House of Commons

Treasury Committee

Economic Crime

Eleventh Report of Session 2021–22

Report, together with formal minutes relating to the report

Ordered by the House of Commons
to be printed 26 January 2022

HC 145
Published on 2 February 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), Tony Verran (on secondment from HM Revenue & Customs), 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.

Contents

Summary

Economic crime is a major and rapidly growing problem in the UK. This Report follows up on the two reports covering different aspects of Economic Crime published in 2019 by our predecessor Committee. It looks at the effectiveness of measures taken to address economic crime since 2019 and at the Government's Economic Crime Plan.

Since 2019, it appears that economic crime has not reduced but has instead continued on an upward trend. The Minister for Security and Borders at the Home Office told us that he was "not happy" with the progress that the Government had made in tackling economic crime. Nor are we. But we accept that a plan to co-ordinate this work, such as the existing Economic Crime Plan, is a sensible approach. 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. The Government should consider whether policy responsibility should be centralised in a single Government department.

Economic crime seems not to be a priority for law enforcement. 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 the Government needs to consider whether there should be a single law enforcement agency with clear responsibilities and objectives to fight economic crime. The Government must ensure that law enforcement agencies are appropriately resourced to tackle the scale of the problem.

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.

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. 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. Online companies should not profit both from paid-for advertising for financial products and for warnings issued on their platforms by the FCA about those advertisements. We encourage all online companies to work constructively with Government agencies and the wider public sector to fight online scams and fraud. The Government 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.

The work of the Payment Systems Regulator (PSR) to improve the Contingent Reimbursement Model (CRM) Code is welcome. We recommend that the Government urgently legislates to give the Payment Systems Regulator (PSR) powers to make

reimbursement mandatory. 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.

The Suspicious Activity Reports (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. It is, however, disappointing that the programme is not yet complete and that no timetable or target date for its completion has been published. A timeline showing when the milestones are expected to be met, and an annual progress report on the programme, should be provided to this Committee. The SARs reform programme can only deliver change if the Government ensures that the law enforcement agencies have the ongoing capacity and funding to tackle the criminal activity indicated by SARs.

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. 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. 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.

HMRC's self-assessment of its performance in supervising anti-money laundering (AML) is not truly independent, and we recommend that HMRC finds a way to give independent assurance about its AML performance. The Treasury's review of the regulatory and supervisory regime for anti-money laundering should also consider HMRC's role as a supervisor.

The new assertive approach by the FCA is welcome. The prosecution of NatWest is a major success. 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.

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.

We note the increasing risks around cryptoassets and economic crime. We welcome the announcement by the Treasury that the Government will legislate to bring advertising of cryptoassets advertising into line with that of other financial services and products, and that the FCA is strengthening financial promotion rules, including those for cryptoassets. 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. Not all cryptoasset firms have been registered for anti-money laundering (AML) purposes. It is unacceptable that, having introduced AML regulations for cryptoasset firms in 2020, there are so many firms which have not yet been registered.

We are disappointed that the Government has not yet implemented reform of corporate criminal liability. 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.

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.

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.

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 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.

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

1 Introduction

1. The Committee opened an inquiry into Economic Crime on 23 October 2020. Our aim was to review what progress has been made in combatting economic crime since the former Committee's inquiry on the subject in the previous Parliament. The previous inquiry was opened on 29 March 2018 and led to two reports: *Economic Crime – Anti-money laundering supervision and sanctions implementation*, published on 8 March 2019,[1] and *Economic Crime: Consumer View*, published on 1 November 2019.[2] The Government responses were published in two special reports.[3]

2. Several Government departments are involved in Government policy on fighting economic crime, including HM Treasury, the Home Office, the Ministry of Justice, the Department for Business, Energy and Industrial Strategy, and Her Majesty's Revenue and Customs (HMRC). Since the previous inquiry ended in 2019, the Government has introduced its Economic Crime Plan;[4] has taken steps to set in statute a new Economic Crime Levy to raise money from the sector regulated for money laundering, to improve funding for anti-money laundering efforts; and has published a Draft Online Safety Bill with economic crime elements.[5]

3. A wide range of other steps have been taken:

- Anti-money laundering regulation has been extended to cryptoasset firms by regulation,[6] and to electronic money institutions, payment institutions and deposit-taking businesses by the Financial Services Act 2021;[7]
- Rules around trusts registering with HMRC's Trust Registration Service were tightened up by the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020;[8]
- The Financial Conduct Authority claims to have implemented a more assertive regulatory policy;[9]
- HMRC has improved its anti-money laundering supervision work;
- The Payment Systems Regulator has consulted on mandating a new fraud compensation scheme for banks;

1 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime - Anti-money laundering supervision and sanctions implementation, 8 March 2019, HC 2010
2 Treasury Committee, Third Report of Session 2019, Economic Crime - Consumer View, 1 November 2019, HC 248
3 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, HC 2187, 7 May 2019 and Treasury Committee, Second Special Report of Session 2019–21, Economic Crime: Consumer View: Government and Regulators' Responses to Committee's Third Report of Session 2019, HC 91, 13 March 2020
4 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019
5 Department for Digital, Culture, Media and Sport and Home Office, Landmark laws to keep children safe, stop racial hate and protect democracy online published, 12 May2021 [Extracted 29 December 2021]
6 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, (SI 2019/1511). This was a recommendation of the former Committee report, see Treasury Committee, Twenty-Second report of Session 2017–19, Crypto Assets, HC 910, para 90- 106
7 Financial Services Act 2021, section 32
8 The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020 (SI 2020/991)
9 Financial Conduct Authority, Business Plan 2021/22, page 4

- The Home Office has progressed its programme for reform of Suspicious Activity reports (SARs):
- The Law Commission has begun a review of corporate criminal liability; and
- The Department for Business, Energy and Industrial Strategy (BEIS) has consulted on Companies House reform.

These activities are considered in more detail in this report.

4. The inquiry which underlies this report had two major strands:

- The development and effectiveness of anti-money laundering systems, and
- How consumers are affected by economic crime.

Terms of reference for the inquiry are on the Committee's webpages.

5. Chapter 2 examines the scale of economic crime and the Government's Economic Crime Plan, which was launched in July 2019.

6. Chapter 3 deals with the problem of online platforms being used to promote fraud and what is being done about it.

7. Chapter 4 examines the problem of "authorised push payment fraud" and what the Payment Systems Regulator, amongst others, is doing about it.

8. Chapter 5 looks at money laundering and at anti-money laundering regulations.

9. Chapter 6 examines the fraud and economic crime issues that have arisen from the growth in cryptocurrency and cryptoassets.

10. Chapter 7 sets out how companies may be used as a vehicle for economic crime, and the steps that might be taken to reform Companies House and its operations to help tackle economic crime.

11. We hope that this Report helps the Government, regulators and law enforcement agencies make progress in tackling economic crime and thereby reducing the harm it causes. The report is informed by written submissions from a wide range of individuals, businesses and third sector organisations, most of whom highlighted concerns with the continuing growth in fraud and economic crime. 19 witnesses, including key regulators and John Glen MP, Economic Secretary to the Treasury, and the Rt Hon. Damian Hinds MP, Minister for Security and Borders, Home Office, gave evidence over the course of five oral evidence sessions. We thank all the witnesses for their time and expert comment, and we are grateful to everyone who submitted written evidence. Both the oral evidence and the published written evidence is available on the Committee's webpages.

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

The growth in economic crime and fraud

12. Economic crime is a broad term used to cover all types of financial crime. The National Economic Crime Centre, part of the National Crime Agency, states that it encompasses fraud, money laundering, counterfeit currency, bribery and corruption.[10] Economic crime, including fraud, is a growing problem. The Government's Economic Crime Plan stated in July 2019 that "all assessments within the public and private sectors indicate that the scale of the economic crime threat continues to grow".[11] Since then, fraud has continued its upward trend. The Crime Survey for England and Wales[12] shows that for the year ending June 2021, compared to the year ending June 2019, the level of crime overall was 12% higher, driven by a 43% increase in fraud and computer misuse. Fraud itself was up by 32%. The increase in fraud and computer misuse more than offset reductions in other types of crime. Fraud and computer misuse is now greater than all other types of crime put together, according to ONS research.[13]

13. The National Crime Agency says that money laundering (covered in Chapter 5) threatens national security and prosperity.[14]

14. The Office for National Statistics (ONS) also reported in November 2021 that Action Fraud (the public-facing national fraud and cybercrime reporting centre) reported a 36% rise in fraud offences (to 424,397 offences) for the year ending June 2021, compared with the year ending June 2020. The data showed a 34% increase in "online shopping and auctions" fraud in the latest year (from 70,761 to 94,795 offences) and a 51% increase in "financial investment fraud" (from 14,685 to 22,200 offences).[15]

15. The schemes to support businesses during the pandemic were subject to very substantial levels of fraud. The Department for Business, Energy & Industrial Strategy estimates that the value of fraudulent loans under the Bounce Back Loan Scheme, as at 31 March 2021, was £4.9 billion.[16] In November 2021, HMRC's estimate of the amount lost to fraud and error in each of the schemes which it administered during 2020 and 2021 was 8.7% of payments made under the Coronavirus Job Retention Scheme, 2.5% of payments under the Self Employed Income Support Scheme phases 1–3 and 8.5% of payments under the Eat Out to Help Out scheme, equating to £5.8 billion overall.[17] In 2020–21, HMRC recovered £536 million of overclaimed grants, and an HMRC taxpayer protection taskforce is expected to recover between £800 million and £1 billion from fraudulent or incorrect payments during 2021–22 and 2022–23.[18]

10 National Crime Agency 'Economic Crime Threats' [extracted 12 January 2022].
11 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, para.15
12 The Crime Survey for England and Wales is the source for the Office for National Statistics, Crime in England and Wales: year ending June 2021 (4 November 2021)
13 Office for National Statistics, Crime in England and Wales: year ending June 2021 (4 November 2021), page 2
14 National Crime Agency, Money laundering and illicit finance [extracted 12 January 2022]
15 Ibid page 23
16 Report by the Comptroller and Auditor General, "The Bounce Back Loan Scheme: an update", HC 861 (2021–22), 3 December 2021, p.4
17 Our approach to error and fraud in the COVID-19 support schemes - GOV.UK (www.gov.uk)
18 Lord Agnew responding to an Urgent Question, HL Deb 24 January 2022, col 19

16. On 24 January, shortly before this Report was finalised, Lord Agnew, the joint Treasury and Cabinet Office Minister for Efficiency and Transformation, resigned. In an article in the Financial Times on 25 January, he was sharply critical of failure by the Government to address fraud:

> Fraud in Government is rampant. Public estimates sit at just under £30 billion. There is a complete lack of focus on the cost to society or indeed the taxpayer.

He was particularly concerned by losses to fraud under the Bounce Bank Loan Scheme:

> The government machine has failed spectacularly both in the business department in its weak oversight of the British Business Bank and in the Treasury for allowing such dysfunctionality to continue on such a colossal scale.[19]

17. Fraud in coronavirus support schemes has not been a focus of this inquiry, although it is a subject which we have addressed regularly[20] and to which we expect to return. We also note the work of other committees and of the National Audit Office in this field.[21]

18. A more detailed picture of fraud is provided by UK Finance in their publication *Fraud, The Facts 2021*.[22] That report shows that particular types of fraud have been driving up the overall volumes and value of fraud, for example advanced fee scams (up 32% in volume and 34% in value), romance scams[23] (up 38% in volumes and 17% in value), investment scams (up 32% in volume and 42% in value), and impersonation scams (up 94% in volume and 15% in value). The statistics for Authorised Push Payment Fraud (see Chapter 4) show that it is up 71% by value in the first half of 2021 when compared to the first half of 2020.

19. Graeme Biggar, Director-General at the National Economic Crime Centre, National Crime Agency, told us:

> We have a serious problem with fraud in this country; it has been growing steadily. That has largely mimicked the rise of the internet in the UK, which has allowed more and more crime to take place. In the UK, we do not place the highest priority on fraud across law enforcement and policing. As you said, in the Crime Survey in England and Wales, it accounted for about a third of the crime that is reported. It is a lot less in actual reports that actually get to the police—about 12% … Only about 1% or less of police resources and personnel are devoted to fraud. There are fewer police than you would expect looking at that.[24]

19 Fraud is rampant—and no one in government is paying attention, Financial Times 25 January 2022

20 See for example oral evidence given by HMRC on the HMRC Annual Report and Accounts, 7 December 2020, and oral evidence given by the National Audit Office on the Economic Impact of Coronavirus, 18 April 2021

21 See for example Report by the Comptroller and Auditor General, "The Bounce Back Loan Scheme: an update", HC 861 (2021–22), 3 December 2021; Fraud and Error, Ninth Report from the Committee of Public Accounts, HC 253, Session 2021–22

22 UK Finance, Fraud the Facts 2021.

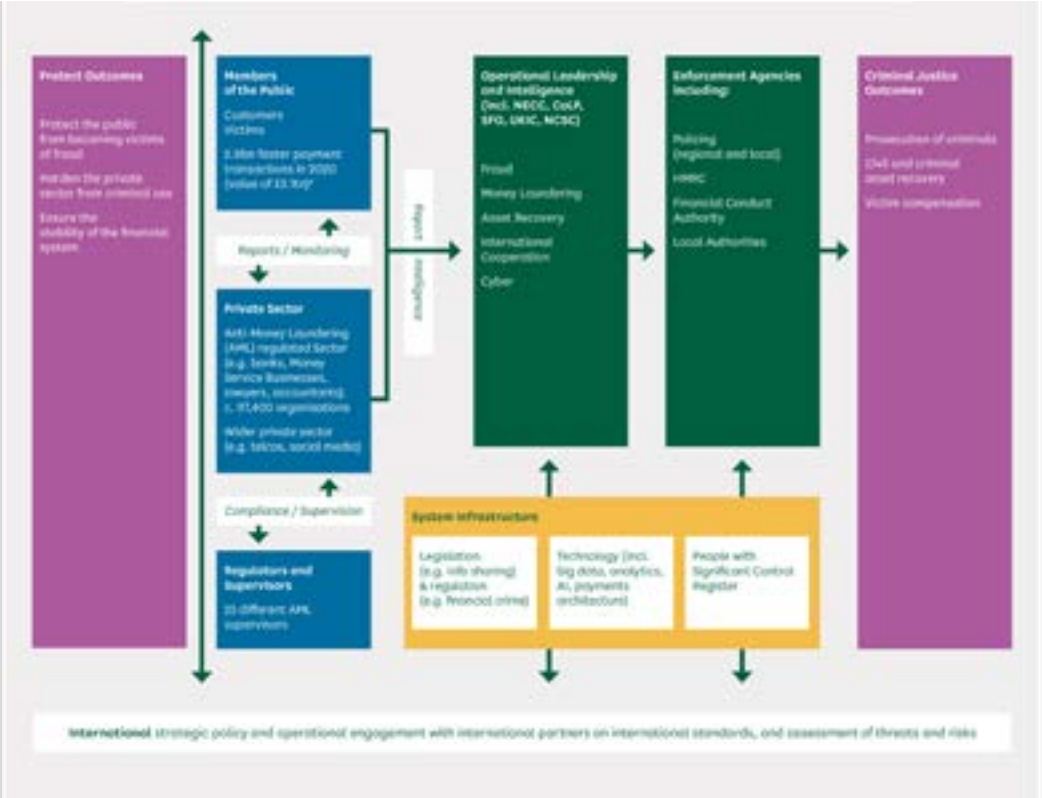
23 A "romance scam" is where fraudsters create fake accounts on dating sites and develop relationships with victims. Once victims are emotionally invested, fraudsters pretend to be in urgent need of money and request assistance.

24 Q2

The size of the challenge, and the Government's Economic Crime Plan

20. Economic crime presents a major challenge for Government. The Government's approach to the problem has different Government departments working on policy relevant to their departmental responsibilities, with additional policy work carried out by regulators and agencies, and partnerships with private sector bodies (see Figure 1 below). This work has been brought together to form a cross-Government Economic Crime Plan, which was published in collaboration with UK Finance.[25]

Figure 1: The UK Government's system for combatting economic crime



Source: HM Treasury[26]

21. The Economic Crime Plan 2019 to 2022[27] was published on 12 July 2019. This plan builds on previous cross-Government plans of a similar kind, such as the UK Anti-Corruption Plan (2014),[28] the UK's Anti-Money Laundering and Counter-Terrorist Financing Action Plan (2016),[29] the UK Anti-Corruption Strategy (2017) ,[30] and the Serious and Organised Crime Strategy (2018).[31]

22. The Government told us in its response to the previous Committee's March 2019 report that the Economic Crime Plan:

25 UK Finance is the collective voice for the banking and finance industry. See UK Finance, 'About Us', [Extracted 4 January 2022]
26 HM Treasury (ECC0100)
27 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019
28 UK Government, UK Anti-Corruption Plan, December 2014
29 HM Treasury and Home Office, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, 21 April 2016
30 Department for International Development and the Home Office, UK Anti-Corruption Strategy 2017-2022,December 2017
31 Home Office, Serious and Organised Crime Strategy 2018, Cm 9781, November 2018

> … will respond to the Financial Action Taskforce's recommendations as well as those put forward by the Committee. This will be the first major output under the direction of the new Economic Crime Strategic Board. The Board, which is co-chaired by the Chancellor and the Home Secretary, is driving the public and private sector response to economic crime, by setting strategic priorities, ensuring resources are allocated to address capabilities and to scrutinise overall performance against the economic crime threat.[32]

23. The Economic Crime Plan has the following seven strategic priorities:

- Develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime
- Pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants
- Ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible
- Strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime
- Build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision
- Improve our systems for transparency of ownership of legal entities and legal arrangements
- Deliver an ambitious international strategy to enhance security, prosperity and the UK's global influence.[33]

These are then broken down into 52 specific actions.

24. The plan is overseen by a Ministerial level public-private board, the Economic Crime Strategic Board. The following chart shows how governance of economic crime works:

32 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 4

33 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019

Figure 2: Economic Crime governance

HS: Home Secretary, CX: Chancellor of the Exchequer, HO: Home Office, HMT: HM Treasury, UKF MD: UK Finance managing director, DD: Deputy Director.

Source: HM Treasury[34]

25. The Strategic Board appears to have met three times only, twice in 2019[35] and then on 17 February 2021.[36] It has not met since. We asked the Rt Hon. Damian Hinds MP, Minister of State at the Home Office and Security Minister, whether the infrequency of Board meetings implied that the Government was not prioritising the Plan and the growth in fraud. He said:

> That would be an erroneous interpretation of life. We have different levels of entity and board. The Joint Fraud Taskforce meets in the interim. We also have a set-up that meets more regularly, and it does the delivery—whatever the big strategic objectives are, it makes sure that it is actually happening from month to month. In fact, we are meeting, discussing, reviewing and tracking progress very regularly".[37]

26. Mr Hinds also commented on the overall progress with the 52 actions in the plan. He said that: "34 out of 52 are completed, and 18 others are well under way."[38]

27. Some witnesses thought that the Government had made progress with the Economic Crime Plan. David Clarke, Chair of the Fraud Advisory Panel, told us on 8 July 2021 that "The Plan is a welcome step. It was good to see it coming in. The concern we have

34 HM Treasury (ECC0101)
35 The Board met on 14 January 2019, HM Treasury and Home Office Economic Crime Strategic Board January 2019 agenda and minutes, and on 10 July 2019: Economic Crime Strategic Board minutes and agenda: July 2019
36 HM Treasury and Home Office Economic Crime Strategic Board 17 February 2021 agenda and minutes,
37 Q512
38 Q513

is that fraud does not feature enough in it". However, he also added that "We are also concerned that only seven of the 52 actions in that Plan relate to fraud, and this seems to be systematic of fraud over the years."[39]

28. Helena Wood, Associate Fellow, RUSI Centre for Financial Crime and Security Studies, which publishes an online tracker of progress on the Economic Crime Plan,[40] saw positives but also some areas for improvement. She said:

> If we look at it across that broad economic crime waterfront, I would give the Economic Crime Plan and its progress to date a pretty mixed scorecard.
>
> We have had some real areas of delivery that we can give credit for. I would particularly point to the redesign of the SARs IT system, which is long overdue but is happening. We have had some really useful steps forward in digital ID and its role in tackling, again, fraud[41] …
>
> We have had some good progress, but a keen-eyed observer looking at RUSI's Economic Crime Plan tracker might observe the biggest areas of progress are in the arguably easier, and I would say cheaper, areas of policy transformation.[42]

29. Richard Piggin, Head of External Affairs, Which?, thought that success of the Plan should be measured by its impacts on levels of fraud. He said:

> The success of the Economic Crime Plan can be judged on the outcomes it is delivering. Is it reducing the harm and the impact on individuals? One of those measures is the level of fraud. As David [Clarke] talked about, the level of fraud, which is the most common economic crime faced by consumers, and the losses incurred from fraud are not going down. In fact, in recent years we have seen a significant increase in the amount of online fraud and the number of authorised push payment scams … In neither of those areas has the Government or regulatory response been swift enough or strong enough, in our opinion."[43]

30. We asked Helena Wood, of RUSI, what the Government needs to do to get ahead of, and halt, the rise in economic crime. She said:

> They would do well to recognise that the economic crime problem will not be solved by July 2022, when the current Plan comes to an end. I would like to see them commit pretty early to a second economic crime plan, which will kick off soon. They will need to start thinking about that pretty soon if they are going to do it.[44]

31. During oral evidence to the Committee on 29 November 2021, we asked the Rt Hon. Damian Hinds MP, Minister for Security and Borders, Home Office, if he was happy with progress that the Government had made in tackling economic crime. He said:

39 Q200
40 Royal United Services Institute, Economic Crime Plan Online Tracker, extracted 7 December 2021
41 Q201
42 Q202
43 Q203
44 Q263

> Am I happy? No, I am not happy. If you want us to sit here and say that we are happy with the progress made today, no, of course not: we have a great deal further to go. There have been some really important aspects of progress. John [Glen] can talk more about the supervisory regime, but on our side, we have law enforcement with the development of the National Economic Crime Centre, the SARs reform programme, and some of what has been happening on fraud and some of the extra people we are going to be putting in place. Those are all important steps forward.
>
> […]
>
> … there is a big distance still to go, and however fast we deal with the current landscape, the fact is that this is a rapidly growing area of crime.[45]

32. We also asked Mr Hinds how long it would take for fraud levels to flatten off. He said:

> I want fraud levels to flatten off. I want them to fall. I do not have a way of telling you a moment when that is going to happen. I can tell you that the time to be working on it is right now, and that is what we are doing.[46]

When pressed for a date by which fraud might fall, he said:

> I could absolutely give you a date that I would like to put on it, but you asked me a moment ago to predict it. What I think we need to do is work night and day to do all the things that we know and believe can make the biggest difference.[47]

33. **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.**

34. **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.**

35. **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.**

36. ***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,***

45 Q435
46 Q505
47 Q506

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.

37. ***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.***

Funding the fight against economic crime

38. The 2021 Spending Review promised the Home Office new investment of £18 million in 2022–23 and £12 million in both 2023–24 and 2024–25 for tackling money laundering and fraud.[48] It also promised an additional £63 million over the Spending Review period to support reform of Companies House.[49]

39. The Government has also introduced a new Economic Crime Levy, to be paid by entities subject to the Money Laundering Regulations (MLRs), to help fund new Government action to tackle money laundering. Legislative provision for the Economic Crime Levy is contained within the Finance (No. 2) Bill, which has yet to complete its passage through Parliament.[50]

40. The Levy will apply to all businesses which have an annual turnover of more than £10.2 million and which are registered for anti-money laundering purposes. There are three charging rates, depending on the size of the business. The Levy is charged at a flat rate within those bands:

- Small entities (less than £10.2m turnover)–exempt
- Medium businesses (£10.2m to 36m turnover)–£10,000 per year
- Large businesses (£36m to £1bn turnover)–£50,000 per year
- Very large businesses (over £1bn turnover)–£250,000 per year

The Government has projected the yield of this Levy at £100 million per year from 2022–23.[51]

48 HM Treasury, Autumn Budget and Spending Review 2021: A Stronger Economy for the British People, 27 October 2021, para 4.19 p. 99

49 HM Treasury, Autumn Budget and Spending Review 2021: A Stronger Economy for the British People, 27 October 2021, para 4.73 p. 114

50 Finance (No. 2) Bill, [Bill 184, 2021–22]

51 HMRC, Economic Crime (Anti-Money Laundering) Levy, (impact assessment)

41. When we took evidence from Mark Steward, Director of Enforcement, Financial Conduct Authority, he appeared relaxed that the FCA had sufficient resources for its role under the Economic Crime Plan, but he pressed for more money for the National Economic Crime Centre (NECC).[52] He said:

> We certainly have the resources to tackle what we are doing under the Economic Crime Plan. More generally, it is very clear to us that tackling economic crime across the spectrum requires all of us to work together. That is why the NECC is such an important part of the approach here. As Simon [York[53]] mentioned, if you ask Graeme [Biggar] what the NECC needs, it needs more resource. The FCA is also a founding member of the National Economic Crime Centre. We think the NECC needs more resourcing. It needs dedicated resourcing, so that that cross-partnership work that it is vital for all of us to be engaged in can happen more effectively.[54]

42. Helena Wood, Associate Fellow, RUSI Centre for Financial Crime and Security Studies, speaking to us before the Spending Review, expressed concern that the Economic Crime Levy was not enough and agreed that the NECC needed more funding. She said:

> It is not enough to look purely to the private sector to fund this. While £100 million sounds a lot, it is not in terms of the scale of the problem that we have all pointed to … We are going to have one of the most heavily contested spending reviews that we have ever seen and one that I doubt will be noted for its generosity, but it would be a real signal of intent from the Government if they gave a someway decent settlement to funding of fraud policing in particular, but economic crime across the board, and a better funding of the National Economic Crime Centre, setting out what role it can play in transforming the policing response for the future.[55]

43. These witnesses' comments were made before the Spending Review allocated an additional £42 million to the Home Office to tackle economic crime. The Spending Review did not make it clear whether the NECC would get the additional funding which Mark Steward and Helena Wood called for.

44. Helena Wood was also concerned that the cuts in the overseas aid budget meant that the National Crime Agency (NCA) would lose funding. She said:

> Just to build on what Duncan [Hames] said about the scale of kleptocratic wealth finding itself in the UK and looking at the international components of the economic crime plan, there is absolutely no doubt in my mind that the cuts to the UK aid budget are going to have an impact on the UK's ability to deliver that part of the plan. For example, we have already seen the planned growth of the international corruption unit at the NCA put on ice because of cuts to the aid budget.[56]

52 The NECC launched on 31 October 2018 and is overseen by the National Crime Agency (NCA). It brings together the NCA, Serious Fraud Office, Financial Conduct Authority, City of London Police, HMRC, Crown Prosecution Service and Home Office.

53 Director of the Fraud Investigation Service, HM Revenue & Customs, another witness at the session

54 Q188

55 Q209

56 Q208

45. We asked the Economic Secretary to the Treasury, John Glen MP, about what the Spending Review meant for funding to fight economic crime. He said:

> In the recent Spending Review settlement—the Economic Crime Levy will give us £100 million in '23-'24—we will have combined funding totalling £400 million to deal with the economic crime need. That is new investment for the Home Office of £18 million for '22- '23, and £12 million for '23-'24 and '24-'25, plus the continued £30.5 million per annum of RDEL announced in the previous spending review. I mentioned earlier the extra £63 million across the spending review for BEIS to accelerate the Companies House reform. Obviously, that is a key priority coming out of FATF [Financial Action Task Force] and just generally. We have worked to implement the collection mechanism through the Gambling Commission, FCA and HMRC across the 25 PBSs [Professional Body Supervisors] for the Economic Crime Levy, which is another contribution of £100 million.[57]

46. Speaking about what the yield from the Economic Crime Levy would be spent on, he said:

> There was a consultation on what it should be used for, and it was to be used for anti-money laundering activities, not wider fraud or other areas. It will be important for us to be accountable for using that money in that way.[58]

47. **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.**

48. ***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.***

49. ***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.***

57 Q500
58 Q501

Effectiveness of law enforcement agencies

50. Various agencies have responsibility for law enforcement in relation to economic crime. The *National risk assessment of money laundering and terrorist financing 2020,* published jointly by HM Treasury and the Home Office, contains details of all the enforcement agencies involved in the fight against money laundering and economic crime:[59]

- The National Crime Agency, which is the lead law enforcement agency in England and Wales for serious and organised crime, dealing with the highest-level criminality. Their tools and powers include: intelligence and evidence gathering; cash seizure and forfeiture; restraint and confiscation; and civil recovery and taxation.

- The National Economic Crime Centre (NECC), hosted within the NCA, which was established in 2018 and which leads and co-ordinates the UK's response to economic crime both at home and abroad that has a national impact.[60] The Centre is comprised of representatives from a variety of law enforcement and Government departments,[61] who work together to progress national and departmental priorities on economic crime.

- The UK Fraud Intelligence Unit (UKFIU), which is an operationally independent part of the NECC. It receives financial intelligence gathered from Suspicious Activity Reports (SARs),[62] 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),

- Police forces in England and Wales, which have collaborated to form Regional Organised Crime Units (ROCUs) across nine policing regions. These units deliver specialist investigative and intelligence capabilities within their regions and are the primary interface between the NCA and local forces. Within each ROCU is a Regional Economic Crime Unit (RECU), whose main role is to recover criminal assets through confiscation and civil powers on behalf of the regional and local forces, and other agencies such as HMRC, NCA and Trading Standards.

- The policing response to serious and organised crime is a devolved matter. Police Scotland works closely with the NCA, HMRC, the FCA and other relevant agencies in investigating economic crime. The Scottish Crime Campus is a multi-agency centre, established by the Scottish Government in 2014, which accommodates the key agencies involved in tackling economic crime in Scotland.

- The Police Service of Northern Ireland (PSNI), which is the lead operational agency for serious and organised crime in Northern Ireland and the NCA and other UK law enforcement agencies work closely with them. PSNI has a dedicated Economic Crime Unit with specialist investigative capabilities.

59 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020, chapter 2

60 The NECC's work covers England and Wales and it also works closely with Police Scotland and Police Service Northern Ireland

61 The NECC has officers or representatives from the NCA, SFO, FCA, City of London Police, HMRC, Crown Prosecution Service, Cabinet Office, Home Office and Foreign, Commonwealth and Development Office

62 Suspicious Activity Reports

- The Serious Fraud Office (SFO), which is an independent Government department that investigates and prosecutes serious or complex fraud, bribery and corruption and associated money laundering. It has jurisdiction in England, Wales and Northern Ireland but not in Scotland, where this responsibility rests with the Crown Office and Procurator Fiscal Service.

- HMRC, as the UK's tax authority, which is a non-ministerial department reporting to Parliament through the Financial Secretary to the Treasury. As well as being an anti-money laundering supervisor, it is responsible for investigating serious tax fraud using its extensive range of civil, criminal and tax investigation powers. This includes money laundering linked to tax offences.

- Border Force, which is a law enforcement agency of the Home Office, responsible for keeping the border secure and promoting national prosperity by facilitating the legitimate movement of individuals and goods, while preventing those that would cause harm from entering the UK. Border Force says that it performs "a unique role within law enforcement anti-money laundering activity through a continued focus on the deterrence and prevention of illicit cash and listed asset smuggling across the UK border".[63]

- The Financial Conduct Authority (FCA), which is a statutory money laundering supervisor and which investigates and prosecutes for money laundering when that is ancillary to offences that the FCA is responsible for under its statutory objectives, including market manipulation, insider dealing and unauthorised business activity such as boiler room frauds.[64]

- The Gambling Commission, which is an anti-money laundering supervisor.

51. We heard evidence that crime agencies were not prioritising fraud and that they need more money, including for law enforcement itself. Angela McLaren, Assistant Commissioner for Economic and Cybercrime, City of London Police, said: "It is a very small number of police resources available to deal with what is a large problem". But she also highlighted recent improvements:

> … the national fraud policing strategy, which was agreed by the National Police Chiefs' Council in October 2019. … is important to highlight because that was bought into by all police forces and ROCUs [Regional Organised Crime Units] across the UK. As a consequence of that, we are implementing new structures, both in terms of how we co-ordinate and the resources that are available. In this year and moving forward we are looking to see an uplift in resources in both the regional crime units and, indeed, as part of the City of London's police uplift, which will be dedicated to looking at fraud as well.[65]

52. Mark Steward, Director of Enforcement, Financial Conduct Authority agreed. He said:

63 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, paragraph 2.49

64 A "boiler room" is an office out of which fraudsters contact people out of the blue to try to convince them to invest in schemes or products which are worthless or do not exist. See Action Fraud "Boiler Room Fraud". [Extracted 17 January 2022]

65 Q4

> More money needs to be spent on law enforcement … We have not really talked about the expectation gap that we all face as regulators, with the lack of priority that fraud really has for law enforcement. It is not their fault either because of the choices they need to be making as well. It is enormously frustrating, particularly when we face a significant expectation gap between what people think we can do and what we can actually manage. …. There is a huge amount of goodwill around this table, as there is among the members of the National Economic Crime Centre, but we need money to make things happen.[66]

53. Graeme Biggar told us that fraud is a third of all reported crime but accounts for 1% of police resources.[67] He said:

> … of the 3.8 million or 4.3 million offences, in about 1 million of those, there was no loss from the fraud—it was attempted fraud that did not lead anywhere—and in about another 2 million of those, the victim was reimbursed, often straightaway by a bank. You are then getting down to figures that are a bit more like the ones that get reported to Action Fraud. They are still large—I do not want to diminish them in any way—but you are down to the 800,000-odd that get reported to the National Fraud Intelligence Bureau in one of several ways. In about 40% of those offences, the loss is £100 or less, and in about 10%, the loss is £1,000 or more."[68]

> It is still 12%—please correct me if I have got that figure wrong—of crime that is reported to police, which is quite a lot, and a fair chunk of that is very serious. I think we would all agree that we need to do more, not just for policing, but across law enforcement in the round, so absolutely involving the National Crime Agency and others, and the financial sector and many more.[69]

54. David Clarke said "There are just too many agencies involved in the fight on fraud. We are siloed. It is a real pickle."[70]

55. Helena Wood thought the Government could learn from the systems in place in the USA. She said:

> We are not stepping up to the threat. If we really want to maintain our position as a global financial centre, we have to take the responsibility that comes with that, and that needs this much more robust response we see in the States. Accordingly, they resource their response properly.[71]

56. ***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***

66 Q194
67 Q2
68 Q2
69 Q3
70 Q200
71 Q204

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.

57. ***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.***

58. **There may be many reasons for low prioritisation of economic crime by crime-fighting agencies. It does not happen in the street, but often in people's homes. Consumers often, apart from inconvenience, do not suffer directly, since they may be repaid by banks. But these are not reasons to not engage more forcefully with the problem.**

An Economic Crime Bill

59. When Lord Agnew resigned as Minister of State on 24 January 2022,[72] he told the press that "an economic crime bill was foolishly rejected last week as a candidate bill for the next parliamentary session."[73] Although we are aware of calls for an Economic Crime Bill,[74] Ministers made no mention of a forthcoming Economic Crime Bill when they appeared before the Committee on 29 November 2021. Some relevant primary legislation (including the Finance (No. 2) Bill and the planned Online Safety Bill) is either already before Parliament or is expected to be introduced soon.

60. Notwithstanding that many of the recommendations contained in this Report do not require legislation or might be brought into effect through secondary legislation, it would be highly unfortunate if the Government were to decide not to bring forward an Economic Crime Bill where such a bill would have the potential to add considerably to the fight against fraud and other forms of economic crime.

61. ***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.***

72 HL Deb, 24 January 2022, [cols 19–22]

73 "UK anti-fraud minister quits over 'lamentable' Covid loan oversight", the Financial Times, 25 January 2022

74 See for instance the Backbench Business debate on Economic Crime, 2 December 2021

3 Online economic crime

Why online fraud is an issue

62. UK Finance's half-year fraud update highlights the increase in fraud and in particular the growth in impersonation scams (where criminals pose as banks Government bodies or health officials to trick people out of their money), purchases scams (where people make payments for goods which never materialise), and investment scams (where people are persuaded to "invest" substantial amounts of money in non-existent assets). UK Finance says that many of these scams use online platforms, including fraudulent advertising through search engines and social media, and fake websites. Their analysis conducted earlier in 2021 found that 70 per cent of authorised push payment scams (See Chapter 4 for definitions) originated on an online platform.[75]

63. The FCA has also highlighted the growth in online scams. In its *Perimeter Report 2020/21*, it said:

> There are few practical barriers for online scams. Fraudsters have unprecedentedly cheap access to an online population of consumers who find it difficult to differentiate legitimate offers from fraudulent ones. There are promotions online for firms that do not exist, for firms that falsely claim to be regulated, for firms that claim to be based in the UK but are not, for products for which spurious claims of returns are made and for clones of legitimate authorised firms. This is a fast-growing problem: From April 2020 to March 2021 consumers reported 30,000 potential scams to us. This is 77% higher than in the previous 12 months.[76]

64. Another type of online promotion which is of concern is advertising of tax avoidance schemes. For example, BBC *File on 4* reported on 10 May 2021 that Facebook had been used to recruit directors for limited companies set up to exploit the Employment Allowance.[77]

65. Angela McLaren, Assistant Commissioner for Economic and Cybercrime, City of London Police, told us in oral evidence on 25 January 2021:

> "[…] If we look at the types of fraud that are most emergent at the moment, the vast majority of them will rely on some form of social media platform. That applies whether it's romance fraud, investment fraud or online shopping. Absolutely: the consistent theme through all these frauds is, obviously, the use of social networking and social media sites.[78]

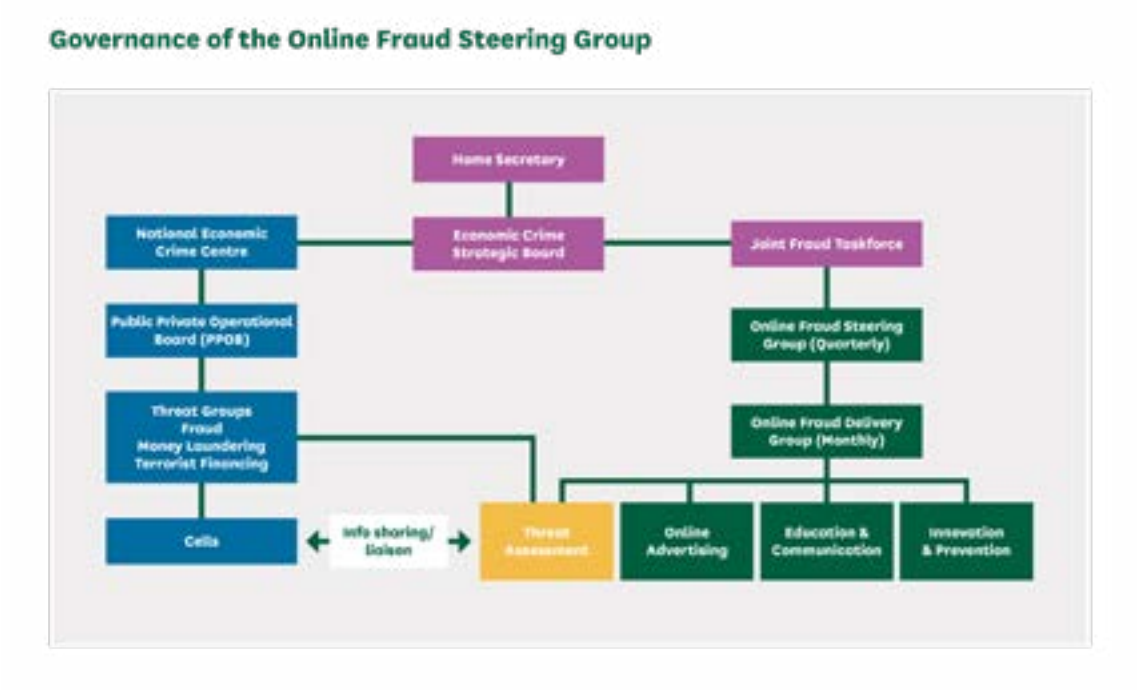
She also noted that "In 2019–20, social media featured in more than 39,000 crime reports to Action Fraud, with losses of over £120 million".[79]

66. Online companies have been taking steps to tackle frauds and scams perpetrated through their sites, whether user-generated or through advertising. The Online Fraud Steering Group (OFSG) is a public-private group set up following a roundtable hosted

75 UK Finance, 2021 Half Year Fraud Report, (22 September 2021) p.2
76 Financial Conduct Authority, Perimeter Report 2020/21, 21 October 2021, page 30
77 BBC News "Thousands recruited to front UK firms in 'tax dodge'" extracted 21 December 2021
78 Q81
79 Q81

by Government Ministers in April 2021, and consists of representatives from the Home Office, the Financial Conduct Authority, law enforcement agencies and online industry group techUK. The Group is co-chaired by the National Economic Crime Centre (NECC), UK Finance and techUK, and is focused on reducing the threat from online and cyber enabled-fraud in the UK.[80] TechUK explain how the governance of the Group works in the context of governance of economic crime across Government as follows:

Figure 3: Governance of the Online Fraud Steering Group



Source: techUK, December 2021[81]

The Draft Online Safety Bill

67. The abuse of online channels by fraudsters is something that the Government is seeking to address, in part through legislation to improve safety from online threats. On 12 May 2021 the Government published a Draft Online Safety Bill, designed to deal with problems of online harm and online crime. While the Draft Bill deals mainly with the regulation of online content for the purposes of child safety and the prevention of terrorism, the Government announced that the Bill would also include measures to protect people against user-generated financial fraud on social media and dating apps, including measures to protect people from romance scams and fake investment opportunities.[82] The Prime Minister confirmed that tackling fraud was integral to the Bill when he appeared before the Commons Liaison Committee in July 2021:

> I am very concerned that we should tackle fraud. Indeed, I am told that the Online Safety Bill does just that […] one of the key objectives of the Online Safety Bill is to tackle online fraud.[83]

80 National Crime Agency, Online Fraud Steering Group, [extracted 3 January 2022]
81 Published on Committee website
82 Department for Digital, Culture, Media and Sport and Home Office, Landmark laws to keep children safe, stop racial hate and protect democracy online published, 12 May2021 [Extracted 29 December 2021]
83 Oral evidence taken on 7 July 2021, HC 491 (2021–22), Qq 78–79 [The Prime Minister]

68. The Draft Online Safety Bill was considered by a Joint Committee of both Houses of Parliament,[84] which published a report on 10 December 2021 setting out its views on the draft Bill.[85]

69. During this inquiry and in evidence before the Joint Committee there have been calls for the anti-fraud elements of the Bill to be enhanced. Richard Piggin, Head of External Affairs, Which?, told us on 8 July that the Government should "swiftly introduce and give online platforms the legal responsibility to identify, remove and prevent fake and fraudulent content appearing on their sites."[86]

70. In the same oral evidence session, David Clarke, Chair, Fraud Advisory Panel, told us that online companies already had the technology to identify fraud but failed to apply it. He said:

> There is technology available to identify that and the big tech companies do not use it. They keep the data, but they do not show you it. They actually take down stuff. […] Technology could be switched on tomorrow to protect the consumer […].[87]

71. Angela McLaren, Assistant Commissioner for Economic and Cybercrime, City of London Police agreed. In oral evidence on 25 January, she said:

> There is absolutely more that can be done in that technology space. As I say, for every site we take down, more sites will come in, and if we go back to the victim within all this, they are absolutely preying on people's vulnerabilities, whether that is loneliness or concerns about their future financial security. These are not just sites that cause no harm; these are absolutely focused on really vulnerable people, or people who are vulnerable at a point in time.[88]

72. Mark Steward, Director of Enforcement, Financial Conduct Authority, expressed concern about another issue with the Bill, which is that it may lack flexibility to deal with new developments in finance. Speaking to the Joint Committee on the Online Safety Bill in oral evidence on 18 October 2021, he said:

> There needs to be a mechanism that allows the Bill to operate in a travelling way as the market becomes more sophisticated, and perhaps more complicated, as new harms arise. It does not really matter to us what the mechanism is for the Bill to have a greater say in this space, as long as there is a way in which Ofcom and the regulators can act flexibly with an evolving market. As a regulator with a fixed statutory perimeter that we find enormously difficult, there needs to be some flexibility in some way, shape or form for the regulator.[89]

84 House of Lords House of Commons Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill Report of Session 2021–22, HL Paper 129/HC 609

85 Joint Committee on the Draft Online Safety Bill, report of Session 2021–22, Draft Online Safety Bill (HL Paper 129/HC 609)

86 Q248

87 Q236

88 Q81

89 Oral evidence taken on 18 October 2021 by the Joint Committee on the Draft Online Safety Bill Q126 [Mark Steward]

73. The Joint Committee recommended that a "fraud offence" should be included in the list of "relevant offences" in Clause 41(4) of the draft Bill, and that designating online fraudulent content as "priority illegal content" (defined in Clause 41(5)(c)) would place a duty on providers to minimise the risk that the content would appear on their service in the first place, rather than just remove it on request.[90] The Joint Committee also recommended that:

> … the Government should consult with the regulatory authorities on the appropriate offences to designate under this section. The Government should ensure that this does not compromise existing consumer protection regulation.[91]

74. ***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.***

Financial advertising

75. An important focus of evidence to our inquiry was harm caused by the advertising of fraudulent financial products. Fraudulent user-generated content, such as fake investment opportunities posted by users on social media, would be regulated under the Draft Online Safety Bill. But paid-for advertising is specifically excluded from the scope of regulation under the draft Bill by Clause 39(2)(f). In a press release accompanying publication of the draft Bill, the Department for Digital, Culture, Media and Sport said that "fraud via advertising, emails or cloned websites will not be in scope because the Bill focuses on harm committed through user-generated content."[92]

76. Witnesses have argued, in the course of both this inquiry and previous inquiries, that paid-for advertising should be included in the scope of regulation under the Online Safety Bill. The issue arose during our inquiry into the FCA's regulation of London Capital and Finance, and we recommended at the end of that inquiry 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".[93]

77. Some have questioned whether there is a distinct boundary between user-generated content and paid-for advertising. On 18 October 2021, Martin Lewis OBE, Founder

90 Joint Committee on the Draft Online Safety Bill, report of Session 2021–22, Draft Online Safety Bill (HL Paper 129/HC 609) paras 191 and 194

91 Joint Committee on the Draft Online Safety Bill, report of Session 2021–22, Draft Online Safety Bill (HL Paper 129/HC 609) para 194

92 Department for Digital, Culture, Media and Sport and Home Office, Landmark laws to keep children safe, stop racial hate and protect democracy online published, 12 May2021 [Extracted 29 December 2021]

93 Treasury Committee, Fourth Report of session 2021–22- The Financial Conduct Authority's Regulation of London Capital & Finance HC 149 para 192

and Chair at MoneySavingExpert.com and Money and Mental Health Policy Institute, appeared before the Joint Committee on the Online Safety Bill, and when commenting on whether the Bill should cover advertising, made that point:

> You tell me: if I do a post and then pay to promote it, is it an ad or is it user-generated? If I do a dating profile and then pay to promote it, is it an ad or is it user-generated? Where do I cross the line? If the answer is that as soon as I pay it is an advert, all I have to do is pay a penny and everyone in my user-generated post is not covered by this Bill. It is ridiculous. It is farcical … .[94]

78. Online social media platforms rely on advertising revenue and have hosted advertising of financial services and products which are either fraudulent or not compliant with regulations designed to protect the consumer. We asked Mark Steward, Director of Enforcement, Financial Conduct Authority, about the increase in economic crime since the start of the COVID-19 pandemic in 2020. He said:

> The area where it is most noticeable for the FCA has been the increase in online scams and frauds. The particular focus for us is online advertising of regulated activities—those that we regulate—by firms that are not authorised by us. In many instances, we believe that some of those ads are scams and frauds.[95]

79. The FCA has been posting its own advertisements online to warn consumers about the risks of harm from online adverts for fraudulent financial investment products. Reports appeared in the press suggesting that the FCA had paid Google £600,000 a year to post scam warnings.[96] Mark Steward told us:

> We would prefer that these ads were not published in the first place, to be really frank. The irony of us having to pay social media to publish warnings about advertising that they are receiving money from is not lost on us."[97]

80. There is currently no legal requirement for internet platforms and social media companies to do any Know Your Customer checks on their advertisers. This makes it easy for fraudsters to purchase advertising, and more difficult for social media companies and internet platforms to filter it out. This is in contrast to the financial services companies, who are required to do Know Your Customer checks when onboarding new customers.

81. Mr Steward believed that advertising should be regulated under the Online Safety Bill. He said:

> "[…] It should be clearly included; otherwise, there is no mechanism for social media to be legally obligated to do some very basic things that do not happen now, such as ensuring that the person who is placing the ad is someone they know, they know where the person is, and they know that the

94 Oral evidence taken on 18 October 2021 by the Joint Committee on the Draft Online Safety Bill , Q112 [Martin Lewis]
95 Q96
96 See for example UK online harms bill misses fraud's gateway, Financial Times 16 May 2021
97 Q124

> address and contact details are correct, or, where the person is advertising a financial investment, that that firm is properly authorised by the FCA to do so. […]"[98]

82. The Internet Advertising Bureau (UK)[99] expressed concerns about the current debate about online advertising and the Online Safety Bill, and it defended the industry's approach:

> Scam advertising is a devastating crime against consumers and legitimate advertising businesses alike. The advertising industry has responded with both determination and creativity and is committed to continuing to address it. IAB UK is troubled by generalised assertions that the industry response as a whole has come late and falls short. We do not dispute that these efforts should evolve and be responsive to the changing patterns of criminal activity. The DCMS Online Advertising Programme and the Home Office Fraud Action Plan workstreams are both conducting work to examine potential solutions, and this work should include devoting proper time and attention to understanding and examining both the substance and quality of the industry response and what it has achieved, as well as the evolving criminal behaviour the industry experiences.[100]

The law on financial promotions

83. Section 21 of the Financial Services and Markets Act 2000 regulates the ability to advertise financial products or services. Mark Steward explained to us how this worked on 14 June 2021:

> … there is a provision in the Financial Services and Markets Act that means that particular financial promotions can be communicated only by a person who is authorised by the FCA, or the communication must be approved by a person authorised by the FCA.[101]
>
> Online companies which facilitate access to promotions which are not communicated in line with the requirements of the Act may also fall foul of section 21 if they provide optimised or value-added services in relation to that promotion.

84. We note that the requirement for approval by a person authorised by the FCA is not a complete solution to the problem of financial advertising. For example, London Capital and Finance, the subject of our recent report,[102] was authorised by the FCA, but weaknesses in the supervisory regime still led to harm to investors.

85. The FCA has indicated that it wants more powers to force online companies to comply with the law. In a letter to the Committee on 14 July 2021, the FCA explained that

98 Q120

99 The Internet Advertising Bureau (IAB UK) is the industry body for digital advertising, with 1200 members. See iabUK, 'about us' [extracted 10 January 2022]

100 Internet Advertising Bureau UK (ECC0094)

101 Q133. See also letter Mark Steward to Chair, Treasury Committee dated 14 July 2021 which explains that the relevant legislation is section 21 of the Financial Services and Markets Act 2000.

102 Treasury Committee, Fourth Report of Session 2021–22, The Financial Conduct Authority's Regulation of London Capital & Finance plc. HC 149, 24 June 2021

it has powers to investigate and prosecute for offences listed in section 168 of the Financial Services and Markets Act 2000 (FSMA); but that list does not include prosecutions for offences solely under the Fraud Act 2006. The FCA could prosecute for fraud offences when they were additional to offences listed in section 168 of FSMA, but they would need to be brought as private prosecutions. The FCA pointed out that prosecutions under the Fraud Act encounter a very high bar for proof of fraud in the case of online companies.[103]

The FCA's work with online companies

86. During 2021 the FCA began working with online companies to ensure that they did not accept advertising for regulated financial products which were not in accordance with the law. Following pressure from the FCA, Google agreed to only allow financial services advertisements approved by an authorised firm to appear in its optimised search services.[104] This change was announced on 30 August and took effect from 6 September 2021[105] and was welcomed by Charles Randell, Chair of the FCA.[106]

87. As part of the deal that it reached with Google, the FCA accepted a $3 million advertisement credit from Google and the offer of another $2 million worth of advertisement credits to support industry awareness campaigns.[107] Following our oral evidence session with online companies on 22 September 2021, our Chair wrote to a range of online companies, including those which had given oral evidence, asking them to clarify what their policies were regarding advertising, and whether they had received payments from the FCA for warning advertisements.

88. The Chief Executive of the Financial Conduct Authority wrote to us on 19 January 2022[108] explaining in more detail payments that the FCA has made to online companies for scam warning messages in relation to investments, pensions and loan fee fraud. These are set out in Table 1 below:

Table 1: Costs of delivering scam messages to end November 2021

	2019	2020	2021
Google	£217,264.72	£256,145.50	£217,521.91
Twitter	£32,536.31	£64,354.49	£64,343.56
Meta (includes Facebook and Instagram)	£153,730	£123,440	£86,940

Source: Financial Conduct Authority

The letter explains that the sums in the table do not include spending on other activities and campaigns which the FCA has carried out through channels such as those run by

103 Letter from Mark Steward, FCA Executive Director of Enforcement and Market Oversight to Chair, 14 July 2021, 'Assessment of Corporate Fraud Through Online Promotion'

104 Letter from Mark Steward, FCA Executive Director of Enforcement and Market Oversight to Chair, 14 July 2021, 'Assessment of Corporate Fraud Through Online Promotion'. See also Financial services advertising in the United Kingdom, Google.com extracted 20 December 2021

105 Google (ECC0086) page 1

106 See FCA, 'Speech by Charles Randell, Chair of the FCA and PSR, to the Cambridge International Symposium on Economic Crime', 6 September 2021. [Extracted 10 January 2022]

107 Google (ECC00086)

108 Letter Nikhil Rathi to Chair of Committee, 19 January 2022

Microsoft, Snapchat and TikTok (for example the InvestSmart campaign).[109] TikTok disclosed to us that they had been paid £50,000 by the FCA.[110] This means that, between 2019 and 2021, the FCA has paid at least £1,179,336 to online companies to warn about scams and on other campaigns.

89. On 10 December 2021, techUK, the trade body for UK online companies, announced that Facebook (now known as Meta), Twitter and Microsoft had committed "to introduce a revised advertising onboarding process that requires UK regulated financial services to be authorised by FCA prior to serving financial services adverts to their sites". Similar steps had already been taken by Google, TikTok and Amazon. We note however that "there is no set timeline for when these changes will come into force, and processes will vary from company to company".[111]

90. We also note that some major online platforms have yet to make similar commitments. We wrote to Snap Inc (owner of Snapchat, an instant messaging app), asking what plans they had to comply with FCA advertising policy. In its reply, Snap Inc (which is not a member of techUK), did not disclose any plans to change its systems to ensure that advertisers of financial promotions are authorised by the FCA.[112] Nor did eBay provide any such statement when responding to a letter from the Committee.[113]

91. We asked John Glen MP, Economic Secretary to the Treasury, whether he believed that online advertising should be included in the Online Safety Bill. He said that "the big area that we want to look at very carefully before that legislation comes into force is advertising".[114] He added that: "We welcome the efforts that some of the platforms are taking, but we have to have an effective response. The online advertising programme is at the moment what we need DCMS to come forward with. Clearly, we need an effective intervention that deals with the nature of the risks around advertising".[115]

92. When we asked whether the Treasury will be pushing for online advertising to be included in the Bill, he said:

> It depends what happens with the online advertising programme that DCMS is responsible for. I met the previous Minister, Caroline Dinenage, at least once—I think twice—before she left office. This is a massive problem, and a significant opportunity which we cannot miss in the absence of a better solution. That seems to me the right approach. However, I recognise the complexity in delivering it in a coherent and legally sensible way.[116]

93. The Rt Hon. Damian Hinds MP, Minister for Security and Borders, Home Office, was uncertain that the Online Safety Bill was the right vehicle for regulation of online advertising. He said:

109 Financial Conduct Authority, "InvestSmart", [extracted 19 January 2022]
110 TikTok [ECC0093]
111 techUK, 'Major technology companies step up efforts to tackle financial fraud and scam adverts,' extracted 21 December 2021
112 Written Evidence from Snap Inc (ECC0098),
113 Ebay (ECC0088)
114 Q428
115 Q429
116 Q432

> … we are also very conscious that there are other types of fraud where the business model is about advertising online, and we need to bear down on that. The question we are facing is not whether to bear down on it, but how: what is the best way to do it? Is it best to do it through the Online Safety Bill? Is it best to do it through the online advertising programme, or some other way …[117]

Online advertising: our conclusions

94. **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.**

95. ***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.**

96. ***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.***

97. **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.**

Compensation for victims of fraud by online companies

98. It has been proposed that online companies should be liable to compensate victims of frauds conducted through their websites, in much the same way that banks are required to reimburse victims of unauthorised payment fraud and card fraud.[118] Anthony Browne MP, a member of our Committee, wrote an article for the *Times* in which he argued:

> … Unless social media companies pay compensation, promoting fraud will remain a profitable activity for them, so they have no internal financial incentives to reduce it. …
>
> […]

117 Q433

118 See The Payment Services Regulations 2017 (SI2017/752) regulations 76 and 77. Authorised push payment (APP) fraud can be reimbursed by banks under the voluntary Contingent Reimbursement Model Code", and the Payment Systems Regulator and Government have announced that reimbursement of customers suffering APP fraud will be made mandatory.

> But fraud will remain endemic while technology firms make huge profits promoting fraudsters. Their refusal to compensate means victims who can't get compensation from banks don't get any money back. There is a clear line of responsibility: the social media company has a financial relationship with the fraudster and the click-throughs show how they delivered the victims.
>
> Under the "polluter pays" principle, the Government should, through its Online Safety Bill, require social media and telecoms companies to join banks in compensating victims. […][119]

99. In oral evidence, Google and Facebook said their aim was to stop fraud happening in the first place, implying that there was no need for them to contribute to compensation. Amanda Storey, Director of Trust and Safety, Google, told us that "we are working hard to make sure that we are never in a position where a user needs to be compensated".[120] Allison Lucas, Content Policy Director, Facebook, said that "I can also say that we are investing money to tackle the underlying issues and to prevent the ads from running in the first place" and that "we are also committed to solving this bigger picture".[121]

100. We asked the Rt Hon. Damian Hinds MP, Minister for Security and Borders, Home Office, whether he thought that online companies should be made responsible for paying customers back when they have hosted advertising that leads to fraud. He said:

> I want everyone's incentives to be aligned. Right now, the banks have a strong incentive not to have fraud taking place through their channels, because they incur a cost. In other parts of the economy, there is not that incentive, and in some parts, you could even say that there is an incentive the other way. I don't think that people think this way, but you can see how it could happen that if you are receiving advertising revenue as a result of people defrauding others, your incentive might be in the opposite direction. I want us to find a way to ensure that everyone's incentives are aligned.[122]

101. **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.**

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

Overall conclusions on self-regulation of online companies

103. **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**

119 The Times "Tech giants must pay for the rise in online fraudsters" 17 November 2021
120 Q409
121 Q414 and Q416
122 Q488

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.

104. **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.**

105. ***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.***

4 Authorised push payment fraud

106. Fraud committed against consumers was the subject of a report by the previous Treasury Committee in 2019[123] and continues to be a problem. In this inquiry we have focussed on a type of fraud known as Authorised Push Payment Fraud, which is the subject of ongoing work by the Payment Systems Regulator.

Unauthorised and authorised push payment fraud

107. In an unauthorised fraudulent transaction, the account holder does not provide authorisation for the payment to proceed, and the transaction is carried out by a third party, the fraudster. A payment can be "push", which is when the customer directly arranges for the payment, or "pull", when a payment is taken from a customer's account, for example by direct debit. Either way, if the payment is unauthorised by the account holder, the Payment Services Regulations 2017 provide statutory protection for consumers from fraud.[124]

108. Fraudsters may also try to trick the account holder into authorising payments to be made to another account which is controlled by the fraudster. This type of fraud is "authorised" because the customer has authorised the payment but has not realised it is to a fraudster. This type of fraud is known as an "authorised push payment"(APP) fraud.[125] There is no statutory protection for consumers who are victims of authorised push payment fraud, in contrast to unauthorised payment fraud.

109. APP fraud is a growing problem. UK Finance, the trade body for around 300 firms in the banking and finance industry, publishes regular updates about fraud. Its latest half-year fraud report, published on 22 September 2021, highlights the increase in fraud and particularly the increase in APP fraud. In the first half of 2021, losses due to unauthorised financial fraud using payment cards, remote banking and cheques rose seven per cent compared to the first half of 2020, to £398.6 million. But £355.3 million was lost to authorised push payment scams, an increase of 71 per cent compared to losses seen in the same period in 2020.[126] For the first time, APP fraud in the UK now exceeds card fraud.[127]

The Contingent Reimbursement Model Code

110. Although the problem of APP fraud is growing, it is not new. In 2016, in response to the rise of APP fraud, the consumer campaigning group Which? made a "super-complaint" to the Payment Systems Regulator (PSR), the relevant regulator.[128] In April 2018, the PSR set up an industry steering group to create a voluntary industry code to provide reimbursement for victims of APP Fraud. This led to the Contingent Reimbursement Model (CRM) Code, which came into effect on 28 May 2019.[129]

123 Treasury Committee, Third Report of Session 2019, Economic Crime - Consumer View, 1 November 2019, HC 248
124 The Payment Services Regulations 2017 (SI2017/752)
125 UK Finance, 2021 Half Year Fraud Report, (22 September 2021) p.6
126 UK Finance, 2021 Half Year Fraud Report, (22 September 2021) p.6
127 UK Finance, 2021 Half Year Fraud Report, (22 September 2021) p.2
128 Payment Systems Regulator, Which super-complaint on payment scams, extracted 16 December 2021.
129 A full history of the CRM code is provided by the PSR: Payment Systems regulator 'A history of our work to prevent APP scams', and Lending Standards Board , 'Contingent Reimbursement Model Code for Authorised Push Payment Scams', 20 April 2021.

111. Payment service providers (PSPs) which have signed up to the Code agree to reimburse victims of APP fraud where the customer has met the standards expected of them. The CRM Code has benefited many consumers, but it is non-statutory and voluntary. At present there are only nine signatory PSPs (Barclays, HSBC, Lloyds, Metro, Nationwide, RBS, Santander, Starling and Co-Op).[130] TSB has decided not to sign because it has its own repayment guarantee.[131]

112. On 1 November 2019, our predecessor Committee, in a report titled *Economic Crime: Consumer View*, recommended that the Contingent Reimbursement Model (CRM) Code should be made compulsory through legislation.[132] The Government, in its response published in March 2020, said that "The Code is still in its infancy and the Government believes it should be given time to embed and take full effect before its effectiveness can properly be assessed."[133]

113. On 11 February in 2021 the PSR launched a "*Call for views*" about the future of the CRM code, recognising that improvements are needed. In their *Call for views* they said:

> Though the CRM Code has improved outcomes for customers, our analysis suggests that its application hasn't yet led to the significant reduction in APP scam losses incurred by customers that is needed. We estimate the overall level of reimbursement and repatriation is less than 50% of APP losses assessed under the CRM Code. This figure also varies considerably across signatory Payment Service Providers (PSPs.)[134]

They proposed:

- mandatory protection of customers, by changing industry rules so that all payment service providers (PSPs) are required to reimburse victims of APP scams who have acted appropriately.
- requiring PSPs to publish their APP scam, reimbursement and repatriation levels, to improve transparency
- requiring PSPs to adopt a standardised approach to risk-rating transactions and to share the risk scores with other PSPs involved in the transaction, to improve information sharing about suspect transactions.[135]

114. On 18 November 2021 the PSR launched a second stage consultation.[136] It stated that it intended to:

- Require publication of comparative data of re-imbursement rates between different banks
- Support and require the industry to improve intelligence sharing

130 Payment Systems Regulator, Authorised Push Payment (APP) scams: Call for views, 11 February 2021
131 TSB, Fraud Guarantee, accessed 16 December 2021
132 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246, para 114
133 Treasury Committee, Second Special Report of Session 2019–21, Economic Crime: Consumer View: Government and Regulators' Responses to Committee's Third Report of Session 2019, HC 91, page 11
134 Payment Systems Regulator Authorised Push Payment (APP) scams: Call for views 11 February 2021, para 1.5
135 Ibid para 1.10
136 Payment Systems Regulator, Authorised push payment (APP) scams consultation paper, 18 November 2021

- Make reimbursements mandatory.

115. At the same time, the Economic Secretary to the Treasury, John Glen MP, confirmed that the Government would now legislate to require firms to make refunds, just as the previous Treasury Committee had called for in 2019. He said:

> Push payment fraud is posing an escalating risk to UK customers, with increasingly sophisticated scams that can be detrimental to people's lives. The Government's position is that liability and reimbursement requirements on firms need to be clear so that customers are suitably protected. It is welcome that the Payment Systems Regulator is consulting on measures to that end, and to help prevent these scams from happening in the first place. The Government will also legislate to address any barriers to regulatory action at the earliest opportunity.[137]

116. **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.**

117. **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.**

118. ***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.***

Confirmation of Payee

119. Confirmation of Payee (CoP) is a way of giving customers (both personal and business) greater assurance that they are sending payments to the intended recipient, helping them to avoid making accidental, misdirected payments to the wrong account holder, as well as providing another layer of protection in the fight against fraud and scams.[138] When making a payment to a new payee electronically, CoP gives the details of who the payee's account is in the name of, giving the payer a chance to stop the transaction before a fraudulent payment is made.

120. The Payment Systems Regulator (PSR) used its regulatory powers (in the form of Specific Direction 10) to implement CoP in August 2019 to require members of the UK's six largest banking groups to implement CoP by the end of March 2020. Recognising

137 Payment Systems Regulator, PSR announces plans to stop APP scams, accessed 16 December.
138 UK Finance, 'Confirmation of Payee' extracted 16 December 2021

the pressure on businesses due to COVID-19, the Regulator announced that it would not take formal action until 30 June 2020 as long as consumers were not disadvantaged over the additional three months.[139] Though the CoP direction applies only to the six largest banking biggest payment service providers, the PSR says that this covers 90% of payments in the UK.[140]

121. On 21 May 2021 the PSR consulted on improving the CoP process and extending it to other payment service providers (PSPs).[141] Its consultation document evaluated the impact of CoP and noted that:

> … PSPs that have enabled CoP over the past year have seen a reduction in the types of APP scams that CoP can prevent, compared to an increase in such scams for PSPs not participating in the service. This suggests that CoP has improved transaction security for PSPs offering the service.[142]

The PSR published a summary of the responses to its consultation on 6 October 2021, at the same time setting out its own views.[143] It then published a further technical consultation in December 2021.[144]

122. At the time of the Report by the previous Treasury Committee, following its inquiry on consumer fraud in 2019, the Confirmation of Payee regime had not yet been implemented, and the then Committee recommended that it should be introduced as a matter of urgency.[145]

123. **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.**

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

125. ***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.***

139 Payment Systems Regulator PSR confirms widespread implementation of name-checking system, Confirmation of Payee, 1 July 2020, extracted 21 December 2021
140 Payment Systems Regulator, CP21/6 - Confirmation of Payee - Phase 2 Call for Views, 20 May 2021, para 2.2
141 Payment Systems Regulator, CP21/6 - Confirmation of Payee - Phase 2 Call for Views, 20 May 2021
142 Payment Systems Regulator, CP21/6 - Confirmation of Payee - Phase 2 Call for Views, 20 May 2021, para 2.6
143 Payment Systems Regulator, Confirmation of Payee Response to our call for views CP21, 6 October 2021
144 Payment Systems Regulator, Confirmation of Payee Ending dual running, December 2021
145 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246, para 41

5 Anti-money laundering

126. A House of Commons Library briefing paper provides the following description of money laundering:

> Money laundering describes the procedures used to make money which has been acquired from criminal activity appear to have been lawfully acquired. These procedures are typically highly complex and by design hard to trace. Funds, whether generated through organised crime, terrorism or drug trafficking, will be placed within the mainstream economy or financial sector and the source and origin of the funds will be progressively concealed with each transaction. These transactions must be carried out in such a way as to avoid attracting the attention of the authorities and with it the risk of detection, confiscation and criminal proceedings. Because of the laundering, the funds will appear to be lawful.[146]

127. Governments around the world legislate to prevent and criminalise money laundering. There is an extensive legislative framework in the UK, the full details of which are set out by the Government in Chapter 2 of the *National risk assessment of money laundering and terrorist financing 2020*.[147] Legislation aims to restrict criminals' ability to operate in the UK and alert law enforcement agencies when criminals attempt to move money around the economy. Money laundering is an offence in its own right, but it is closely related to other forms of serious and organised crime, as well as the financing of terrorism. Legislation provides for "supervision" of firms to ensure that they comply with anti-money laundering laws. Supervision is split between the FCA (which supervises banks), professional bodies (which supervise their members, and which are in turn supervised by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS)), the Gambling Commission (which supervises casinos and betting firms) and HMRC (which supervises a wide range of other firms). This inquiry has concentrated on the effectiveness of the UK anti-money laundering (AML) regime.

128. The National Crime Agency (NCA) says that money laundering underpins and enables most forms of organised crime, allowing crime groups to further their operations and conceal their assets. It also says that the UK remains an attractive place for criminals from around the world who want to set up companies to launder their profits,[148] and that money laundering threatens national security:

> The critical importance of the financial sector to the UK's economy means that money laundering, particularly high-end money laundering (the laundering of large amounts of illicit funds through the financial and professional services sectors) can threaten the UK's national security and prosperity, and undermine the integrity of the UK's financial system and international reputation.[149]

146 Money Laundering Law, Briefing Paper no. 2593. House of Commons Library, 14 February 2018
147 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020
148 National Crime Agency, National Strategic Assessment of Serious and Organised Crime 2020,, para 161
149 National Crime Agency, Money laundering and illicit finance [extracted 12 January 2022]

Scale of the problem

129. The scale of money laundering is difficult to quantify. The inter-governmental Financial Action Taskforce (FATF) offers statistics from the United Nations Office on Drugs and Crime (UNODC), which estimated in 2009 that criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered. The FATF also continues to cite figures produced by the International Monetary Fund, which stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product.[150] The National Strategic Assessment of Serious and Organised Crime 2020 suggested that hundreds of billions of pounds could be laundered in the UK annually.[151]

130. The 2019 report by the previous Treasury Committee, *Economic Crime – Anti-money laundering supervision and sanctions implementation*,[152] recommended that the Government should attempt to quantify the scale of the problem. In the Government's Economic Crime Plan 2019–2022, Strategic priority 1 includes actions to understand the economic crime threat.[153] and the *National risk assessment of money laundering and terrorist financing* provides the latest assessment of the scale of the problem.[154] However the risk assessment says merely that:

> It remains difficult to quantify the scale of the money laundering threat to the UK, but it is likely there has been an increase in the amount of money being laundered since 2017.[155]

131. Graeme Biggar, Director-General at the National Economic Crime Centre, commented on the Committee's 2019 recommendation when giving oral evidence on 25 January 2021:

> I think we have done a good job in improving our understanding of economic crime. One of the recommendations of this Committee previously was that we should come up with better overall estimates of the scale of economic crime, particularly money laundering. That is really hard, so we are struggling with doing that, but we are beginning to get under the skin of where elements of it are coming from. We have made some much better assessments now of the scale of money laundering—cash money laundering in this country on the back of crime in this country, as opposed to money that comes from other countries.[156]

The effectiveness of the SARs process

132. A key part of the anti-money laundering (AML) legislation in the UK and elsewhere in the world is suspicious activity reports (SARs). In the UK these are sent to the UK

150 Financial Action Taskforce, 'How much money is laundered per year?' [extracted 10 January 2022]
151 National Crime Agency, National Strategic Assessment of Serious and Organised Crime 2020, para 160
152 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime - Anti-money laundering supervision and sanctions implementation, 8 March 2019, para 16
153 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, page 22
154 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020
155 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020, para 3.6
156 Q40

Financial Intelligence Unit (UKFIU) by regulated firms when they handle money that might possibly be laundered. There are two types of SARs: ordinary SARs and "defence" SARs, of which in turn there are two types, Defence Against Money Laundering (DAML) and Defence Against Terrorism Financing (DATF) SARs. "Defence" SARs are made by firms when they need to make a transaction which could itself be money laundering because of their suspicions about the nature of a client.

133. The number of SARs has steadily increased. The National Crime Agency (NCA) publishes an annual report about SARs, the most recent being from 2020. This shows that the total number of SARs was 573,085 between April 2019 and March 2020, a 19.78% increase on numbers of SARs submitted in the previous year April 2018 and March 2019.[157] The NCA also recorded 62,408 "defence SARs".[158] Graeme Biggar, Director-General at the National Economic Crime Centre, spoke about the increasing numbers of SARs in oral evidence to the Committee on 25 January 2021:

> Twenty years ago, we got 20,000 suspicious activity reports in, largely from banks. This year, we would not be surprised if we got three quarters of a million, and the number of defence against money laundering SARs, where we are told in advance and given the option to refuse permission to proceed, is going to double, we think, this year. The sheer volume coming through is really significant and very hard to deal with.[159]

134. Mr Biggar also said that the increase in the numbers of SARs has led to an increase in staff in the NCA Financial Intelligence Unit, noting on staff numbers that "in 2018, it was 80; it is now 140. The plan is to get close to 200."[160] Recognising the need to analyse all the data from the SARs to extract crime fighting intelligence, he said: "We are putting in place new IT to make it easier for reporters to get the information to us in the first place, and to give us much stronger analytical tools to use when we have it."[161] Going on to talk about the benefits of SARs, he said that "the amount of money that has been restrained as a result of SARs has tripled in the last three years, or two and a half years, from about £50 million to £171 million."[162]

135. Asked about what can be done to improve the SARs regime, Mr Biggar told us that banks should share information with the NCA even in cases where the current legal level test of suspicion may not be met:

> … what does not happen very much at the moment is banks sharing information on something they are looking at for which they do not think they have yet met the legal threshold of suspicion, but which they are concerned about. If they did that more often, they would be able to pull together much more substantial intelligence reports for us. We are now working with them on how to do that within the current legal framework, and on what further legal changes might be necessary to enable more of that to happen.[163]

157 National Crime agency, SARs Annual Report 2020, p. 4
158 Ibid
159 Q10
160 Q10
161 Q10
162 Q10
163 Q53

136. Mark Steward, Director of Enforcement, Financial Conduct Authority, told us that the FCA has seen an increase in DAML SARs submitted by banks into the UK Financial Intelligence Unit (FIU). He contrasted the SARs regime with the software available to the FCA to tackle insider trading:

> … The amount of data that flows into the FIU is large, but it is not beyond the ability to manage that size of data using the kinds of software applications and algorithms that now exist.
>
> … we have also noticed an increase in defensive SARs being filed by banks. They are often rather more interesting. … we have also used them as a launch pad to freeze money. We get a very limited space of time in which we can do that, under the process, but we have been doing that as well. …. More needs to be done in order to get more out of the valuable data that is in there. Otherwise, it just sits there."[164]
>
> If I think about the other databases that we administer, we get a many-times multiple of that amount of data every day into our market data processor, where we analyse market transactions, looking for insider dealing and manipulation. It is a much bigger database, and yet we have the software to be able to analyse that in real time. The same can be done with the FIU.[165]

137. In 2017 the Government announced a SARs reform programme, led by the Home Office, jointly with the National Crime Agency,[166] which began in July 2018.[167] That reform programme constitutes Action 30 in the Economic Crime Plan.[168] It set out a range of actions to improve the SARs regime, including "IT transformation", "a comprehensive regime-wide approach to feedback and guidance to iteratively improve SARs quality and regime processes", and an increase in analytical resource and capabilities for the UK Financial Intelligence Unit[169] and for Regional Organised Crime Units.[170] The programme also aims to "address the Financial Action Task Force's criticisms regarding the role and resourcing of the UKFIU".[171]

138. The previous Treasury Committee's Report, *Economic Crime - Anti-money laundering supervision and sanctions implementation*, welcomed the SARs reform programme, which in 2019 was relatively new,[172] and it presented evidence on what was needed in the way of reform. The problems identified in that Report still stand. The Government said in response to the Committee's Report:

164 Q186
165 Q187
166 National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017, page 29
167 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020, para 2.9
168 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, page 45
169 The NCA says that the "key function of the UKFIU is to receive, analyse and disseminate Suspicious Activity Reports (SARs) through the SARs regime" and that "The UKFIU has a duty to ensure that the financial intelligence available within SARs is being fully exploited in order to effectively tackle serious and organised crime, specifically within the areas of money laundering and terrorist financing." See SAR Online Information (ukciu.gov.uk)
170 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, page 45 para 5.36
171 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, page 45 para 5.37. The FATF criticisms of UKFIU resources are in its review of the UK, "'Anti-money laundering and counter-terrorist financing measures in the United Kingdom", 2018, see page 39
172 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime - Anti-money laundering supervision and sanctions implementation, 8 March 2019, para 163

> The Government is committed to reforming the SARs regime. In particular, the Government wants to reduce tick-box compliance, direct the regime to focus on the highest threats, help firms better protect themselves and improve law enforcement outcomes.[173]

139. Exactly what the SARs reform programme has achieved so far, what is still to be done and when it will end, is unclear. The Home Office does not appear to have published any detailed information about what the programme is doing or what milestones have been set for it. The Government's *National Risk Assessment on Money Laundering* says "The SARs reform programme has … increased capacity of the UK Financial Intelligence Unit (UKFIU) to deliver feedback to reporters on SARs reporting, which will enhance the quality of information submitted to law enforcement in the future".[174] The Home Office has recently appointed a new Programme Director, Duncan Tessier, who gave oral evidence to the inquiry on 29 November 2021. He said:

> The problems of the SARs regime are well known. It certainly needs reform, and that was something that came out quite clearly in the 2018 FATF review. We are doing three things. First, we are replacing the IT, which is over 20 years old and in real need of a comprehensive upgrade, so we are taking that forward. Secondly, we are reviewing the legislation and regulations that sit around the SARs regime, particularly targeting the issues of over-reporting in some sectors and under-reporting in others. Thirdly, we are looking to increase the staffing in both law enforcement and within the UK Financial Intelligence Unit, which we are making some really good progress on.[175]

140. The SARs reform programme is on the list of Government Major Projects which are being reviewed by the Infrastructure and Projects Authority. In its 2020–21 annual report,[176] the Authority notes that the project status is "amber",[177] which means "Successful delivery appears feasible but significant issues already exist, requiring management attention. These appear resolvable at this stage and, if addressed promptly, should not present a cost/schedule overrun."[178]

141. **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, so as to make full use of them in the fight against economic crime and organised crime more generally.**

142. **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.***

173 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 12

174 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020, see para 7.34

175 Q531

176 Infrastructure and Projects Authority, Annual Report on Major Projects 2020–21,

177 Ibid, page 51

178 Ibid, page 35

143. **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.**

144. ***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.***

Supervision of professional bodies and the Office for Professional Body Anti-Money Laundering Supervision (OPBAS)

145. OPBAS provides supervision of 25 Professional Body anti-money laundering (AML) Supervisors, each of which are responsible for AML supervision in a field within the accounting and legal sectors.[179] OPBAS was created as part of a wider package of reforms in 2017 to strengthen the UK's AML and Counter Terrorist Financing (CTF) regime. It became operational on 1 February 2018 as part of the FCA.[180] The powers of OPBAS are contained in the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017. These regulations place responsibility on the FCA to "have regard to the importance of ensuring that self-regulatory organisations comply with any supervision requirement".[181]

146. OPBAS publishes reports about the progress it has made in improving anti-money laundering compliance within the professional bodies. The most recent report was published in September 2021.[182] It found that professional body supervisors (PBSs) were "generally compliant" but it also found evidence of inconsistency and "significant weaknesses".[183] Examples of such weaknesses identified in the report are that:

- Only 15% of PBSs were effective in using predictable and proportionate supervisory action
- 50% failed to ensure that members took timely action to correct identified gaps
- Only 33% were effective in developing and recording in writing adequate risk profiles for their sector and only 29% were effective in regularly reviewing and appraising risks.

179 The relevant bodies are listed in the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (SI2017/692), see Schedule 1. In addition to the 22 listed there, OPBAS also has responsibility for those with delegated regulatory functions: CILEx Regulation, Bar Standards Board and Solicitors Regulation Authority. See OPBAS, 'Progress and themes from our 2020/21 supervisory assessments' page 30

180 OPBAS, Themes from the 2018 OPBAS anti-money laundering supervisory assessments, March 2019.

181 The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, (SI2017/1301). regulation 3

182 OPBAS, Progress and themes from our 2020/21 supervisory assessments, September 2021

183 Ibid, para 2.6 page 5

147. We questioned witnesses about OPBAS. Giving evidence in January 2021, Graeme Biggar, Director-General at the National Economic Crime Centre, told us that OPBAS was:

> … doing a very good job. They will, I am sure, want to get firmer and more assertive with the supervisors that they are supervising … I think there will be a question for Government—it is probably not immediate—about whether a system that has 22 supervisors for the legal and accountancy sector can be right. We should give OPBAS a really good opportunity to show that this can work, but there will be a question about whether it does.[184]

148. Helena Wood, Associate Fellow, RUSI Centre for Financial Crime and Security Studies, told us that:

> OPBAS has done a really good job of setting out expectations, but it has not been able to deal with the fundamental problem with our AML supervision system, which is that it is fragmented and broken.[185]

Highlighting what she sees as a fundamental problem with the way the system works, with supervision done by private sector professional bodies, she said:

> we are outsourcing what is a public good to private sector actors that are under-resourced. They do not have access to the specialist intelligence tools …. They do not have recourse to proper intelligence, undercover officers and all those sorts of assets that you need to do this properly. We need to consider whether that system creates a credible deterrent in the first place.[186]

149. Duncan Hames, Director of Policy, Transparency International UK, was also concerned about OPBAS and the professional body supervision system. He said:

> … one of the problems here with the supervision system is that there is a conflict of interest by some of these professional body supervisors. They do not want to take the kind of action that is necessary because they know it would have consequences for them as an institute or a members' body.[187]

Going on to talk about what was needed he said:

> … there is a problem in supervision that the small team in OPBAS has been trying to crack. It seems that the way it is designed makes this an inevitable problem, which is why we have been calling for consolidation of anti-money laundering supervision, as it is far too fragmented and conflicted.[188]

150. Noting the limits of what the current supervision system can do, Mr Hames said:

> If you really wanted to focus on where you could make the biggest difference quickly, … there are lots of issues with anti-money laundering supervision, which remains a highly fragmented system. The Government's own

184 Q62
185 Q263
186 Q263
187 Q222
188 Q223

> oversight body, the Office for Professional Body Anti-Money Laundering Supervision—OPBAS—has presented some pretty critical findings about the capabilities of professional body anti-money laundering supervisors.[189]

151. The previous Treasury Committee's Report, *Economic Crime: Anti-money laundering supervision and sanctions implementation,*[190] published in 2019, has a chapter entitled "A fragmented approach to AML supervision",[191] which recommended a more joined up approach. It said:

> With the creation of OPBAS, the Government acknowledged that consistency across AML supervisors was important. The Committee recommends that it should go one stage further, by creating a supervisor of supervisors. The aim of this institution would be to ensure that there is consistency of supervision across all the AML supervisors, whether statutory or professional body[192]

The report also called for OPBAS to be placed on a firmer statutory footing, akin to the Financial Ombudsman Service.[193]

152. The Government, in its response to this recommendation,[194] said that HM Treasury would, as required by regulations, publish a review by June 2022 of the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017.[195] The Treasury has begun that process, publishing a *Call for Evidence: Review of the UK's AML/CFT regulatory and supervisory regime* in July 2021.[196]

153. **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.**

154. ***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***

189 Q208
190 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime – Anti-money laundering supervision and sanctions implementation, 8 March 2019, para 163
191 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime – Anti-money laundering supervision and sanctions implementation, 8 March 2019, page 13
192 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime – Anti-money laundering supervision and sanctions implementation, 8 March 2019, para 111
193 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime – Anti-money laundering supervision and sanctions implementation, 8 March 2019, para 113
194 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 10
195 This is required by The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, (SI 2017/1301). regulation 32
196 HM Treasury, Call for Evidence: Review of the UK's AML/CFT regulatory and supervisory regime, July 2021

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.

155. ***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.***

HMRC as a supervisor

156. HMRC is an anti-money laundering supervisor of firms which are not supervised by the FCA or Gambling Commission and are not covered by the professional body supervision of OPBAS. It currently supervises over 30,000 businesses in nine sectors.[197]

157. Our predecessor Committee recommended that the Treasury should consider whether HMRC should lose its anti-money laundering (AML) supervisory functions. This proposal was prompted in part by comments by Sir Jonathan Thompson, who was at that time Chief Executive Officer at HMRC, when he suggested that a transfer of responsibility should be considered as part of the 2019 Spending Review discussion.[198] HMRC has not presented similar evidence to this inquiry. The Government response to the report did not imply that any change in responsibilities was under discussion.[199]

158. In the Economic Crime Plan 2019–22, HMRC committed to delivering an enhanced risk-based approach to its supervision by March 2021 and to carrying out an annual self-assessment of its money laundering supervision.[200] The latest self-assessment was published on 17 March 2021. This found "that HMRC's performance overall is currently broadly in line with both the relevant Money Laundering Regulations and with OPBAS' Sourcebook advice on best practice".[201]

159. We asked Simon York, Director of the Fraud Investigation Service, HM Revenue & Customs, whether having HMRC do a self-assessment meant it was "marking its own homework". He said:

> No, not at all. This was a commitment that we made as part of the Government's Economic Crime Plan that we would work to the standards set by OPBAS and, as part of that, carry out a self-assessment each year to check that. We carried out the first one of those and involved OPBAS in that

197 HMRC, HMRC Anti-Money Laundering Supervision annual assessment, para 1.12. Also listed there are the sectors involved and in Annex A numbers of registered businesses by year and sector.

198 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime - Anti-money laundering supervision and sanctions implementation, 8 March 2019, the comments of Sir john Thompson are reported at para 104, the recommendation para 106

199 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 9

200 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, Action 35, page 50

201 HMRC Anti-Money Laundering Supervision annual assessment

> process, and the Treasury signed off the final document. It was a thorough investigation. I have read through the whole thing and it was conducted by someone independent from this area of business within HMRC.[202]

160. HMRC's self-assessment also shows a big jump in penalties for money service businesses in 2019–20, leaping from £384,000 in 2018–19 to £7.8 million in 2019–20. Giving oral evidence on 8 July 2021, Helena Wood, Associate Fellow, RUSI Centre for Financial Crime and Security Studies, praised HMRC in this regard:

> "They [HMRC] have certainly shown what they are capable of in the past two years under their re-formed strategy for AML supervision. They have done some great work around money service businesses, for example."[203]

161. HMRC supervises Trust or Company Service Providers (TCSPs), which present the risk that they are used by criminals to set up companies and trusts to launder money. The Treasury and the Home Office, which jointly produced the *National risk assessment of money laundering and terrorist financing 2020*, point to the risks around TCSPs. Explaining what they are and why they present problems, the assessment said:

> TCSPs can be exploited, either wittingly or unwittingly, to enable the laundering of significant illicit flows through companies, partnerships and trusts. They often offer services which can enhance the attractiveness of companies and partnerships to criminals, for example increasing anonymity or creating complex structures.
>
> […]
>
> Although UK companies and partnerships can be set-up directly with Companies House with comparative ease and low cost, approximately half of corporate entities are still established through TCSPs. TCSPs offer a convenient method to establish a company for legal purposes, but many of their services can be exploited by criminals, including the use of nominee directorships, UK mail forwarding services and providing a registration address for hundreds of companies at single addresses. This is particularly attractive for those establishing a UK company from overseas, since the company must have a UK registered office to serve as its official address but is not required to operate in the UK or have a UK bank account.[204]

162. However, Helena Wood had concerns about supervision of TCSPs:

> […] I would really like to see [HMRC] apply that new model [HMRCs reformed strategy for AML supervision] to the trust and company service provider system, which I have publicly called the wild west. It has been so under-regulated and under-supervised that we frequently see these company factories emerging, where you have individuals at certain addresses registered to hundreds of companies. There is a lot there that HMRC could do to use them as the first line of defence in that system.[205]

202 Q141
203 Q240
204 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing 2020, December 2020, paras 11.14- 11.15
205 Q240

163. Graeme Biggar, Director-General at the National Economic Crime Centre, expressed concern about the low numbers of SARs from TCSPs. He told us:

> Trust and company service providers can take many forms, but the ones that tend to be more high-risk are those that do not fit under another body and are therefore supervised by HMRC. We see them crop up repeatedly in our investigations, […] yet the numbers of SARs that we have had from trust and company service providers last year was 31. We measure all the other numbers in thousands, but there were literally 31 SARs from trust and company service providers.[206]

164. When asked what was being done about this, Mr Biggar said:

> We did an intelligence assessment last year—it is now just under a year ago—to look into trust and company service providers. We are developing a plan with HMRC and the Treasury to have both more supervision of, and more enforcement against, company formation agents. We are on it, but it is not the most developed of our plans. We have really got to do more work on that.[207]

165. Written evidence to the inquiry from investigative journalists Richard Brooks and Simon Bowers was also critical of HMRC's role in respect of TCSPs. Their evidence centred on the FinCEN files, which showed substantial abuse of UK companies for money laundering purposes, and they noted difficulties with HMRC's enforcement in this field. They gave two interesting examples:

- one 24-year-old setting up multiple limited liability partnerships (LLPs) and limited partnerships (LPs) from his flat in North London on the instructions of a lawyer in Latvia. Many of the shell entities he created went on to open bank accounts at the notorious Estonian branch of Danske Bank[208] and to appear in the FinCEN Files.

- nine LLPs that had together failed to report $4.1 billion of income in annual accounts submitted to Companies House. When [Brooks and Bowers] spoke to the Belgian-based dentist whose name and signature was on these accounts, he insisted he knew nothing of them and his signature had been forged. When [they] approached HMRC with this information, officials said the evidence [they] had gathered pointed to a case of false accounting, which was not a matter for HMRC.[209]

166. ***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.***

206 Q63
207 Q93
208 The Danske Bank Estonian Branch was investigated for money laundering in 2017. This found a series of major deficiencies in the bank´s governance and control systems which made it possible to use Danske Bank's branch in Estonia for suspicious transactions. A criminal investigation is still ongoing. See Reuters, 'Danish prosecutors drop money laundering charges against former Danske Bank CEO' 29 April 2021, [extracted 10 January 2022]
209 Richard Brooks, Private Eye magazine, and Simon Bowers (ECC0067) para 24

167. **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.

168. ***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.***

Financial Action Task Force

169. The Financial Action Task Force (FATF) was established in 1989.[210] The UK is a founding member and strong supporter of FATF, which sets global anti-money laundering and counter-terrorist financing ("AML"/ "CTF") standards. These standards, as outlined in the FATF Recommendations and Methodology, were generally incorporated into UK law through the transposition of EU directives.[211]

170. The FATF publishes evaluations of regimes in different countries. Its most recent evaluation of the UK AML regime was in 2018. The Government points out in the Economic Crime Plan that:

> The UK's AML/CTF regime was evaluated in 2018 by the Financial Action Task Force's (FATF) mutual evaluation report (MER). Altogether, the findings of the MER showed that the UK has the strongest overall AML/CTF regime of over 60 countries assessed to date. In particular, the MER praised the UK's understanding of risk, response to terrorist financing and our targeted financial sanctions regime.[212]

171. Duncan Hames, Director of Policy, Transparency International UK, was concerned that the FATF evaluation measured legislation and not implementation. He said:

> The response has to be commensurate with the scale of the problem. Treasury officials and Ministers will be proud to tell you that the UK's evaluation by the Financial Action Task Force is world leading. It largely measures whether the policy is right, and many of their criticisms are about how we are not deploying the solutions that we have available at a scale necessary to have the right effect. …[213]

172. **The UK is a world-leading financial centre and needs an extensive legislative and regulatory regime to protect its financial system from money laundering. But it also needs enforcement and to ensure compliance with legislation. It is not obvious that**

210 See FATF, History of the FATF, [extracted 3 January 2021]

211 See Explanatory memorandum to the money laundering and terrorist financing (amendment) (eu exit) regulations 2020 (SI 2020/991) para 7.2

212 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, para 1.34

213 Q205

either regulation or enforcement systems are robust enough or up to the job required of them. While the latest evaluation by the Financial Action Task Force of the UK's anti-money laundering and counter-terrorist financing regime is positive, the Government should not be complacent. The FATF evaluation finds room for improvement in enforcement and compliance, and there is still much that the Government needs to do to make it more difficult to launder money in the UK. The latest FATF report is over three years old. In that time money laundering undertaken in the UK has not gone away: it has grown. The response to this threat seems slow and inadequate given the scale of the threats it poses.

The FCA's enforcement of AML and the NatWest prosecution

173. The Financial Conduct Authority is one of the three statutory anti-money laundering supervisors.[214] The Financial Conduct Authority has stated in its business plan for 2021/22 that it will be more assertive, testing the limits of its powers and engaging with partners to make sure they bring their powers to bear.[215] While this intention was expressed in general terms, it is clearly relevant to the FCA's anti-money laundering role.

174. Commenting on enforcement of the Money Laundering Regulations on banks, Mark Steward told us:

> We have a very significant programme to tackle a lack of money laundering systems and controls by firms that we regulate. Some of the largest fines that we have imposed have been against banks for systems and controls failures.[216]

175. On 16 March 2021 the FCA announced that it had begun criminal proceedings against NatWest for breach of money laundering regulations.[217] This was the first criminal prosecution by the FCA under money laundering regulations that have been in place since 2007. On 7 October 2021 the FCA announced that NatWest had pleaded guilty[218] and had been convicted of the offences. Sentencing took place on 13 December 2021, and NatWest was fined £268.4 million.

176. The offences related to NatWest's failure to deal with money laundering by a customer, Fowler Oldfield, which had been depositing large amounts of cash into the Bradford branch of NatWest. The Fowler Oldfield raid took place in 2016, so it was some five years after that raid that the FCA succeeded in its prosecution.[219] We wrote to the FCA about this apparent delay, and they provided a full reply on 13 December.[220] The FCA explained that it had begun its investigations in 2017 and that its work had required extensive analysis

214 HM Treasury, Anti-money laundering and counterterrorist financing: Supervision Report 2019–20, November 2021, p37

215 Financial Conduct Authority, Business Plan 2021/22, page 4. See also Financial Conduct Authority, Highlights of the FCA's new approach in 2021, 31 December 2021, [Extracted 31 December 2021]

216 Q118

217 Financial Conduct Authority, FCA starts criminal proceedings against NatWest Plc, 16 March 2021 [Extracted 29 December 2021]

218 Financial Conduct Authority, NatWest Plc pleads guilty in criminal proceedings, 7 October 2021, [extracted 29 December 2021]

219 Bradford Telegraph and Argus, 12 people were arrested from Fowler Oldfield in Hall Lane, with three men held on suspicion of money laundering, 9 September 2016 [Extracted 29 December 2021]

220 Letter from Nikhil Rathi to Chair of Treasury Committee, Prosecution of NatWest Bank for failures to comply with the Money Laundering Regulations 2007, 13 December 2021

of NatWest's anti money-laundering systems and controls over the duration of the bank's relationship with Fowler Oldfield, a period of nearly six years. In response to our question about why the FCA had chosen to prosecute, Nikhil Rathi (Chief Executive at the FCA) said:

> The FCA's decision to pursue a criminal prosecution rather than a civil or regulatory outcome in this case was made in light of all the evidence, including NatWest's August 2020 statement in response to the FCA's cautioned interview questions. The decision was made applying both the evidential and public interest tests in the Code for Crown Prosecutors. In this case, the evidence demonstrated particularly egregious failures and there were compelling public interest factors, including the public interest in banks complying with obligations under the Money Laundering Regulations.[221]

177. In response to our question about why no individuals at NatWest were prosecuted, he explained:

> The role of individuals was carefully considered throughout the investigation. However, there was insufficient evidence to establish individual liability given the distribution and allocation of system knowledge and responsibilities for AML functions to support a case against any officer. As well, most of the conduct in issue in the case predated the commencement of the Senior Managers & Certification Regime (which applied to NatWest from 7 March 2016).[222]

178. The NatWest prosecution follows a fine of £102.2 million in 2019 imposed on Standard Chartered Bank for poor AML controls,[223] and a £63.9 million fine imposed on HSBC for money laundering offences, announced on 17 December 2021.[224]

179. **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.**

De-risking

180. "De-risking", in the context of economic crime, is a term used when a financial institution either ends a customer relationship because it deems that that customer poses too high a risk of economic crime, or refuses access to banking services for similar reasons.

221 Ibid
222 Ibid
223 Financial Conduct Authority, FCA fines Standard Chartered Bank £102.2 million for poor AML controls, 9 April 2019 [extracted 29 December 2021]
224 Financial Conduct Authority, Decision Notice, HSBC Bank PLC, 14 December 2021

181. The former Treasury Committee's Report, *Economic Crime: Consumer view*[225] (published on 1 November 2019) expressed concern that freezing accounts and de-risking had become too widespread and was having a detrimental effect on innocent businesses and consumers.

182. The Report recommended that there should be greater transparency by banks about de-risking decisions.[226] It also called upon the FCA and the Financial Ombudsman Service to ensure that all instances when banks and customers had not agreed about de-risking decisions were fully investigated, and that banking services were restored as quickly as possible and appropriate.[227] The then Committee also called for banks to be careful to prevent bias in their use of artificial intelligence systems used to make de-risking decisions.[228]

183. In its response, the Government said:

> Where individuals or businesses are de-banked, it is important that they understand why they have been de-banked, and the FCA is working with financial institutions to help improve communications, including through a set of principles on how de-banking decisions should be made. Following the implementation of the Payment Services Regulations (2017), banks seeking to withdraw account services from payment services providers must submit an application to the FCA and PSR, who will assess these against criteria of being proportionate, objective and non-discriminatory. The Government is further working to ensure de-risking does not create issues in the remittances sector by taking forward recommendations of the G20 taskforce on remittances, and working with stakeholders to ensure this can be done in a way that allows legitimate risks to be countered by financial institutions.[229]

184. Following press reports in 2021,[230] our Chair wrote to Nikhil Rathi, Chief Executive at the Financial Conduct Authority, asking what progress the FCA had made with the recommendations on de-risking in the previous Committee's report.[231] In his reply, Mr Rathi said that the FCA was "not aware of a substantive cross-sector issue of banks freezing accounts for no reason". He added that:

> … the FCA continues to supervise bank's compliance with Regulation 105 of the Payment Services Regulations 2017, which requires banks to provide payment service providers access to payment accounts on a proportionate, objective and non-discriminatory basis. We want firms to take decisions on a case-by-case basis rather than a blanket approach.[232]

225 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246
226 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246, para 76
227 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246, para 77
228 Treasury Committee, Third Report of Session 2019, Economic Crime: Consumer view HC 246, para 78
229 Treasury Committee, Second Special Report of Session 2019–21, Economic Crime: Consumer View: Government and Regulators' Responses to Committee's Third Report of Session 2019, 13 March 2020, HC 91, page 7
230 The Sunday Times, "The great bank account shutdown", 18 July 2021.
231 Letter to the Chief Executive of the Financial Conduct Authority related to frozen bank accounts, dated 22 July 2021
232 Letter from the Chief Executive of the Financial Conduct Authority relating to Derisking - 29 July 2021

185. Mr Rathi's reply also drew our attention to a report commissioned by the FCA from the Alan Turing Institute, about the responsible use of Artificial Intelligence (AI) in the context of financial services,[233] and a forum that the FCA had established with the Bank of England to better understand the use and impact of AI in financial services.[234]

186. ***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.***

233 The Alan Turing Institute, AI in Financial Services, 14 June 2021

234 Financial Conduct Authority Artificial Intelligence Public-Private Forum, extracted 21 December 2021

6 Cryptoassets and economic crime

Background to cryptocurrencies and cryptoassets

187. 'Cryptocurrencies' are a digital means of financial exchange, and all use distributed ledger technology to verify transactions.[235] Well known examples include Bitcoin and Ethereum. Recent years have seen an increase in cryptocurrency transactions and a proliferation of new cryptocurrencies. Cryptocurrencies are often described as assets, or "cryptoassets", and this has been adopted as a term by the Bank of England and FCA. It is also how they were described by the former Treasury Committee in its report "*Crypto-assets*", published in September 2018.[236]

188. As a relatively new financial phenomenon, cryptoassets are largely outside existing regulatory frameworks, but they have attracted the attention of regulators around the world.[237] In the UK, cryptoassets are a type of financial asset which largely sit outside the "perimeter", which is a term used to refer to the scope of FCA powers.[238] The FCA has warned about the potential harms for consumers and markets from cryptoassets whilst acknowledging that cryptoassets and their underlying technology may offer potential benefits for financial services.[239] It warns that consumers who invest in these assets should be prepared to lose all their money and that they will not be protected from losses, due to the unregulated nature of the products and services. The regulation of cryptoassets is outside the scope of this inquiry but is, at the time that this Report was published, the subject of a Treasury-led consultation.[240]

189. Cryptoassets are increasingly being used for economic crime and fraud. The potential for fraud is highlighted by a campaign led by UK Finance—Take Five to Stop Fraud—which provides the following consumer fraud warning about cryptoassets on its website:

> Cryptocurrencies are known for their market volatility, so the value of investor's assets go up and down quickly. Criminals have taken advantage of the unregulated nature of cryptocurrencies to scam consumers.
>
> Criminals advertise schemes promising, in some cases, high returns through cryptocurrency investing or mining. These adverts may look official, include celebrity endorsements or personal testimonies. Often the celebrities may not even know their name or photograph has been used.[241]

190. Giving evidence to our inquiry on the Future of Financial Services on 25 October 2021, John Collins, Chief Legal and Regulatory Officer, Santander UK, said:

235 Cryptocurrencies: Bitcoin and other exchange tokens, House of Commons Library Briefing Paper no. 8780, 19 February 2020

236 Treasury Committee, Crypto-assets, 19 September 2018, HC 910 2017–19, para 5

237 For example, see Financial Times, "US regulators signal bigger role in cryptocurrencies market". 30 May 2021

238 Part of the legal basis for the "perimeter" is the Financial Services and Markets Act 2000, which defines regulated activities in section 22(1) to be "an investment of a specified kind". Specified investments are specified in regulations made by Treasury. This was extended by Financial Services Act 2021, section 7 which amended section 22. Cryptoassets are regulated for anti-money laundering purposes.

239 See for example Financial Conduct Authority Perimeter Report 2020/21 21 October 2021 page 32

240 HM Treasury, UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence, 7 January 2021

241 Take Five To Stop Fraud, Cryptocurrency scam, accessed 21 December 2021

> … Putting aside the scams that are criminals pretending to be crypto, within the system the most obvious stat that I can call upon is that the DCPCU [Dedicated Card and Payment Crime Unit], which is the cards unit that the industry works with the police on, has found a very high—as in plus-80%—level of criminals arrested with crypto wallets on their phones. They are using them as part of the mechanism to layer, disguise and then cash out, and it is a very significant problem at the moment. Cryptoassets are a risk for economic crime partly because they are not well regulated and sit outside the perimeter.[242]

191. In evidence to this inquiry on 14 June 2021, Mark Steward, Director of Enforcement, Financial Conduct Authority, while discussing money laundering, told us that " … the area that is most acute now is the crypto world … ".[243]

192. Banks appear increasingly worried about the risks to consumers from cryptoassets, and about the warnings from the FCA.[244] For example, HSBC does not process cryptocurrency payments or allow customers to bank money from digital wallets.[245] Lloyds does not allow purchase of crypto currencies using credit cards.[246] TSB does not "facilitate transactions to cryptocurrency exchanges".[247]

Cryptoassets and advertising

193. Recently there has been an increasing number of advertisements for cryptoassets. Such adverts have become common on the London Underground.[248] The Advertising Standards Authority has recently stopped various cryptoasset advertisements and has issued a public statement about the work they are doing to protect consumers from misleading advertisements for cryptoassets.[249]

194. On 18 January 2022, HM Treasury announced that the Government would legislate to address misleading cryptoasset promotions, and to bring into line advertising of cryptoassets with that of other financial services and products.[250] On 19 January the FCA announced a consultation on strengthening financial promotion rules for high risk investments, including cryptoassets.[251]

195. **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.**

242 Treasury Committee, Oral evidence taken on 25 October 2021, HC (2021–22) 147, Q298 [John Collins]
243 Q149
244 For an overview, see Which?, Banks ban crypto payments over fraud spike. [Extracted 29 December 2021]
245 The Times, "Bitcoin holders barred from depositing profits in UK banks" 9 January 2021
246 The Guardian, "Lloyds Bank bans customers from buying bitcoins using credit cards"5 February 2018
247 TSB, Fraud Prevention Centre, [extracted 29 December 2021]
248 BBC news, "Crypto adverts on London Tube under investigation" 18 November 2021
249 Advertising Standards Authority , "ASA statement on crypto-assets", 23 November 2021
250 HM Treasury, "Government to strengthen rules on misleading cryptocurrency adverts", 18 January 2022
251 Financial Conduct Authority, "CP22/2: Strengthening our financial promotion rules for high risk investments, including cryptoassets", 19 January 2022

196. ***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.***

Regulation of cryptoassets for money laundering

197. Criminals use cryptoassets to launder money, and press reports have indicated that new forms of cryptoassets (such as Monero) can be particularly attractive because they are designed to be untraceable.[252] Once acquired, cryptoassets can easily be exchanged, and the original source obscured. On 25 June 2021, the Evening Standard reported that detectives investigating money laundering had seized crypto-currency worth £114 million.[253]

198. International bodies such as the Financial Action Task Force[254] and the International Monetary Fund[255] have consistently highlighted the money laundering risks of cryptoassets. As the National Crime Agency notes in its *National Strategic Assessment of Serious and Organised Crime 2020*:

> Trends identified in 2018 have become more prevalent during 2019, including the increased criminal use of encryption tools, the dark web and virtual assets, which refers to technologies such as Blockchain, Bitcoin, crypto assets and virtual currencies.[256]

In relation to money laundering specifically, the NCA notes that "UK-based criminals continue to identify new ways of using virtual assets, such as cryptocurrencies, to launder their profits, although more traditional methods are still favoured."[257]

199. Money laundering and terrorist financing risks associated with crypto-assets were addressed by our predecessor Committee in a report in 2018 on Crypto-assets.[258] It concluded that, due to lack of regulation (at that time) and anonymity, cryptoassets could be used for money laundering purposes. Noting the adoption of cryptoassets by the EU in the Fifth Anti-Money Laundering Directive, meaning that cryptoasset exchanges would have to comply with anti-money laundering and counter-terrorist financing rules, the then Committee urged the Government to bring the directive into UK law as a priority. The Government met this recommendation with the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.[259]

200. The Economic Crime Plan does not include measures to cover consumer protection from fraud specifically relating to cryptoassets, but it does set out the Government's intention that the FCA should become the supervisor of cryptoassets for anti-money

252 Financial Times " Monero emerges as crypto of choice for cybercriminals", 22 June 2021.
253 Evening Standard "Detectives investigating money laundering seize crypto-currency worth £114 million", 25 June 2021
254 Financial Action Task Force, 'Money laundering risks from "stablecoins" and other emerging assets', 18 October 2019
255 IMF, FinTech Note 19/03, Regulation of Crypto Assets,10 January 2020, pages 3 and 4
256 National Crime Agency, National Strategic Assessment of Serious and Organised Crime 2020, para 29
257 National Crime Agency, National Strategic Assessment of Serious and Organised Crime 2020, para 168
258 Treasury Committee, Twenty-Second report of Session 2017–19, Crypto Assets, HC 910, para 90- 106
259 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, (SI 2019/1511)

laundering (AML) purposes, from January 2020.[260] Regulations to establish the FCA as the supervisor came into effect on 10 January 2020[261] and required cryptoasset businesses to comply with AML laws and register with the FCA. In order to allow consideration of applications, the FCA permitted applicants temporary registration until 9 July 2021. On 3 June 2021 the FCA announced that it was extending the temporary registration scheme for existing cryptoasset businesses from 9 July 2021 to 31 March 2022 (while it worked through a backlog of registration applications). It also said:

> A significantly high number of businesses are not meeting the required standards under the Money Laundering Regulations. This has resulted in an unprecedented number of businesses withdrawing their applications.[262]

201. Registration of cryptoasset firms for money laundering has been slow. The FCA stated in its *Perimeter Report* on 21 October 2021 that 12 firms have been registered and that 90% of firms assessed had withdrawn their applications for registration.[263] This adds to existing concerns that cryptoassets are being used for money laundering and other financial crime. Nikhil Rathi, Chief Executive of the FCA, said in oral evidence on 8 December 2021:

> … we see a serious link to money laundering and serious organised crime being propagated through crypto exchanges and a culture in many of those organisations that does not respond to the level of systems and controls we would need from those firms as they are growing. We have allowed 17 through, but it has been a very challenging set of conversations. That is consistent with the posture we are adopting in the gateway.[264] […]

202. Notwithstanding the requirement to register for AML purposes, the FCA also publishes a list of companies which appear to be trading in cryptoassets but which are unregistered in the UK for anti-money laundering.[265] There are over 200 companies on the unregistered list.[266] It is unclear what sanction if any these companies face, and it is likely that trading with these firms is more attractive for criminals. We asked Nikhil Rathi, Chief Executive of the FCA, whether this list was helpful to criminals. He told us that "The purpose of it is to make sure consumers who look at our website recognise that they should be very cautious about interacting with those firms …". However, he acknowledged that:

> … it could be used by criminals who are also entrepreneurial. With other law enforcement agencies, we clearly need to work hard to clamp down on that kind of behaviour. Our priority is to make sure consumers know they should not be investing with those firms, because those firms may be making improper claims about their status.[267]

260 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, see action 37
261 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, (SI 2019/1511), regulation 1
262 Financial Conduct Authority, 'Temporary Registration Regime extended for cryptoasset businesses', 3 June 2021 [Extracted 3 January 2022]
263 Financial Conduct Authority Perimeter Report 2020/21 21 October 2021 page 33
264 Oral evidence taken on 8 December 2021 by the Treasury Committee on the work of the Financial Conduct Authority, Q231 [Nikhil Rathi]
265 Financial Conduct Authority, 'Unregistered Cryptoasset Businesses', [Extracted 4 January 2022]
266 See The Sunday Times, "Why are there now so many bitcoin trading firms?", 9 January 2022
267 Oral evidence taken on 8 December 2021 by the Treasury Committee on the work of the Financial Conduct Authority, Q252 [Nikhil Rathi]

203. **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.**

204. ***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.***

205. ***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.***

7 Companies and economic crime

Companies and criminal liability

206. The report of the previous Treasury Committee, *Economic Crime - Anti-money laundering supervision and sanctions implementation,* set out problems with the corporate criminal liability framework which hinder work to combat economic crime, as illustrated by evidence provided to that inquiry by (amongst others) the Serious Fraud Office (SFO).[268] A key problem is the "identification principle"—a legal principle which provides that a company can only be made criminally liable by establishing that a person who was the "directing mind and will" of the company at the relevant time carried out the acts and had the necessary mental state. In practice this makes it difficult to land a prosecution of a company of any size for some types of economic crime.[269] The SFO also called for the introduction of a new offence of failing to prevent economic crime.[270]

207. The Ministry of Justice launched a call for evidence on *Corporate Liability for Economic Crime* on 13 January 2017.[271] In the former Treasury Committee's Report, *Economic Crime - Anti-money laundering supervision and sanctions implementation*,[272] the then Committee noted that at that time there had been no response from the Government following the Ministry of Justice's call for evidence, and it recommended:

> […] that the Government responds to the evidence submitted in response to the 2017 *Corporate liability for economic crime: call for evidence* and undertake further consultation on proposals for legislation by the next Queen's Speech.[273]

The Government responded that "analysis of the responses to this call for evidence has concluded, and the MoJ will respond shortly".[274]

208. On 3 November 2020, the Government published its response to the MoJ's 2017 consultation.[275] It concluded that it "was not persuaded that a sufficient evidence base had been provided on which to make immediate legislative change to the criminal law in relation to economic crime."[276] Instead of bringing forward changes in the law to introduce a "corporate failure to prevent" offence at that point, the Government therefore decided that:

268 Treasury Committee, Twenty-seventh Report of Session 2017–2019, Economic Crime - Anti-money laundering supervision and sanctions implementation, HC 2010, see Chapter 4, page 54
269 Ibid, para 185
270 Ibid, para 188
271 Ministry of Justice, Corporate Liability for Economic Crime, 13 January 2017
272 Treasury Committee, Twenty-seventh Report of Session 2017–2019, Economic Crime - Anti-money laundering supervision and sanctions implementation, HC 2010
273 Treasury Committee, Twenty-seventh Report of Session 2017–2019, Economic Crime - Anti-money laundering supervision and sanctions implementation, HC 2010, para 202
274 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 15
275 Ministry of Justice Corporate Liability for Economic Crime Call for Evidence: Government Response
276 Ibid, Para 62

> … because of the highly complex nature of the laws concerned and the implications of any future change, the Government is commissioning the Law Commission to undertake a detailed review of the identification doctrine, with a particular focus on economic crime.[277]

209. The Law Commission published a discussion paper, *Corporate Criminal Liability,* on 9 June 2021.[278] The terms of reference for its project are for it to decide whether the identification principle is fit for purpose and how to improve the criminal and civil law on corporate liability.[279] The Law Commission has not yet concluded its work.

210. We asked David Clarke, Chair of the Fraud Advisory Panel, what changes in the law he wanted to see in this area.

> I would like to see a "failure to prevent" offence that really puts the focus on companies. It is difficult. We have had long discussions about this. It has been discussed at some length. The Law Commission is looking at it. It would also help here with the fraud side, so we would like to see that failure to prevent offence.

211. **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.**

Company registration and use of UK companies by economic criminals

212. The UK is home to a large, highly regulated financial sector, which benefits from a low corruption environment. Moving money through UK companies is likely to attract much less suspicion than directly using companies in secrecy havens. It is therefore attractive to sophisticated money laundering operations. Written evidence to the inquiry from Transparency International UK indicates the scale of the problem. They said:

> We have identified 929 UK companies involved in 89 cases of corruption and money laundering, amounting to £137 billion in economic damage.[280]

213. Duncan Hames, Director of Policy at Transparency International UK, spoke in evidence about the scale of the problem with UK companies and of the importance of cleaning up the UK company register. He said:

277 Ibid, para 71
278 Law Commission, Corporate Criminal Liability A discussion paper, 9 June 2021
279 Law Commission Corporate Criminal Liability [extracted 29 December 2021]
280 Transparency International UK, (ECC0051), para 14.

> … UK companies are a global problem. UK companies were connected with transactions relating to the ammonium nitrate explosion in Beirut. UK shell companies were connected with sanctions-busting arms deals in Sudan. UK companies were involved again in the Moldovan bank robbery that took an eighth of the country's GDP in an industrial-scale fraud, so this is not even just about what happens here. There are victims right around the world, and the imposition of a rules-based system on all sorts of important security considerations right around the world is undermined because of the ability to use UK companies to get around important rules that are there to protect all of us.[281]

214. In September 2020, the "FinCEN files" were leaked to the media.[282] FinCEN is the acronym for the Finance Crimes Enforcement Network, which is a unit of the US Treasury responsible for receiving suspicious activity reports under anti-money laundering laws in the USA. The leak was of over 2,100 suspicious activity reports (SARs) sent by banks in the USA or overseas banks with US branches under US money laundering regulations between 2009 and 2017.

215. Graeme Biggar, Director-General at the National Economic Crime Centre, told us about the extent of the abuse of UK company structures for money laundering. He said:

> … we are one of the biggest financial centres in the world, we know that we have prided ourselves as a country on the ease of doing business here and of setting up companies, and I think we also know that, as a result of that, it can be too easy to set up companies here, as we have seen repeatedly over the years. We have done some analysis recently on some of the laundromats that have come out of Russia and the former Soviet Union, and a disturbing proportion of the money that comes out of those laundromats—not much shy of 50% in one case—were laundered through UK corporate structures.
>
> That is not through the UK or UK financial institutions—some of the money will never have touched the UK—but corporate structures that have been set up through UK systems."[283]

216. As cited at paragraph 165 above we received evidence from investigative journalists Simon Bowers and Richard Brooks about the FinCen files.[284] Their evidence provides insight into the potential scale of the problem. In their view, the FinCEN files show that UK anonymous shell companies were involved in suspicious transactions linked to criminal activity and money laundering. They also set out what they see as the common characteristics of these shell companies, including use of nominee owners who are based in secrecy havens such as the Seychelles, Nevis, the Marshall Islands, Belize, Dominica and Panama. These nominee companies were fronts for the real owners who remained hidden. When the UK companies or LLPs were registered, paperwork was signed by a "straw man" with no knowledge of the true affairs. Addresses given were mailboxes.

281 Q205
282 BBC News FinCEN Files: All you need to know about the documents leak, 21 September 2020 accessed 21 December 20201
283 Q8
284 Richard Brooks , Private Eye Magazine, and Simon Bowers [ECC0067]

Their evidence also suggests that particular company formation agents were involved in suspicious companies and were being used to facilitate the company formations in the most obscure way possible.

217. The FinCEN files also highlighted the continued use of Scottish Limited Partnerships (SLPs) to move dubious funds. Other recent investigations have highlighted how criminal money from abroad has passed through the accounts of SLPs. SLPs are a form of LLPs which have their own distinct legal personality. This means that a company can hold assets and enter into contracts in its own right, obscuring the identities of those running it behind the veil of incorporation.

218. The abuse of UK company structures is not new. In 2014 the Government's UK Anti-Corruption Plan noted that "numerous studies have identified the role of company misuse through hidden ownership in facilitating money laundering and corrupt activity."[285] In order to show who controls companies, the Government introduced provisions to establish a register of company beneficial ownership in the Small Business, Enterprise & Employment Act 2015. The register launched in 2016 and is known as the People with Significant Control (PSC) register.[286] The Government said it was the first such register in the G20.[287]

219. The previous Committee's report, *Economic Crime – Anti-money laundering supervision and sanctions implementation*, published in 2019,[288] covered the problems of company ownership and identified weaknesses in Companies House processes.[289] The Government responded by promising a consultation.[290] In May 2019 the Department of Business, Energy & Industrial Strategy launched its consultation *Corporate Transparency and Register Reform,* which it described as a "consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities".[291] The consultation noted that there were still problems which the introduction of the People with Significant Control register had not solved. Issues included:

- Misuse of UK registered entities by international criminals and corrupt elites
- The accuracy of information held at Companies House
- The abuse of personal information on the register
- The limited nature of cross checks between Companies House and other public and private sector bodies.[292]

220. The Government responded to this consultation on 18 September 2020 with a range of proposals. These include:

285 UK Government, UK Anti-Corruption Plan, December 2014, para 6.10
286 GOV.UK, 'People with Significant Control' Companies House register goes live, 30 June 2016
287 Alan Duncan (FCO), Sanctions and Anti-Money Laundering Bill [Lords] debate, 20 February 2018, Volume 636
288 Treasury Committee, Twenty-Seventh Report of Session 2017–19, Economic Crime – Anti-money laundering supervision and sanctions implementation, 8 March 2019
289 Ibid, para 63
290 Treasury Committee, Eleventh Special Report of Session 2017–19, Government Response to the Committee's Twenty-Eighth Report: Economic Crime—Anti-money laundering supervision and sanctions implementation, page 6
291 Department of Business, Energy & Industrial Strategy, Corporate Transparency and Register Reform May 2019
292 Ibid, pages 12–13

- Verifying identity for all directors and PSCs and those filing information about companies
- Imposing regulation on company formation agents
- Enhancing the powers of the registrar of Companies
- Reviewing exemptions for micro or dormant accounts
- Enhancing compliance and share intelligence to deter abuse of corporate entities.[293]

221. The next step was the launch of the following three further consultations by the Department for Business, Energy and Industrial Strategy on 9 December 2020:

- Increasing powers of the registrar[294]
- Improving the quality and value of financial information on the UK company register,[295] and
- Implementing the ban on corporate directors[296]

222. These three consultations closed on 3 February 2021, since when nothing more has been said by the Government, more than two years after the consultation process began.

223. Graeme Biggar attached great importance to the reform of Companies House, and he welcomed the commitments made by the Government in its response in September 2020 to the initial consultation. He said:

> … We put a very strong response into the consultation that the Government did on Companies House, and the Government's response to that was announced in September [2020]. It is a really good response. It does not cover absolutely everything that we asked for, but it was at the higher end of our expectations and was widely welcomed. What we would really like to see now is the legislation that will enable that being put to Parliament and the funding that will come with it to enable the reform being voted on. It was pleasing to see in the Spending Review £20 million for the reform of Companies House.[297]

224. The importance of these reforms was also stressed by Duncan Hames, Director of Policy at Transparency International UK, when giving oral evidence to the inquiry on 8 July 2021. He said:

293 For a full list of proposals see Department of Business, Energy & Industrial Strategy, Corporate Transparency and Register Reform Government response to the consultation 18 September 2020, page 8

294 Department of Business, Energy & Industrial Strategy and Companies House, Corporate transparency and register reform: powers of the registrar, 9 December 2020

295 Department of Business, Energy & Industrial Strategy and Companies House, Corporate transparency and register reform: improving the quality and value of financial information on the UK companies register, 9 December 2020

296 Department of Business, Energy & Industrial Strategy and Companies House, Corporate Transparency and Register Reform: Consultation on implementing the ban on corporate directors. 9 December 2020

297 Q8

> … We are soon going to be in a situation, with the publication of the Elections Bill this week, where you will require more evidence of your ID to vote in a parish council election than you do to set up a network of shell companies at Companies House. We need to address that deficit, because what you are capable of doing, if you want to be involved in money laundering with a network of companies at Companies House, potentially has very great impact indeed, and perhaps more so than my vote in the local elections.[298]

225. Giving oral evidence to the inquiry on 29 November 2021, John Glen MP, Economic Secretary to the Treasury, told us about the need to reform. He said:

> Clearly, what we want is a situation where we have as much transparency as possible, and we want to encourage, and make it straightforward for, people to set up businesses in this country. I think that is healthy. What we do not want is a situation where people are setting up companies without due checks on who is doing it and the propriety of that, and then those entities are used as vehicles for fraud. We have to interrogate the data around that, and you have probably heard representations around the gap that exists in the quality of the IT infrastructure supporting Companies House.[299]

226. The Government acknowledges that these reforms require not only changes to the law and powers but also transformation of Companies House's operations. The consultation response includes a chapter on the operational transformation of Companies House, which says "The transformation is not only necessary to deliver these reforms, but also to ensure Companies House can meet evolving customer demands, improve its service offer and meet increasing demand for its data."[300]

227. At the Autumn Budget and Spending Review on 27 October 2021, the Treasury announced that there would be £63 million over the Spending Review 2021 period (the three years ending on 31 March 2025) to support reform of Companies House.[301] This is out of a BEIS annual budget of between £19 billion and £23 billion up to 2025.[302]

228. We asked the Economic Secretary to the Treasury, John Glen MP, about the pace of reform at Companies House, when he gave oral evidence to the inquiry on 29 November 2021. He said "I sincerely want to see significant progress. That money has been allocated to speed up the process of Companies House reform."[303]

229. Another issue is whether the scope of the reforms is sufficient to stop limited partnerships, and Scottish Limited Partnerships in particular, being used to hide ownership. When asked whether the reforms were sufficient, Martin Swain, the Director for Strategy and Policy at Companies House, told us that " … it is more complicated for limited partnerships, and we are working through it at the moment."[304]

298 Q238
299 Q502
300 Department of Business, Energy & Industrial Strategy, Corporate Transparency and Register Reform Government response to the consultation 18 September 2020, page 71
301 HM Treasury Autumn Budget and Spending Review 2021, para 4.73
302 HM Treasury Autumn Budget and Spending Review 2021, table 4.11 page 112
303 Q466
304 Q145

230. **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.**

231. ***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.***

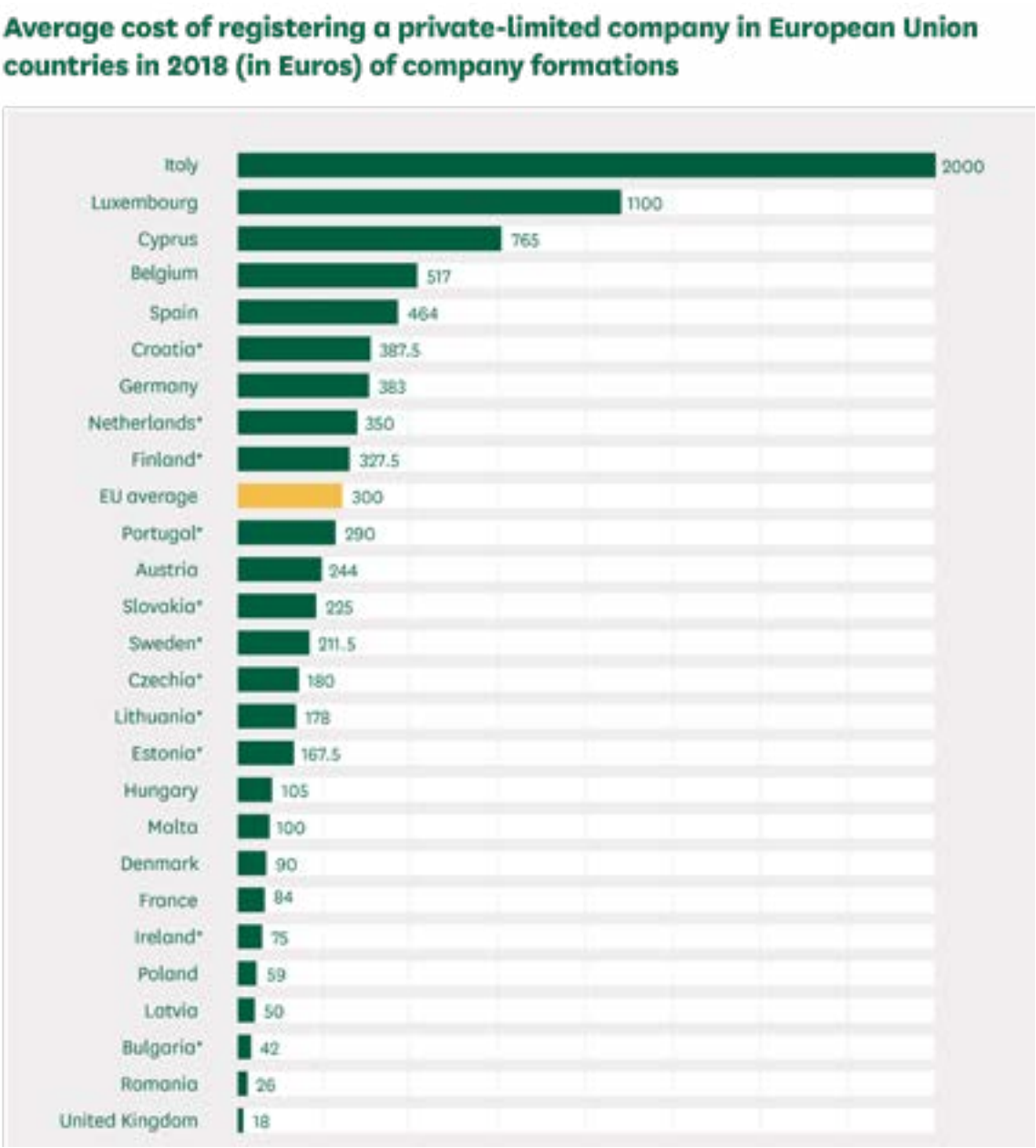
232. ***The Government should supply us with details of the project milestones for the Companies House transformation programme, together with an annual progress report.***

The cost of company formation and the funding of Companies House

233. The UK has one of the most attractive legal regimes in the world and is one of the most important financial centres. These factors make UK companies as attractive to criminals as they are to genuine financial services and enterprise. But the cost of company formation is very low by international standards (see Figure 4 below) and compared to other Government services. For example the cost of a passport is £75.50,[305] and an annual TV licence costs £159.[306] Yet the online cost of company incorporation online is £12 and, for a Limited Liability Partnership, £13.[307]

305 Passport Fees (Gov.UK) [Extracted 29 December 2021]
306 TV Licence (Gov.UK) [Extracted 29 December 2021]
307 Full details of fees are set out at Companies House Companies House fees (as of 23 November 2021)

Figure 4: Average cost of registering a private-limited company in European Union countries in 2018 (in Euros) of company formations



Source: European Commission [extracted 2 January 2022]

234. In the year to 31 March 2021, there were 810,316 company formations in the UK, a year-on-year increase of 21.8%, and the highest number of incorporations on record.[308] If an additional £50 had been paid by each of those companies last year to incorporate, it would have raised over £40 million, while an additional £100 per company would have raised over £80 million.

235. We asked Martin Swain, Director for Strategy and Policy, Companies House, about the cost of company formation. He explained how funding for Companies House works. He told us:

> … In terms of increasing the fee, it is probably worth the Committee being aware that we operate on a cost recovery basis. Legally, we can only recover the costs that we are directly creating for the customer. … the more efficient we become, the more digital we become and the more we drive down the cost. …
>
> I guess the question would be to what level you raise it where it becomes a disincentive for a criminal, be they a low-level criminal or someone involved in serious organised crime, to use the UK system for that abuse. I would not be able to put a figure on it. I would make the assumption that, if an organised criminal gang wanted to use a corporate entity for abuse, even if we had the same fee as some European registers, it would not disincentivise it that much.[309]

236. On the other hand, Helena Wood, Associate Fellow, RUSI Centre for Financial Crime and Security Studies said:

> By international standards, the fees we charge are jokingly low. We currently charge £12 and by way of comparison, if you look at our near neighbours, in France it is around £50. In Germany it is around £100. Our Commonwealth partners, such as Australia, charge about £200. The argument has gone that if we raise the fee it reduces our competitiveness. That is a joke. It really does not; £12 is a very low bar of entry into the UK's corporate system. What will we do with that money? It is desperately needed to fund the huge transformation in Companies House in order to make it a beating heart of intelligence on abuse of the corporate registry.[310]

237. **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.**

308 Companies House, (official statistics) Companies register activities: 2020 to 2021, 24 June 2021. Also Companies House, Annual Report and Accounts, 2020–21, page 9

309 Q112

310 Q210

238. ***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.***

Beneficial ownership of property and the Registration of Overseas Entities Bill

239. In the UK it is possible to own property without disclosing the real or beneficial owners, for example where the real owner uses a foreign company to hide their ownership. Ownership of companies, limited partnerships and limited liability partnerships can also be hidden. This may make the UK very attractive to those with large amounts of money to hide and to criminals and kleptocrats the world over.

240. According to an article in The Times on 12 November 2021, the number of properties in England and Wales owned by individuals based overseas has trebled since 2010. The article suggested that individuals based overseas own 247,000 properties, almost 1 per cent of all properties.[311] In March 2016, the then Department for Business, Innovation and Skills published a discussion paper on "Beneficial Ownership Transparency".[312] This was followed by an announcement on 12 May 2016 by the then Prime Minister David Cameron, at the London Anti-Corruption Summit, that the Government would introduce a register for owners of overseas companies that own or purchase UK property, or are involved in Government contracts.[313] The Government initially committed to introducing legislation on this register by April 2018.

241. In 2018 a Registration of Overseas Entities Bill was drafted and was subject to pre-legislative scrutiny by a Joint Committee of MPs and Lords Members, which reported on 20 May 2019.[314] The Government responded to the Joint Committee's report in July 2019[315] and committed to deliver the register in 2021. However, the Bill has still not been introduced. The Government included the commitment to transparency of beneficial ownership as Action 44 in its Economic Crime Plan 2019–22.[316]

242. In the meantime, the Pandora papers, which include 11.9 million leaked documents, were released to the media on 3 October 2021.[317] The papers appear to cast light on the underlying ownership of assets including high-value London properties, and the extent

311 The Times, 'Stop property being used for economic crime, demand MPs', 12 November 2021
312 Department for Business, Innovation & Skills, "Beneficial Ownership Transparency"
313 Gov.UK Press release 'PM hosts major summit as part of global drive to expose, punish and drive out corruption' [Extracted 29 December 2021]
314 Joint Committee on the Draft Registration of Overseas Entities Bill, report of Session 2017–19, Draft Registration of Overseas Entities Bill, (HL paper 358 HC 2009), 20 May 2019
315 Department for Business, Innovation & Skills, Draft Registration of Overseas Entities Bill: Government Response to Joint Committee Report 2019 July 2019. Following the response the Joint Committee Chair wrote to the Government, Letter Lord Edward Faulks QC to Kelly Tolhurst MP, 3 September 2019.
316 HM Government and UK Finance, Economic Crime Plan 2019–22, July 2019, action 44, page 57, "Enhance transparency of overseas ownership of UK property and reform limited partnerships"
317 The Guardian 'Pandora papers: biggest ever leak of offshore data exposes financial secrets of rich and powerful', 3 October 2021

to which wealthy overseas politicians and business figures have invested money in the UK and hidden their ownership using anonymous nominee companies set up in secrecy havens.

243. We were told that beneficial ownership of property was not the only area where more transparency was needed. Graeme Biggar, Director-General at the National Economic Crime Centre, told us in oral evidence that " … Trusts is the next area, and that is where we would like to open up more beneficial ownership information, too."[318]

244. Giving oral evidence on 8 July 2021, Duncan Hames, Director of Policy at Transparency International UK, was asked about the scale of the problem and about the Registration of Overseas Entities Bill. He said:

> Our research has identified about £5 billion worth of suspicious wealth that is stashed away in UK real estate. There are currently more than 95,000 properties in England and Wales owned by overseas companies. Of those, 85,000 are owned by companies registered in countries where the names of company owners are not published. This makes it very difficult to do proper due diligence and to protect against our property sector being used as a safe haven for the proceeds of crime and corruption. The measure that you described was the Government's flagship policy to respond to this, and it has cross party support, yet for some reason in Queen's Speech after Queen's Speech it is not making it into the legislative programme.[319]

245. When asked whether the enhanced information which would be derived from a register of beneficial ownership would be sufficient, Mr Hames pointed out that it needs to be backed with proper resourcing for the law enforcement:

> … It is quite a powerful deterrent if people can see what you are doing and that has reputational consequences for you. It increases the jeopardy and the risk that you are going to be in trouble with the law and, indeed, probably points to a greater probability of success for law enforcement… Yes, transparency would make a big difference. It needs to be backed up by proper resourcing for enforcement and action by the police.[320]

246. **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.**

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

318 Q84
319 Q206
320 Q207

Annex

Table 2: Organisations involved in combating economic crime

Organisation	Role in combatting economic crime
Crime fighting organisations	
National Crime Agency (NCA)	Financial intelligence unit for money laundering.
City of London Police	National Lead Force for Fraud
United Kingdom Financial Intelligence Unit	The UK Financial Intelligence Unit (UKFIU) is independently located within the National Economic Crime Command (NECC) as part of the NCA. The key function of the UKFIU is to receive, analyse and disseminate Suspicious Activity Reports (SARs) through the SARs regime.
Police Scotland	Responsible for fraud in Scotland
Serious Fraud Office	The SFO is a specialist prosecuting authority tackling the top level of serious or complex fraud, bribery and corruption
Serious Organised Crime Agency (SOCA)	Abolished 2013- merged into NCA
Local police forces in England and wales	Consumer fraud
Action Fraud	UK's national reporting centre for fraud and cybercrime, run by City of London Police (4 August 2021 govt announced it will be replaced)
National Fraud Intelligence Bureau (NFIB)	National Fraud Intelligence Bureau (NFIB) sits alongside Action Fraud. NFIB receives all Action Fraud's reports.
CAMIS	Fraud reporting database
Regulators	
Payment Systems Regulator (PSR)	Regulates payment services providers (banks) , responsible for faster payments, BACs, CHAPs (sits withing FCA)
Financial Conduct Authority	Responsible for regulating banks and financial service providers. AML regulator of banks and financial service firms.
Companies House	Responsible for registration of companies and maintaining registers of beneficial ownership. Companies house does not have a supervisory or enforcement role.
Consumer fraud	
Financial Ombudsman Service	Handles appeals against banks refusing to reimburse under CRM code
Lending Standards Board (LSB)	Oversees CRM code and published annual report
Payment Systems Regulator (PSR)	See regulators above.
Money laundering	

Organisation	Role in combatting economic crime
HM Revenue and Customs (HMRC)	HMRC is the UK tax authority and also have AML responsibilities as a supervisor of 4000 firms which are not supervised by the FCA or OPBAS. This includes estate agents, art dealers, accountants which are not members of a UK professional body, and financial firms not regulated by the FCA.
Office of Professional Body Anti-money laundering Supervisors (OPBAS)	Based within the FCA and provides AML supervisor for 22 professional bodies which cover accountants and solicitors. OPBAS aims to improve consistency of professional body AML supervision and has powers to ensure they meet regulatory standards. The professional bodies themselves supervise member firms,
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an inter-governmental body which is the global money laundering and terrorist financing watchdog.
The Gambling Commission	AML supervisor for casinos/gambling
Solicitors Regulation Authority	An umbrella organisation for solicitors in England and Wales which is responsible for regulating the professional conduct of more than 125,000 solicitors and other authorised individuals at more than 11,000 firms, as well as those working in-house at private and public sector organisations.
Governance/stakeholder/industry	
Economic Crime Strategic Board	Ministerial level public-private board to oversee economic crime plan
National Economic Crime Centre	Formed in 2018 within the NCA to co-ordinate and task the UK's response to economic crime. Focus on money laundering and corruption. The NECC also uses Unexplained Wealth Orders and Account Freezing orders.
UK Finance	Trade body: UK Finance is the collective voice for the banking and finance industry
Joint Money Laundering Steering Group (JMLSG)	Private sector body that is made up of the leading UK Trade Associations in the financial services industry
Cifas	Not-for-profit fraud prevention membership organisation Specified Anti-Fraud Organisation (SAFO) under section 68 of the Serious Crime Act.
Online Fraud Steering Group	Government and regulators and online companies forum

Conclusions and recommendations

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

1. 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)

2. 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)

3. 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)

4. *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)

5. *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)

6. 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)

7. *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)

8. *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)

9. *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)

10. *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)

11. There may be many reasons for low prioritisation of economic crime by crime-fighting agencies. It does not happen in the street, but often in people's homes. Consumers often, apart from inconvenience, do not suffer directly, since they may be repaid by banks. But these are not reasons to not engage more forcefully with the problem. (Paragraph 58)

12. *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)

Online economic crime

13. *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)

14. 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)

15. *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)

16. 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)

17. *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)

18. 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)

19. 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)

20. *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)

21. 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)

22. 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)

23. *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)

Authorised push payment fraud

24. 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)

25. 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)

26. *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)

27. 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)

28. *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)

29. *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)

Anti-money laundering

30. 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, so as to make full use of them in the fight against economic crime and organised crime more generally. (Paragraph 141)

31. 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. (Paragraph 142)

32. *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)

33. 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)

34. *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)

35. 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)

36. *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)

37. *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)

38. *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)

39. 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. (Paragraph 167)

40. *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)

41. The UK is a world-leading financial centre and needs an extensive legislative and regulatory regime to protect its financial system from money laundering. But it also needs enforcement and to ensure compliance with legislation. It is not obvious that either regulation or enforcement systems are robust enough or up to the job required of them. While the latest evaluation by the Financial Action Task Force of the UK's anti-money laundering and counter-terrorist financing regime is positive, the Government should not be complacent. The FATF evaluation finds room for improvement in enforcement and compliance, and there is still much that the Government needs to do to make it more difficult to launder money in the UK. The latest FATF report is over three years old. In that time money laundering undertaken in the UK has not gone away: it has grown. The response to this threat seems slow and inadequate given the scale of the threats it poses. (Paragraph 172)

42. 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)

43. *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)

Cryptoassets and economic crime

44. 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)

45. *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)

46. 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)

47. *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)

48. *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)

Companies and economic crime

49. 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)

50. 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)

51. *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)

52. *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)

53. 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)

54. *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)

55. 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)

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

Formal minutes

Wednesday 26 January 2022

Members present:

Mel Stride, in the Chair

Rushanara Ali

Anthony Browne

Dame Angela Eagle

Kevin Hollinrake

Alison Thewliss

Economic Crime

Draft Report (Economic Crime) proposed by the Chair, brought up and read.

Ordered, That the Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 247 read and agreed to.

Summary read and agreed to.

Annex read and agreed to.

Resolved, That the Report be the Eleventh Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Adjournment

Adjourned until Monday 31 January 2022 at 3.00 pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 25 January 2021

Graeme Biggar, Director-General, National Economic Crime Centre, National Crime Agency; **Angela McLaren**, Assistant Commissioner for Economic and Cybercrime, City of London Police; **Patrick Campbell**, Temporary Assistant Chief Constable, executive lead for Organised Crime, Counter Terrorism and Intelligence, Police Scotland — Q1–94

Monday 14 June 2021

Mark Steward, Director of Enforcement and Market Oversight, Financial Conduct Authority; **Simon York CBE**, Director of the Fraud Investigation Service, HM Revenue and Customs; **Chris Hemsley**, Managing Director, Payment Systems Regulator; **Martin Swain**, Director of Strategy, Policy and Communications, Companies House — Q95–198

Thursday 8 July 2021

David Clarke, Chair, Fraud Advisory Panel; **Richard Piggin**, Head of External Affairs, Which?; **Helena Wood**, Associate Fellow, RUSI Centre for Financial Crime and Security Studies; **Duncan Hames**, Director of Policy, Transparency International UK — Q199–266

Wednesday 22 September 2021

Amanda Storey, Director of Trust and Safety, Google; **Will Semple**, Director, Global Information Security Team, eBay; **Allison Lucas**, Content Policy Director, Facebook; **Gaon Hart**, Head of Public Policy, Customer Trust, UK & Ireland, Amazon — Q267–426

Monday 29 November 2021

John Glen MP, Economic Secretary to the Treasury, HM Treasury; **Giles Thompson**, Director, Office of Financial Sanctions Implementation (OFSI) and Economic Crime, HM Treasury; **Duncan Tessier**, Director, Economic Crime, Home Office; **Rt Hon Damian Hinds MP**, Minister for Security and Borders, Home Office — Q427–536

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

ECC numbers are generated by the evidence processing system and so may not be complete.

1 Bowers, Simon (ECC0067)

2 Brooks, Richard Private Eye magazine (ECC0067)

3 Amazon (ECC0088)

4 Association of Accounting Technicians (AAT) (ECC0002)

5 Association of British Insurers (ECC0048)

6 Association of International Accountants (AIA) (ECC0057)

7 Association of Taxation Technicians (ECC0023)

8 Barclays Bank (ECC0027)

9 Carnegie UK Trust (ECC0096)

10 Carnegie UK Trust (ECC0054)

11 Centre for the Study of Corruption, University of Sussex (ECC0015)

12 Chartered Institute of Management Accountants (CIMA) (ECC0045)

13 Chartered Institute of Taxation (ECC0022)

14 Chartered Institute of Taxation (CIOT) (ECC0090)

15 City of London Police (ECC0064)

16 Clark, Alexander (Senior Associate, Herbert Smith Freehills LLP) (ECC0070)

17 Cooley, Professor Alex (Professor of Political Science, Barnard College, Columbia University) (ECC0059)

18 Electronic Money Association (ECC0035)

19 Facebook Inc (ECC0087)

20 Financial Conduct Authority (ECC0011)

21 Financial Services Compensation Scheme (ECC0072)

22 Gambling Anti-Money Laundering Group (GAMLG) (ECC0016)

23 Google (ECC0086)

24 Grasso, Dr Costantino (Assistant Professor in Law, Coventry University) (ECC0030)

25 Hall, Ms Demelza (Lecturer in Law, Bristol Law School, University of the West of England, Bristol) (ECC0010)

26 Heathershaw, Professor John (Associate Professor of International Relations, University of Exeter) (ECC0059)

27 HM Treasury (ECC0100)

28 HM Treasury (ECC0102)

29 HM Treasury (ECC0101)

30 ICAEW (ECC0038)

31 Innovate Finance (ECC0049)

32 Institute of Financial Accountants (ECC0060)

33 International Compliance Association (ECC0041)

34 Internet Advertising Bureau UK (ECC0094)

35 Investment Association (ECC0018)

36 JTI (ECC0053)

37 Jee, Mrs Jane (CEO, Kompli-Global Limited) (ECC0039)

38 Lloyds Banking Group (ECC0066)

39 Mastercard (ECC0074)

40 Mayne, Thomas (Research Fellow, Department of Politics and International Relations, University of Exeter) (ECC0059)

41 Microsoft (ECC0097)

42 Office for National Statistics (ECC0073)

43 Onfido (ECC0014)

44 Pasculli, Dr Lorenzo (Associate Head of Research, Coventry Law School; Associate, Centre for Financial and Corporate Integrity; Sessional Lecturer, Imperial College London, Coventry University - Imperial College London) (ECC0017)

45 Pay.UK (ECC0033)

46 Payment Systems Regulator (ECC0032)

47 Personal Investment Management and Financial Advice Association (PIMFA) (ECC0050)

48 Prelec, Dr Tena (Research Fellow, Department of Politics and International Relations, University of Oxford) (ECC0059)

49 Quilter plc (ECC0028)

50 RUSI Centre for Financial Crime and Security Studies (ECC0043)

51 Ryder, Dr Nicholas (Professor in Financial Crime, Bristol Law School, University of the West of England, Bristol) (ECC0010)

52 Sarginson, Richard (ECC0075)

53 Sharman, Professor Jason (Sir Patrick Sheehy Professor of International Relations, University of Cambridge) (ECC0059)

54 Snap Inc. (ECC0098)

55 Soares de Oliveira, Professor Ricardo (Professor of the International Politics of Africa, University of Oxford) (ECC0059)

56 Spotlight on Corruption (ECC0065)

57 Stansfeld, Mr Anthony (ECC0005)

58 Stop Scams UK (ECC0091)

59 TSB (ECC0052)

60 TSB Bank Plc (ECC0095)

61 Taber, Mr Mark (Consumer Finance Expert, Campaigner & Media Contributor, Fixed Income Investments) (ECC0092)

62 The Law Society of England and Wales (ECC0031)

63 The Lending Standards Board (ECC0029)

64 TikTok (ECC0093)

65 Transparency International UK (ECC0051)

66 Transparency Task Force Ltd (ECC0044)

67 Twitter (ECC0099)

68 UK Anti-Corruption Coalition; and Transparency International UK (ECC0055)

69 UK Finance (ECC0068)

70 Which? (ECC0062)

71 Woods, Mr. Martin (Director, AAAML Ltd) (ECC0026)

72 eBay (ECC0089)

List of Reports from the Committee during the current Parliamentary Session

All publications from the Committee are available on the publications page of the Committee's website.

Session 2021–22

Number	Title	Reference
1st	Tax after coronavirus: the Government's response	HC 144
2nd	The appointment of Tanya Castell to the Prudential Regulation Committee	HC 308
3rd	The appointment of Carolyn Wilkins to the Financial Policy Committee	HC 307
4th	The Financial Conduct Authority's Regulation of London Capital & Finance plc	HC 149
5th	The Future Framework for Regulation of Financial Services	HC 147
6th	Lessons from Greensill Capital	HC 151
7th	Appointment of Sarah Breeden to the Financial Policy Committee	HC 571
8th	The appointment of Dr Catherine L. Mann to the Monetary Policy Committee	HC 572
9th	The appointment of Professor David Miles to the Budget Responsibility Committee of the Office for Budget Responsibility	HC 966
10th	Autumn Budget and Spending Review 2021	HC 825
1st Special	Net Zero and the Future of Green Finance: Responses to the Committee's Thirteenth Report of Session 2019–21	HC 576
2nd Special	The Financial Conduct Authority's Regulation of London Capital & Finance plc: responses to the Committee's Fourth Report of Session 2021–22	HC 700
3rd Special	Tax after coronavirus: response to the Committee's First Report of Session 2021–22	HC 701
4th Special	The Future Framework for Regulation of Financial Services: Responses to the Committee's Fifth Report	HC 709
5th Special	Lessons from Greensill Capital: Responses to the Committee's Sixth Report of Session 2021–22	HC 723