotion must ensure that it complies with FCA rules, and this is likely to mean undertaking a degree of due diligence on the person issuing the promotion. While there is not currently an obligation to perform KYC checks, our view is that platforms (depending on how their advertising service operates) must ensure that financial promotions communicated by way of their sites are either made, or approved, by an FCA/PRA authorised firm (s21 FSMA). The implication of this is that authorised firms are subject to robust checks prior to authorisation and must ensure that their financial promotions comply with FCA rules. We agreed with the Committee that online platforms need to set out a clear timetable for delivering their commitments in this area.

The application of the Financial Promotion Regime is covered in further detail in the section below.

Additionally, we welcome the suggestion in the Government's announcement that the codes of practice to be drawn up by OFCOM might include recommendations that platforms check the identities of those wishing to publish adverts on their platforms. We think that understanding who is publishing material is an important step in reducing the risk that platforms are used to promote fraudulent content. We look forward to working closely with OFCOM as it develops the Codes, to ensure platforms minimise the risk of

exposing their users to fraudulent content by conducting KYC checks on advertisers.

The Government should not allow online companies to ignore legislation designed to protect consumers from harm. The Government should ensure that financial services advertising regulations apply also to online companies, and that the FCA has the necessary powers to effectively enforce the regulations. (Paragraph 96)

We note that the Committee's report recommended that the Government should ensure that financial services advertising regulations apply online and that the FCA has the necessary powers to effectively enforce the regulations. We would like to clarify our view of existing regulation in this area.

Under UK law, a person is prohibited from communicating (or causing to be communicated) a financial promotion unless (i) the person is authorised by the FCA/PRA; (ii) the promotion has been approved by a person authorised by the FCA/PRA; or (iii) the promotion is communicated within an exemption in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the 'Financial Promotions Order'). This is known as the 'financial promotion restriction' and is contained in section 21 of the Financial Services and Markets Act 2000.

A general EU-derived exemption in the Financial Promotions Order broadly exempted electronic financial promotions from the scope of the prohibition where these were made from an establishment in an EEA state other than the UK. This exemption was a component of the UK's implementation of the E-Commerce Directive (the 'ECD'). Since 1 January 2021, following the end of the transition period, this exemption no longer forms part of UK law.

The Financial Promotions Order still contains another exemption which has its roots in the ECD. This broadly exempts from the financial promotion restriction communications made by online intermediaries where the communication would fall within the scope of one of the three safe harbours in the ECD ('mere conduits', 'caching' and 'hosting'). Our view, however, is that these safe harbours (and therefore the related exemption in the Financial Promotions Order) do not apply when the intermediary has a significant role in optimising the content or actively determining which recipients receive particular promotions – most obviously in the case of paid for advertising.

As a result of this change, we have been looking at the operations of the major online platforms to determine whether they are subject to the financial promotion restriction and, if so, whether they are compliant. In this context, Google has put in place a new financial services verification policy to ensure financial promotions hosted through its ad service are only made by firms authorised by the UK financial services regulators (or which have otherwise been approved by such a firm). Other tech firms (including Microsoft, Meta and Twitter) have announced that they intend to put in place similar policies in due course (although we note there are no set timescales for implementation).

We continue to believe that 'downstream' provisions within the financial promotion regime are best bolstered by earlier 'upstream' provisions requiring platforms to have appropriate systems and processes in place and so welcome the amendments to the Online Safety Bill. These mean that platforms and social media companies are subject to clear legal obligations to prevent/minimise consumers' exposure to fraud related content on their sites in the first place.

It is not appropriate that online companies should profit both from paid-for advertising for financial products and from warnings issued on their platforms by the Financial Conduct Authority (FCA) about those advertisements. We urge all online companies to work constructively with the FCA and to follow Google's example by giving advertisement credits to the FCA for the future. We also expect them to refund money that has been spent in the past by the FCA. (Paragraph 97)

We strongly agree with the view expressed in the report that it is not appropriate that online companies should profit both from paid for advertising for financial services and also from warnings we place on the same platforms about those adverts. Whilst we have received an offer of advertising credits for future advertising from Google, we understand that there will be no refund of past spending. Also, we would like to make the Committee aware that we have struggled to get engagement on this issue with some other major platforms.

We recommend that the Government seriously consider whether online companies should be required to contribute compensation when fraud is conducted using their platforms. (Paragraph 102)

We note the recommendation that the Government consider whether online companies should be required to contribute compensation when fraud takes place using their platforms. Relatedly, we understand that the Joint Committee on the Online Safety Bill has recommended both:

- The creation of an Online Safety Ombudsman to provide recourse to redress where failure to comply with the provisions of the Bill lead to significant, demonstrable harm; and
- Creating a private right of action for redress for individuals (noting the challenges with individuals using it in practice).

We would be happy to discuss any ideas for redress models which the Government or other regulators would like to develop.

Anti-Money Laundering

The effectiveness of SARs might be increased if banks are permitted to share information with the National Crime Agency and other law enforcement agencies, before the suspicion threshold required under existing anti-money laundering legislation is reached. (Paragraph 144)

The National Economic Crime Centre (NECC) Public Private Partnerships have two Public Private Threat Groups which are focused on Money Laundering and Fraud. These groups have focused on driving greater cooperation between a range of private partners and the NECC to which the FCA is a partner. The groups provide a channel for private partners to provide insight on emerging methodologies that they may identify. There has been work to understand how data sharing from the NECC to private partners could be increased and at a faster pace. The NECC using powers conferred by s7 Crime and Courts Act have made tactical disseminations of data to private partners via the Joint Money Laundering Intelligence Taskforce (JMLIT). However, there is the potential for greater sharing of data which would enable the disruption of serious and organised crime.

One of the limitations that private partners have is that they often have a single view of individuals whereas a synthesised view of a network which may impact on multiple private partners can only be provided after the analysis of bulk SARS. We would welcome any initiatives which could help to build a system which could make these links in a more dynamic or real time environment.

The forthcoming Government review of the regulatory and supervisory regime for anti-money laundering and counter-terrorist financing, expected to conclude by June 2022, needs to address the concerns we have heard in this inquiry about the limited forward steps in compliance that OPBAS has so far secured. The problems which OPBAS identifies are similar to those which our predecessor Committee highlighted in 2019, shortly after OPBAS had been set up. We recommend that the review should not shy away from considering radical reforms, including a move away from the self regulatory model and the creation of a new supervisory body, potentially independent of the FCA, which takes more direct responsibility for policing professional body compliance with anti-money laundering regulations. The review should also take a hard look at enforcement measures which apply to professional bodies. (Paragraph 154)

The case for a supervisor of supervisors—including statutory supervisors—is still as it was at the time of our report in in 2019. We recommend that this idea should also be considered by the review. (Paragraph 155)

We welcome the report's recognition of the progress OPBAS has achieved. Over the last four years, under the supervision of OPBAS, the Professional Body Supervisors (PBS) have made significant improvements in their compliance with their obligations under the MLRs. OPBAS is now focusing on the effectiveness of the PBS AML supervision. As OPBAS states in its third report, while some PBSs are demonstrating good practice, OPBAS found during its 2020/21 assessments, differing levels of achievement and some significant weaknesses in the effectiveness of supervisory frameworks that PBSs have in place – which is informing our future work plan in this area so that effectiveness is improved. OPBAS expects PBSs to continue investing in, and strengthening their AML supervision, to have the greatest impact on the prevention of financial crime and that the PBS will continue to work closely with other authorities to make the UK an inhospitable place for criminals. OPBAS will continue to evolve its approach to supervision, using a wider range of methods to enrich its understanding of risks and drive more effective supervision by PBSs. It will continue to make robust interventions where PBSs do not make required progress.

The FCA is engaging with HM Treasury as part of its review of the AML/CTF supervisory regime.

We will continue to monitor the de-risking of customers by banks. We recommend that the FCA report annually on numbers of de-risking decisions and on progress to ensure that banks are not unfairly freezing bank accounts and de risking customers. (Paragraph 186)

Whilst access to banking services is an important consideration for the FCA, firms have commercial freedom, subject to some restrictions, to choose who they do business with. They are responsible for setting their own business models and for setting their risk

appetite on the types of customers they wish to deal with. A bank's decision on whether or not to provide its services to a prospective customer, or to maintain a relationship with an existing customer, can be influenced by a number of factors, including the firm's assessment of the risks associated with that relationship and the costs of providing services to certain customers. Whilst we cannot require a bank to provide services to a particular customer, we expect banks to observe their obligation to pay due regard to the interests of customers.

We collect relevant information from firms on the operation of their financial crime systems and controls, and keep this under review. As part of this work we collect, and have regularly published, information on the number of accounts that are exited for financial crime reasons. Whilst we do not routinely collect data on firms freezing accounts, we expect firms to investigate any accounts they freeze in a timely manner and to unfreeze them promptly when appropriate.

We recognise that a number of stakeholders are concerned that such controls may be unfairly deployed by some firms. We do regularly publish findings from our supervisory work in relation to AML compliance, these focus on supervisory outcomes rather than on the underlying number of accounts exited or frozen. We intend to continue to adopt this approach in line with our focus on outcomes.

We do not consider that the data currently available to us can provide a direct insight into the scale of the potential problem of de-risking and freezing of accounts. There are considerable challenges in obtaining comparable data on all forms of account exit and freezing across the retail banking and e-money and payments sectors. This is due to the variety of business models, and different forms that account exit and account or transaction freezing can take. Rather, we are focusing our data collection on accounts exited for financial crime purposes. We are following up with individual firms on their broader financial crime controls and approach to account exiting and freezing. In our view this is a more effective and outcome-focused use of our supervisory resources than further broadening our collection and publication of data on account freezing and de-risking.

Account freezing and exit is an important and legitimate response to suspicions of money laundering and other economic crime. We take this very seriously and are actively monitoring available intelligence and targeting supervisory resources to identify and address potential cases of unfair account freezing or de-risking. We regularly review the trend in the number of consumers getting in touch with our Contact Centre with concerns about their accounts being frozen or closed. Under Regulation 105 of the Payment Services Regulations, as set out in our Handbook, we require banks to inform us if they refuse a payment services provider access to payment account services and to set out the reasons for the refusal. We have followed up with firms on these returns and, to date, we have found that where banks have exited relationships with payment services providers, they have generally been able to find alternative banking arrangements within a reasonable timeframe.

Crypto assets and economic crime

The work being done by the Advertising Standards Authority to protect consumers from misleading advertisements for cryptoassets is also welcome. The Government should ensure that there is proper consumer protection regulation across the whole cryptoasset industry. (Paragraph 196)

We recognise the benefits that cryptoassets and their underlying technology may offer to financial services and will continue to encourage innovation and support competition in consumers interests. However, like in other areas, different types of cryptoasset activities and business models bring different risks of harm for consumers and markets. Furthermore, we have continued to warn consumers of the risks of investments advertising high returns based on cryptoassets, making clear that they should be prepared to lose all their money. Ultimately, the scope of our regulatory perimeter is a matter for the Government and we are working with them to inform thinking on any further regulatory or legislative actions that may be required to mitigate risks which are not covered by existing regulation.

If, as we recommend, the Government renews the Economic Crime Plan in 2022, it should consider instituting measures specifically to protect consumers from fraud and scams relating to cryptoassets. (Paragraph 205)

A key outcome in our Consumer Investments Strategy is to achieve a reduction in the amount of money consumers lose to investment scams. In support of this, our ScamSmart and InvestSmart campaigns seek to warn retail consumers about the scams and inform them about the risks of investing in high risk investments including cryptoassets.

In response to Russia's invasion of Ukraine on 24 February, we issued a joint statement on sanctions and steps firms should take to avoid cryptoassets being used to evade them on 11 March. On the same date, we also issued a warning on illegal crypto ATMs operating in the UK. We warned operators of crypto ATMs in the UK to shut their machines down or face enforcement action. We are contacting the operators instructing that the machines be shut down or face further action. Finally, since we published the list of unregistered crypto firms that may have been continuing to conduct business, a recent assessment found that 110 are no longer operational.

Temporary Registration Regime (TRR)

While we acknowledge the need to ensure that the gateway for registration of cryptoasset firms for anti-money laundering should be a rigorous process, registration has been too slow. It needs to be speeded up, and the Government should work with the FCA to find a solution. The FCA should not extend the deadline for registration again beyond March 2022. If the FCA sees no alternative, it should write to the Committee to explain its position (Paragraph 204)

The Temporary Registration Regime (TRR) for existing cryptoasset businesses was established in December 2020 to allow existing cryptoasset firms, which applied for registration before 16 December 2020, and whose applications were still being assessed, to continue trading.

A total of 106 firms applied to the TRR. We have been reviewing cryptoasset firms' applications carefully to ensure they meet the minimum standards we expect – that those

who run these firms are fit and proper and that they have adequate systems to identify and prevent flows of money from crime. These are in place so our financial system is not open to abuse by those who want to move and hide money made from violence, drugs, corruption or the exploitation of others. That is why we put in place a rigorous process for assessing applications and, despite allocating considerable resources, that rigour has taken time, especially as many firms were not used to regulation and, in some cases, reluctant to cooperate. A large proportion of firms, around 80%, were unable to meet the required standards. These standards are essential in maintaining the integrity of the UK financial system. We have now registered 33 firms.

Throughout the registration process when we decide a firm does not meet the standard for registration, we are clear with them where they are going wrong. The Money Laundering Regulations do not include a provision allowing firms to withdraw their applications. However, in some cases, we may allow a firm to withdraw, stop operating, make the changes necessary following our feedback and reapply. Firms that do not withdraw are issued a formal decision which they are able to appeal, including through the court. All firms with temporary registration are required to comply with the Money Laundering Regulations and are subject to supervision by us.

We have concluded our assessments of all firms in the TRR and it closed on 1 April, for all but 6 firms where it is strictly necessary to continue to have temporary registration. This is necessary where more time is required for them to provide representations to support appeals already in progress, or where strictly necessary for the winding-down arrangements.

The FCA supports innovation and promotes a welcoming environment for UK business that meet our standards. We continue to see new cryptoasset firms applying at the gateway, despite the number of firms that have been unable to meet the required standards. We have increased our focus on those applications.

NIKHIL RATHI, CHIEF EXECUTIVE

1 April 2022

Appendix 3: response from the Payment Systems Regulator

PSR response to the Treasury Select Committee report on Economic Crime: Eleventh Report of Session 2021–22

I am writing in response to the Treasury Select Committee's report Economic Crime, published on 2 February 2022.

The PSR welcomes the opportunity to provide both written and oral evidence to the Committee, and we have read the report with great interest.

As the regulator responsible for protecting people and businesses when they use payment systems, we are focused on ensuring that more is done to prevent authorised push payment (APP) scams, and to protect people who fall victim. We are developing coordinated action with a range of different parties, including financial institutions, other regulators, Pay.UK, the Lending Standards Board (LSB) and the Financial Ombudsman Service.

The report makes several recommendations for the PSR. This letter sets out our response and, where appropriate, describes our next steps towards implementation.

APP scams

People are losing life-changing sums of money to APP scams. Although there have been significant steps taken in the fight against these scams, more must be done. The scale and significant increase in APP fraud means urgent action is needed to protect consumers and make it harder to commit these crimes. Our annual plan explains how we are looking at more ways to protect people.

The contingent reimbursement model (CRM)

We recommend that the Government urgently legislates to give the Payment Systems Regulator (PSR) powers to make reimbursement mandatory, and that the PSR then take rapid action to protect consumers. We recommend that the PSR and Treasury accelerate their consultation processes to enable quicker implementation of measures to protect consumers from fraud. (Paragraph 11)

Our initial work on APP scams led to the introduction of the CRM Code in May 2019. Since then, there has been a considerable amount of progress to protect victims and improve incentives for payment service providers (PSPs) to prevent APP fraud. The voluntary agreement by signatories to the Code represented a major step forward in increasing the protection that their customers are entitled to, while setting out standards for PSPs to improve fraud prevention and victim care. We welcome the Committee's recognition of our work on the CRM Code and support for the code should be mandatory. The Code is now a key tool in preventing APP scams and has led to better protections for victims since its introduction.

We have seen an industry-wide shift in focus toward prevention, backed by PSR-led initiatives such as Confirmation of Payee (CoP), the name-checking service that has helped reduce fraud and accidentally misdirected payments.

We introduced Phase 1 of CoP in August 2019 when we issued Specific Direction 10 (SD10) to the six largest banking groups, requiring them to implement CoP. Since then, several other PSPs have voluntarily joined the service. Having analysed the impact of Phase 1, we have seen that CoP has limited the increase in APP scams, reduced the levels of fraudulent funds received by PSPs that have implemented CoP, and reduced the number of accidentally misdirected payments.

We recognise that there is still a lot of work to do to stop fraud from happening, to reduce APP scams, and improve consistency and coverage of protection of victims.

In February 2021 we published a call for views on the nature and scale of the issues with the CRM Code. In this document we stated that levels of reimbursement vary materially across PSPs and, as participation in the code is voluntary, many customers fall outside the protections it offers. We also invited views on three complementary measures to prevent APP scams and improve outcomes for victims. In November 2021 we published a consultation paper setting out our upcoming activity and our proposals to tackle this growing issue.

We proposed to:

- Require the 12 largest PSP groups in the UK (including most of the biggest high street brands) and the two next-largest PSPs in Northern Ireland to publish comparative data on:
  - their APP scams reimbursement levels for customers who are APP scam victims
  - which PSPs their fraudulent payments have been sent to

  This means that, for the first time, customers will be able to understand how well their PSP is preventing APP scams and treating victims, and which PSPs are receiving these fraudulent payments.
- Support and require industry to improve intelligence sharing, to improve detection and prevention of APP scams.
- Make reimbursement for scam victims mandatory. While we do not have the powers to do this at present, we welcomed the announcement from John Glen MP, Economic Secretary to the Treasury, that the government will legislate to address any barriers to regulatory action at the earliest opportunity. We continue to work to ensure that we can act quickly once this legislative barrier is removed.

In addition to the above three proposals, we continue to look at other ways of preventing APP scams and reimbursing victims. This includes looking at how the PSR, Pay.UK, and industry could implement rules (for example, in Faster Payments) within the parameters of existing legislation, and wider adoption of existing measures such as Request to Pay and the Biller Update Service.

Next steps

We are considering the responses to our consultation and continue to work at pace to implement these proposals.

On data publication, we have been progressing a trial with 14 PSPs to understand what data is available, and to invite industry feedback on data templates and guidance. We plan to publish a direction on data publication in the summer.

On mandatory reimbursement, we continue to work with the government to address the barriers to regulatory action. We are ready to impose measures that require PSPs to reimburse APP scam victims, following legislative change. We have developed our proposals in anticipation of the legislation coming into force, and will publicly announce our approach in autumn 2022.

In the meantime, we continue our engagement with the LSB to ascertain what changes can be made to the CRM Code to improve outcomes.

We are also engaging with a range of stakeholders to identify areas for coordination to drive a consistent and comprehensive approach to APP scams, including other sectors where these scams often originate. While our proposals are focused on our remit, we continue to engage in the broader debate with government, other regulators, and other sectors on what can be done more widely to prevent APP scams.

Confirmation of Payee

We recommend that the PSR supplies a report to our Committee on progress in the implementation of Phase 2 by the end of 2022. (Paragraph 124)

In February this year, we issued Specific Direction 11 (SD11), requiring Pay.UK to close phase 1 CoP by the end of May so that all PSPs are using the Phase 2 technical environment. This will enable a wider group of PSPs to offer Confirmation of Payee to their customers and widen the circle of protection for consumers.

Phase 2 of CoP is aimed at expanding participation to different types of institutions, including those that rely on secondary reference data (SRD), such as building societies. We want more PSPs to adopt CoP, and they can do this without regulatory intervention. However, we are ready to step in if required, and are considering our next steps. In the next three months, we will consult on proposals to direct more PSPs to adopt CoP.

We would welcome the opportunity to provide the Committee with a progress report by the end of 2022.

Data sharing

Improving data-sharing between banks is one of the measures which the PSR is implementing as part of its reform of the CRM Code. The Treasury should be ready to bring forward any legislation which is needed to enable this, and the PSR should ensure that banks act quickly in putting in place the necessary changes. (Paragraph 125)

We recognise the role that data plays in the fight against APP scams. Our proposal on data sharing aims to improve intelligence sharing between PSPs about the risks of payments, which should improve scam prevention. A number of PSPs, along with UK Finance and Pay.UK, have initiated a joint industry working group to assess the specific information that could be shared. This group is looking to identify the data that should be shared and the best way of sharing it – for example, between PSPs when a payment relationship is first set up, or as part of the payment itself.

The working group aims to have high level proposals on these points by the end of May 2022. We welcome industry organising the joint working group, and its efforts to find workable solutions to sharing information in a timely manner to prevent fraud. We have asked the group to develop a plan of outcomes and timelines, and to report back to us on progress. This group is making progress and its aims align with our objectives to improve fraud prevention and detection. We will keep the Committee informed on progress.

Finally, we echo the Committee's call for a multi-channel approach. To ensure better protection for customers, we need to begin by stopping scams happening in the first place. This requires coordinated action across a wide range of different parties, and a greater focus on where money is being sent. Payment system operators have a key role to play, but this is only one element of what is required. All platforms where criminals recruit their victims also need to play their part, including large social media firms.

Thank you for the opportunity to respond to the Committee's report. We look forward to keeping the Committee updated on the progress of our work to prevent APP scams and protect the victims.

CHRIS HEMSLEY, MANAGING DIRECTOR

1 April 2022