PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

ECONOMIC CRIME AND CORPORATE TRANSPARENCY BILL

First Sitting

Tuesday 25 October 2022

(Morning)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Saturday 29 October 2022

The Committee consisted of the following Members:

Chairs: † Mr Laurence Robertson, Hannah Bardell, Julie Elliott, Sir Christopher Chope

† Anderson, Lee *(Ashfield)* (Con)
† Ansell, Caroline *(Eastbourne)* (Con)
† Byrne, Liam *(Birmingham, Hodge Hill)* (Lab)
† Crosbie, Virginia *(Ynys Môn)* (Con)
† Daly, James *(Bury North)* (Con)
† Doyle-Price, Jackie *(Minister of State, Department for Business, Energy and Industrial Strategy)*
† Hodge, Dame Margaret *(Barking)* (Lab)
† Huddleston, Nigel *(Lord Commissioner of His Majesty's Treasury)*
† Hughes, Eddie *(Walsall North)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Kinnock, Stephen *(Aberavon)* (Lab)
† Malhotra, Seema *(Feltham and Heston)* (Lab/Co-op)
† Morden, Jessica *(Newport East)* (Lab)
† Newlands, Gavin *(Paisley and Renfrewshire North)* (SNP)
† Stevenson, Jane *(Wolverhampton North East)* (Con)
† Thewliss, Alison *(Glasgow Central)* (SNP)
Tugendhat, Tom *(Minister for Security)*

Kevin Maddison, *Committee Clerk*

† attended the Committee

Witnesses

Nick Van Benschoten, Director, International Illicit Finance, UK Finance

Gurpreet Manku, Deputy Director General and Director of Policy, British Private Equity and Venture Capital Association (BVCA)

Nigel Kirby, Head of the Financial Intelligence Unit (FIU), Lloyds Banking Group

Andy Gould, Detective Chief Superintendent and NPCC National Cyber Crime Programme Lead & Interpol Global Cybercrime Expert, National Police Chiefs' Council

Arianna Trozze, PhD student, UCL researching detection and prosecution of cryptocurrency crime

Jonathan Hall KC, Independent Reviewer of Terrorism Legislation

Public Bill Committee

Tuesday 25 October 2022

(Morning)

[Mr Laurence Robertson *in the Chair*]

Economic Crime and Corporate Transparency Bill

9.25 am

The Chair: Good morning, everyone. We are sitting in public and our proceedings are being broadcast. I have a couple of preliminary announcements. *Hansard* colleagues will be grateful if Members could email their speaking notes to hansardnotes@parliament.uk and I remind everyone—including myself—to turn mobile phones to silent.

We will first consider the programme motion on the amendment paper, and then a motion to enable the reporting of written evidence for publication and the motion to allow us to deliberate in private—which will take only a minute or so—before the oral evidence session. I hope to take those motions formally.

Ordered,

That—

1. the Committee shall (in addition to its first meeting at 9.25 am on Tuesday 25 October) meet—

(a) at 2.00 pm on Tuesday 25 October;

(b) at 11.30 am and 2.00 pm on Thursday 27 October;

(c) at 9.25 am and 2.00 pm on Tuesday 1 November;

(d) at 11.30 am and 2.00 pm on Thursday 3 November;

(e) at 9.25 am and 2.00 pm on Tuesday 8 November;

(f) at 9.25 am and 2.00 pm on Tuesday 15 November;

(g) at 11.30 am and 2.00 pm on Thursday 17 November;

(h) at 9.25 am and 2.00 pm on Tuesday 22 November;

(i) at 11.30 am and 2.00 pm on Thursday 24 November;

2. the Committee shall hear oral evidence in accordance with the following Table:

TABLE

Date	Time	Witness
Tuesday 25 October	Until no later than 10.10 am	UK Finance; British Private Equity & Venture Capital Association
Tuesday 25 October	Until no later than 10.30 am	Lloyds Bank
Tuesday 25 October	Until no later than 11.05 am	The National Police Chiefs Council; Arianna Trozze
Tuesday 25 October	Until no later than 11.25 am	Jonathan Hall KC, Independent Reviewer of Terrorism Legislation
Tuesday 25 October	Until no later than 2.30 pm	Companies House; National Economic Crime Centre (National Crime Agency)
Tuesday 25 October	Until no later than 3.00 pm	City of London Police; Serious Fraud Office; The National Police Chiefs Council
Tuesday 25 October	Until no later than 3.45 pm	Spotlight on Corruption; Global Coalition to Fight Financial Crime; UK Anti-Corruption Coalition
Tuesday 25 October	Until no later than 4.15 pm	Oliver Bullough; Bill Browder
Tuesday 25 October	Until no later than 4.45 pm	Professor John Heathershaw, University of Exeter; Chatham House
Thursday 27 October	Until no later than 12.00 noon	Centre for Financial Crime and Security Studies at RUSI; Transparency International
Thursday 27 October	Until no later than 12.30 pm	OpenCorporates; Elspeth Berry, Nottingham Law School
Thursday 27 October	Until no later than 1.00 pm	Graham Barrow
Thursday 27 October	Until no later than 2.20 pm	Institute of Chartered Accountants in England and Wales
Thursday 27 October	Until no later than 2.50 pm	The Chartered Governance Institute UK & Ireland; City of London Law Society
Thursday 27 October	Until no later than 3.10 pm	Catherine Belton
Thursday 27 October	Until no later than 3.30 pm	Professor Jason Sharman, University of Cambridge

3. proceedings on consideration of the Bill in Committee shall be taken in the following order: Clauses 1 to 48; Schedule 1; Clauses 49 and 50; Schedule 2; Clauses 51 to 90; Schedule 3; Clauses 91 to 100; Schedule 4; Clauses 101 to 134; Schedule 5; Clauses 135 to 141; Schedule 6; Clause 142; Schedule 7; Clauses 143 to 153; Schedule 8; Clauses 154 to 162; new Clauses; new Schedules; remaining proceedings on the Bill;

4. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 29 November.—*(Jackie Doyle-Price.)*

The Chair: The Committee will proceed to line-by-line consideration of the Bill on Tuesday 1 November at 9.25 am.

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Jackie Doyle-Price.)*

The Chair: Copies of written evidence that the Committee receives will be made available in the Committee Room and will be circulated to Members by email.

Resolved,

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—*(Jackie Doyle-Price.)*

9.27 am

The Committee deliberated in private.

Examination of Witnesses

Nick Van Benschoten and Gurpreet Manku gave evidence.

9.30 am

The Chair: We are now sitting in public. Good morning to our first witnesses. I am going to crack on straightaway, because the timetabling is tight this morning, but you are very welcome. Thank you for coming. I remind everyone we are now being broadcast. Do any Members need to make a declaration of interest? No. Witnesses, will you briefly introduce yourselves, please?

Nick Van Benschoten: My name is Nick Van Benschoten. I work at UK Finance, which is the voice of the UK's banking and finance industry. I work in our economic crime policy unit.

Gurpreet Manku: I am Gurpreet Manku. I am the BVCA deputy director-general and director of policy. The BVCA is the representative body for private equity and venture capital in the UK. We look after the smallest venture capital firms investing in start-ups all the way through to growth capital and private equity firms offering across the UK and worldwide.

The Chair: Thank you. You are welcome. Given the time constraints, I will ask Members for short, snappy questions, so short, snappy answers will be very much appreciated. I start with the Opposition spokesman.

Q1 Seema Malhotra (Feltham and Heston) (Lab/Co-op): I will put one brief question to each of the witnesses, as I know colleagues have other questions.

First, thank you for giving evidence. Nick, I am conscious of your perspective for the whole of the financial services sector and I want to ask a question specifically about data and information sharing: is enough happening in the Bill to deal with what has been described to me as the chilling factor of sharing information? What might come back in the consequences of promoting sharing?

Ms Manku, you gave evidence in which you described the "unintended consequences" of requiring limited partnerships to have a registered office. I am not sure that we would necessarily agree with that, so I am interested in your argument.

Nick Van Benschoten: We welcome the provisions in the Bill for private sector information sharing. We are very glad to see that they apply across the AML regulated sector—not just banking, but payments, crypto, e-money and so on—which allows us to follow the money and the data as criminals move across sectors to obscure their tracks. That is very welcome.

We also welcome the protection from breach of confidence. That can be in common law and, typically, in terms and conditions. It is important to be able to encourage people to do the right thing without the fear that they might be subject to litigation. However, we note that the Bill falls short in the way in which we can share information with the National Crime Agency, which is a disapplication of all civil litigation. We would like to explore whether we could go further in the Bill, but those provisions are very welcome.

I will not say too much. An expert colleagues from one of our member banks is speaking to you later, but I stress the fact that we want to encourage the use of information sharing as much as possible. It is not just where customers are exited, but where a restriction is placed on them, such as additional monitoring or thresholds—there are a lot of ways in which the banks put each other on notice. We want to encourage that use as much as possible in true cases of economic crime.

Gurpreet Manku: We welcome the provisions in the Bill to ensure that limited partnerships are not abused by criminals—I want to make that clear. On the point about having a registered office, we agree that there needs to be a service address in the UK for the delivery of documents and for the registrar to contact the organisation, but our concern is actually in reference to the legal meaning of "registered office" in the Companies Act 2006 when it comes to standard companies. We know that the term means something else in that context, so it is actually quite a knotty legal point rather than an objection to the principle of having a link to the UK.

It is just about ensuring that any existing arrangements that have been set up for legal and regulatory purposes for international funds structures remain intact. We will need to work through the process of what this means in practice. We were speaking to BEIS officials as soon as yesterday to talk through what it means in practice. This is more of an implementation point, and we have suggested edits that will come through to officials.

The Chair: Would you like to follow up, Seema?

Seema Malhotra: Quite a lot of people want to ask questions, so I will make further remarks later.

The Chair: Dame Margaret?

Q2 Dame Margaret Hodge (Barking) (Lab): Gurpreet, your written evidence is very negative. At one point, it states:

> "We do not think these proposed changes support the Bill's central aim of reducing the use of limited partnerships for money-laundering, since criminal users of limited partnerships will simply ignore them."

That suggests to me that we are not going far enough. We are aiming to catch the people who are guilty of economic crime. Attached to that, somehow I cannot see any investor wanting anything other than to know that they are putting their money into a kosher investment. Even if you are just a pension fund putting your money into a scheme, it does not seem a bad idea to check that the person behind it is legitimate and not a drug or people smuggler.

Gurpreet Manku: Absolutely. We agree with you that it is not in our interests to have our limited partnership fund structure abused by criminals for all those reasons. We believe that the introduction of annual confirmation statements, the requirement to have authorised corporate service providers register limited partnerships and the power for HMRC to obtain accounts will deter criminals and prevent them from using the vehicle—we hope that they have stopped using it now given that these reforms are finally going through Parliament.

On how those points link to the evidence you quoted specifically, which was actually about some niche requirements on passive investors in a limited partnership fund, a worry there is that those investors might be deterred from using the UK limited partnership structure

because they feel that their liabilities are being increased, that they are being asked to do the job of management and that criminal sanctions are attached to that. That part of our evidence applied not to the Bill as a whole but to those specific areas.

Q3 Alison Thewliss (Glasgow Central) (SNP): I have some questions for UK Finance about verification at Companies House. What would it take to have confidence in that verification system? You said in written evidence that Companies House should avoid over-reliance on UK-registered trust and company service providers. Can you tell us a bit more about that and what you would like to see put in place?

Nick Van Benschoten: We think that the Bill's provisions for Companies House reform definitely point in the right direction. The question for us is, "Are they going far enough and will they be implemented fast enough?" Companies House abuse is, as I am sure you are all aware, a significant problem that we in the regulated sector have been trying to compensate for, but we cannot. We need Companies House to act as a proactive gatekeeper.

On the verification measures, one of the key points is that they fall short of minimum industry standards. Verification of identity is necessary but not sufficient. A key thing we have noted is that the Bill does not provide for order-making powers to allow Companies House to verify the status of directors or beneficial owners, and for that sort of requirement on company information agents and so on. That seems an odd gap. We understand that it may be a matter of phasing or resourcing, which can be dealt with in the implementation, but not if we do not have the order-making powers in the bill.

I have spent 12 years arguing for Companies House reform in my various roles. I do not have another 12 years in me, to be frank. We need to make sure that the Bill gives the powers so that the debate can be had during implementation and, if necessary, a phased or risk-based approach. What I mean is that there is a real risk of nominee directors and abuse thereof. Companies House needs to be able to verify that and therefore bring other things within its realm of power, querying and amending the register.

The how is maybe another question for more detail, but a risk-based, reasonable approach is also minimum industry standards. We have not yet seen it, but I note that the international body FATF—the Financial Action Task Force—agreed last Friday that it was going to consult on best practice guidance on implementing new standards for company registers. These are the same reforms that the Government pushed for as part of their G7 presidency. It has been part of the change: the US is setting up a register; Switzerland is moving. The UK cannot fall behind these new standards, so it is important that the Committee takes cognisance of that.

Trust or company service providers is one of those cases where we know that there is an issue; the banking sector and other industry partners in the joint money laundering intelligence taskforce and another four along with the National Crime Agency did a study of the risks of abuse in the UK trust or company service provider sector. We found shortfalls. There was a remediation exercise agreed. I understand that the remediation exercise is still ongoing. It is one of those sectors where there are concerns. We are doing other work that I am not at liberty to discuss, but it is about that sector.

That means that Companies House needs to be careful and cautious. There need to be strict legal undertakings with proper penalties, not just that they have met the standard of verification but that they have done everything they should be doing as a regulated sector. There needs to be access to the evidence of these checks, and that evidence needs to be something that, on a risk basis if necessary, can be queried—not just the information in the register but the actual checks undergoing. There needs to be the ability for Companies House to take sample checks and do also risk-based reviews. That may be something we can come to later on in terms of the querying power. I am sorry for a long answer, but it is an important point.

Q4 Alison Thewliss: Thanks for that, it is really useful. Anti-money laundering responsibility has pushed over on to some of these trust or company service providers, which could be quite a loophole in terms of what you are saying about checks and verification. Would it be useful for Companies House to have that responsibility itself for things registered directly with it?

Nick Van Benschoten: I do not have a view on that. I know that the Treasury will be consulting on reforming the AML supervisory regime. That is something we have been pushing for for quite a while. I know that Jersey, for example, has a very different model where it has most of the regulator sector under one bailiwick, and that includes company formation. That may be something that the Committee looks at in future, but it is not the UK model at the moment.

Our priority would be, rather than look at the cost-benefit narrative and machinery of government change, the co-ordination point. There need to be powers not just to request information but to get information from other supervisors. There needs to be the ability to pass information around the ecosystem, including the National Crime Agency and regulated sector people sharing intelligence. There are some provisions in the Bill at the moment where we think they could go further on that matter, but the key thing is that Companies House needs to be a data hub. On whether it has the responsibility or others, we have not taken a view on that yet, I am afraid.

Q5 Alison Thewliss: That is useful. Incorporation fees are ridiculously low at £12. The Treasury Committee recommended £100. Do you have a view on that?

Nick Van Benschoten: I do not think they are unprecedentedly low. From a very quick survey, we found that Benin and Turkmenistan also have a low figure. I am not sure that is the company the UK wants to keep. There is a question about international competitiveness. It is important to note that in other EU countries with major financial centres it is in the £50 to £100 range. That does not seem an unreasonable amount for us.

Perhaps more importantly, we think Companies House needs to get resourced properly. You have to will the means, not just the ends. It is very important that Companies House fees are set at a reasonable level that would not deter an entrepreneur but would disrupt some of the bulk abuse we have seen, in which criminals set up hundreds and hundreds of shell companies. That is definitely a typology that we have seen.

Once there is enough money coming through main registration, there is then the question of whether Companies House will be granted any investment money out of the economic crime levy that is coming in next year. It is important that the levy is spent on things that actually improve the system, and that we do not just cross-subsidise, and that some of the opportunities also have a benefit for the economy—maybe for streamlining the onboarding of small companies, or for facilitating other access to regulated services.

Obviously, there is the question of what the Government will spend the levy on. We welcome the money that they have spent so far. There is an interesting proposal—by, I think, one of the Committee members' all-party parliamentary groups—that the Government should match-fund the economic crime levy. Obviously, we in the regulator sector would love that. It is something for the Government to consider.

Q6 The Minister of State, Department for Business, Energy and Industrial Strategy (Jackie Doyle-Price): I want to come back to the question that Dame Margaret Hodge asked you, Gurpreet. I hear your point that some of the obligations may deter private equity investment, but through the legislation, we are making the positive statement that we are determined to improve standards of regulation, with a view to tackling crime, and are saying that this country will be safe place in which to invest. To what extent will the Bill be a deterrent? Do you have any evidence or have you made any calcuations on that? If so, which other centres do you expect will benefit from our introducing this system of regulation?

Gurpreet Manku: To clarify, I think this is a really important Bill. We have been saying for a very long time that the provisions need to be implemented quickly. The issues that we have raised are really on points of detail. Raising an international private equity or venture capital fund is quite a complex process. We hope that the swift introduction of the provisions will deter criminals from using the vehicles that we are talking about. When the requirement was introduced for Scottish limited partnerships to go on the people with significant control register, it led to a dramatic drop-off in the use of such partnerships for nefarious purposes. We were not aware that English limited partnerships were being used in that way instead, and we were surprised that they were, because English limited partnerships do not have a legal personality, and so cannot hold assets and should not be able to set up a bank account; certainly, they cannot in this country. We were therefore surprised by the scale of abuse there.

The Government are sending a really strong signal by introducing these provisions, particularly the requirement to have an authorised corporate service provider submit documention and the measures around annual confirmation statements. That should deter criminals. Our version of the limited partnership fund structure has been emulated across the world, so there is a lot of competition, in the sense that international fund groups could set up a vehicle in the UK, the EU or the US. Our wish is for them to be here, because that drives other economic activity.

We have a huge domestic venture capital and growth capital funds industry that invests in small businesses around the country. Two thirds of our investment is outside London; 90% of investment goes to small and medium-sized enterprises. Our managers are small firms; they need a domestic vehicle that works and is trusted by international investors, including those from the US who invest heavily in our members. These vehicles are used by private equity and venture capital funds. They are also used by infrastructure, pension schemes and fund-to-fund investors. Notably, they are also used by the British Business Bank through its equity programmes. It is the largest venture capital and growth equity investor in the UK. It has a really important role in catalysing innovation and crowding in additional institutional investors. I am passionate about the need for a robust UK vehicle, and it has been really disappointing to see the abuse first in Scotland and then in England in recent years.

English limited partnerships and Scottish limited partnerships are popular because they are here. The UK law courts attract institutional investors, as does the fact that we have a large professional services community here. Because we have funds here, we also have the administration here, which means that we have good-quality jobs around the country; some of our members have hubs in Belfast and Southampton. I am passionate about ensuring that this vehicle works, and the rules that are being introduced will deter criminals; they will improve the robustness of the vehicle.

Our points are really points of detail, just to ensure that the limited liability status of investors is protected and that we can implement these reforms in a swift and easy manner.

Q7 Jackie Doyle-Price: That is very helpful, but can I turn the question on its head? To what extent do you think these changes could make this country more attractive, given that we are making a very clear statement about the standards that we expect in these vehicles?

Gurpreet Manku: I think it will make a very good statement, and it will attract international investment. There is a huge level of interest in the UK because we have had some brilliant growth stories in our businesses, particularly in deep tech in life sciences and biotech, especially coming out of the pandemic. There is a lot of interest in investments, and the Bill will send a signal that these investors should be using UK fund vehicles and not those based outside the country.

Q8 Liam Byrne (Birmingham, Hodge Hill) (Lab): Nick, can I check two things that you said, which I think reveal some significant flaws in the Bill? First, I think you said that the verification regime proposed for Companies House is weaker than that for the regulated anti-money laundering sector. Is that the case?

Nick Van Benschoten: That is the case, and perhaps more, in a way, than you might expect. We are not saying that Companies House should be regulated for anti-money laundering, but it does not have the provisions to verify the status of directors or beneficial owners. That is the gap to the standards. I should stress that the industry standards allow reasonable measures in how you verify status, because it is a challenge, but those reasonable measures are a matter of how, not whether.

Q9 Liam Byrne: Right, so we have a risk of a two-tier verification regime: one operated by Companies House and one gold-standard regime operated by the regulated AML sector.

The second thing I think you said is that the verification regime proposed in the Bill runs a risk of failing to establish those in actual economic control of a company. Is that true?

Nick Van Benschoten: There is always the risk, yes, but some of the shortfalls in the Bill can be addressed, and we think they should be, so that we can address the issues that you mention. In specific terms, some of the abuses are going to be abuses that the UK has suffered in the past; others will be abuses that we have seen happening overseas. The key thing is that the Government need to take a risk-based approach to measuring those. At the moment, the Bill does not allow Companies House to pick up some of those measures, including if we identify them in the future and want to remedy the regime.

Q10 Liam Byrne: So you would say to Members of Parliament who are worried about bad people transferring control of an economic asset to proxies that, at the moment, we do not have enough safeguards in the Bill.

Nick Van Benschoten: I think they could be improved, yes.

Q11 Stephen Kinnock (Aberavon) (Lab): A couple of quick questions from me. First, on resourcing, the Bill puts a number of additional tasks, requirements and responsibilities on Companies House. How would you estimate the gap between where Companies House is now and where it would need to be if it were to properly implement and execute the Bill? Secondly, we have seen that a number of other jurisdictions—the Netherlands and Singapore in particular—have moved further and faster than the UK on data sharing. Do you think the Bill will bring us up to the gold standard for data sharing?

Nick Van Benschoten: Are you addressing the question to me?

Stephen Kinnock: To both of you, if you do not mind. It would be good to hear from both of you on both questions.

Nick Van Benschoten: My view is that, in terms of resourcing, there is a lot of new technology. Companies House is quite lucky that it can leapfrog using best practice. We have had a number of meetings with it. I think you may be hearing evidence from Graham Barrow later; we had a roundtable with Graham Barrow, Companies House and some other providers to try to explore this issue. Companies House is quite lucky in that it does not need to be a manual exercise: the goal is to get very much a minority manual review by humans, with the majority being technology and machine learning and so on.

That said, we also did a webinar with a number of data providers, including well-known companies that are looking at the size of the challenge and the opportunities. There is a big difference between quick wins and longer-term investment. Companies House already has a risk engine; it has data analytics already. It is just that its enforcement people, working as hard as they can, have their hands tied behind their back. I think there will be a lot of policy development, and work to implement not just the technology but the way that it interacts with the regime that it wants to set up. It is a challenge, because the short term is a burning platform.

Known patterns of abuse are identified every day. Also, a number of companies may be about to walk off with a lot of stolen public money through bounce back loan scheme fraud, and that is an area where Companies House may or may not have powers. Whatever powers the Bill gives need to be operated at speed. Sorry, that was a roundabout way to get to your question. There are short-term things it can do now, and there is a long-term thing; but it must make sure that it is dealing with the urgent as well as the transformative. We understand that the transformative exercise will take a long time, but there is also need for it to apply more tactical focus around the risks, especially in the short term. What was your second question? Sorry, I forgot it in my enthusiasm.

Stephen Kinnock: On data sharing.

Nick Van Benschoten: Each country has its own threats and problems. Singapore's COSMIC database addresses particular exposures and problems that it has with trade-based money laundering. The UK is in a different place in that market, but we have our own problems. In terms of data-sharing, one of the key things we would like is for Companies House to enable permissioned access to the regulated sector. We have a lot of problems that are not so much in high-end corporate, but in the retail customer base. We have money mules for fraud, we have a lot of spoof companies enabling purchase and investment scams. Trying to work out where exactly the needle is in the haystack is difficult when we do not all have access to the same data.

Companies House seems to be facing a binary choice: either it is public, or it is only for the public sector. There does not seem to be a middle ground that works on a need-to-know basis, where you have an obligation to apply money laundering checks and to have careful, need-to-know handling procedures and anti-tipping off and so on, and where that information is available for the purposes of safeguarding your customer and maintaining the integrity of the market. From a UK perspective, that is definitely something that we would support. We also think it might allow us to develop something equivalent for our own risks, as the Singaporeans and other countries have done.

Gurpreet Manku: We have focused on the limited partnerships provisions in the Bill, but in principle we would support Companies House being appropriately resourced to implement all these changes effectively. I have no objections to data-sharing with relevant authorities. Our investment community operates across the globe, so we are used to this type of activity in other jurisdictions.

The Chair: Perhaps two quick final questions. Alison, you wanted to come back.

Q12 Alison Thewliss: Thank you, Chair. You talked about the impact on SLPs from the changes in legislation. Have you looked at the issue of Irish limited partnerships? Bellingcat has found that over a thousand ILPs were created between the early 1900s and 2014, but 2,400 were set up from 2015 onwards. Are those who are looking to exploit the system just chasing round for the structures that they need?

Gurpreet Manku: We have not looked into that. I do know that Ireland has set up a new funds limited partnership, so that could be part of the reason for their

growth—but that was very recent, so I do not know why that has happened. Again, it is quite worrying if people are just moving around, exploiting different structures.

Q13 Dame Margaret Hodge: It is interesting that in this sitting, we have got rather contradictory evidence. On the one hand, you, Nick, are saying that we are not getting enough information on the basics, such as identity checks, and that we need information about more people; on the other, Gurpreet, you are saying that there is too much data, and it will damage business formation and prosperity. I wanted to give you the opportunity to think again, particularly you, Gurpreet. Have you got any figures? In your evidence, you say that you have to set up a tertiary body somehow. Is that just your guess? I think Alison Thewliss will agree that all our evidence is that the structures we are dicussing are among the most abused, and have facilitated more money laundering and economic crime than almost anything else. If we do not sort this out, it will just add to our problem, rather than enabling us to do what the Minister wants.

The Chair: May I ask for a brief answer?

Gurpreet Manku: We are commenting on different parts of the Bill. On the limited partnerships part, we think that a number of the new provisions being introduced will deal with the issues you have outlined. To reiterate, we are really unhappy and shocked to see the amount of abuse of this fund structure, because it has been in place for decades and is used for legitimate purposes on our side.

When you read the paper cold, you are right—it does look quite negative; we probably should have reinforced our support for the provisions that will work. Sometimes we have a tendency to go into the detail and start thinking about how things will be implemented in practice. We want to ensure that we use the tools and implement the most effective measures in the Bill. If there are other points that, on balance, would not necessarily help with the overall aim of the Bill, perhaps we should look at whether they need to be implemented.

Q14 The Chair: Nick, would you like to come in very briefly?

Nick Van Benschoten: I would just say that we support the application of the Companies House powers to all the entities registered at Companies House. Companies House needs risk-based querying powers and to be able to follow the data and the money. My earlier comments also apply to the point about limited partnerships and verification by trust company service providers; we need a much more cautious approach to the reliability of that service.

The Chair: I call Seema for what is probably the last question.

Q15 Seema Malhotra: I want to come back to where I started and to pick up on the evidence given about regulated and unregulated sectors. Obviously, there are issues in banks and the financial sector, but we have not talked much about cryptocurrency or other areas such as gambling, where there may be flows of illicit finance—cash and so on. Do you think that more needs to be done about unregulated sectors? Does the perimeter need to be extended? What relationships are there between economic crime in the financial sector and that in other sectors?

Nick Van Benschoten: From a financial sector point of view, it is important to look at this as an ecosystem; that is definitely how the criminals look at it. They look for weak points. Sometimes the problems are upstream of the financial sector, but it crystallises in our sector because that is when people realise that the money has gone out of their accounts.

We are very supportive of the fraud provisions in the Online Safety Bill—we think they are critical. We also think it critical that everyone be incentivised to play their part. That includes potential issues around the scope of the economic crime levy, which applied only to the AML regulated sector. The Bill levels up powers for the cryptoasset seizures and freezing orders. That is welcome; it simplifies things. We work with crypto sector associations. They are now trying to realise that they are part of a regulated sector, and they want to be part of the gatekeeper community.

On what the Bill does, it is important, as I mentioned, that there be information sharing across sectors. That is key, because then we can see whether we all have a different piece of the puzzle to put together. A systems approach is definitely needed; that is maybe the context for our point that Companies House should really be an enabling hub. That includes giving access to information that may not be on the public register.

Q16 Seema Malhotra: If this legislation is to be as effective as it needs to be, will there need to be dependencies on other legislation?

Nick Van Benschoten: That is a very good point, yes. There are also the information processing provisions on the identification, prevention and detection of economic crime in the Data Protection and Digital Information Bill, as well as the Online Safety Bill. Obviously, consultation is ongoing about a statutory APP or authorised push payments code. There may also be other vehicles in one of those bits of legislation, or this one, for other measures that we are currently discussing with the Government. I think the Minister made reference to our difficulty with having to process payments within a set period—there is a hard regulatory obligation, even when we have identified economic crime risks. We are still exploring whether that needs guidance or legislation. All these things need to come together if we are to design the right ecosystem. That then raises the question of who is leading the system. We are working on that with the Government.

The Chair: We have less than one minute. Ms Manku, do you want to make a few final comments?

Gurpreet Manku: We are glad that these provisions are being implemented. We have been working on them since 2018, and stand ready to work with officials to ensure that they are implemented effectively to meet the Bill's overall goals.

The Chair: That was good timing. I thank the witnesses for coming to see us and for their answers.

Examination of Witness

Nigel Kirby gave evidence.

10.5 am

The Chair: Thank you for joining us, Mr Kirby. We have until 10.35 am. Would you briefly introduce yourself, please?

Nigel Kirby: Good morning to the Chair and the Committee. I am currently the head of the group financial intelligence unit at Lloyds Banking Group. Across the industry, I am a representative on UK Finance's information and intelligence committee and, for full transparency, as part of that I was deputy director of the economic crime command of the National Crime Agency.

Q17 Seema Malhotra: It is good to have you here, Mr Kirby. Could you give us a little flavour of the kinds of trends and patterns of economic crime that you are seeing? How are criminals behaving? Are you seeing new trends domestically and internationally?

Nigel Kirby: Perhaps I can give a couple of the examples that we used when we were speaking with the Home Office for the formation of the Bill. In one case that involved money laundering, Lloyds identified seven customers that were receiving cash payments into their accounts. We linked those seven customers because they used the same fraudulent documentation—a gas bill—to set up their accounts. They had all been linked using fraudulent IDs. They were sending money to one individual in another bank.

At the moment, we act on such cases by meeting our statutory obligations—we exited those customers—but from the criminal's perspective, the second bank is not aware of the fact that they are receiving those funds, because we do not have the capability to share that information with them. Secondly, it is highly likely that those seven customers moved on to other banks and continued that activity because, again, at the moment we have no capability to share the information about our economic crime concerns in that space.

That is a fairly simple example, but to build on it, the same kinds of techniques were used to launder criminal funds in another case involving three companies that were banking with us. We recognised that they were receiving cash money from the same post office source. They were also receiving money from other companies in banks. That money all got consolidated and was sent out to, if you like, a fifth bank. I do not know what happened to it after that—we cannot see.

Q18 Seema Malhotra: A fifth bank domestically or internationally?

Nigel Kirby: It was, at that particular point, a UK domestic bank, yes. We have this sort of complexity of companies that are linked using different identities and are moving money around, layering it in the system, and sending it to other parts of the system. We are currently limited in what we are able to do.

On those three companies that we at Lloyds could see were receiving money from five other banks, at the time we could not inform those banks of our concerns or explore with them whether that money was legitimate—it is not all illegitimate; it could, of course be legitimate funding. Furthermore, when that money was consolidated and sent to another bank, we were unable to inform that bank.

Whatever the predicate crime—there are all sorts of predicate crimes—the layering is not that complex but it uses the banking system, across the banking system, to obfuscate and layer the funds, and then the criminals move on. The big challenge at the moment is that we can report those entities and companies, but they will just go and open up in another high street bank, and when they have exhausted the five major high street banks, they will go to the challenger banks, and when they have exhausted those, they will go to the fintechs. We are not aware of that in the way that other industries such as the motor industry might well be.

Q19 Seema Malhotra: That is extremely helpful. To follow up, will the measures in the Bill go far enough to enable the critical data sharing and the ability to inform other banks of what you think is important? In doing that and in going as far as you feel is needed, are appropriate safeguards in place for some things that may be legitimate finance and able to be explained by visitors or customers?

Nigel Kirby: To take the first question first—about whether the Bill goes far enough—I commend and compliment the Home Office. It worked with us on the Bill. This piece of legislation was, fortunately, done by the Home Office but using our case examples. The Home Office explored whether the Bill would work with the scenarios we gave them. That helped the information provisions to be pretty much in the right place. There is one key omission from our perspective; I can come back to that, if helpful. There is also one key dependency in another Bill—

Q20 Seema Malhotra: Sorry, what is the omission?

Nigel Kirby: The omission was referred to by Nick Van Benschoten: the civil liability protection. In the UK, we have real trust and confidence built up in voluntary information sharing with the National Crime Agency under section 7 of the Crime and Courts Act 2013. That has been the basis of our voluntary sharing, and we have built confidence in it over seven years.

The legislation has two limbs to civil liability protection—I will have to read my notes to make sure I do not make a mistake. The first limb is

"an obligation of confidence owed by the person making the disclosure"—

that limb is also included in this Bill. The second limb that we rely on is

"any other restriction on the disclosure of information (however imposed)"—

that limb is not included in the Bill.

Our position is that the Bill should align with the existing legislation that we are comfortable with. We would have more comfort in sharing and be more incentivised to share if we had the same protections as we have when we share with the National Crime Agency. The further observation is that there is not just one precedent; another piece of legislation, the Criminal Finances Act 2017—under section 11, I think—had sharing provisions with the purpose, in effect, of bringing better disclosures to the NCA. It had exactly the same two civil liability limbs, written in the same way. We believe that the second limb would be hugely helpful in doing things.

You might want to come back, but the other dependency that is key for us is that the Bill is drafted as an interlink with the GDPR, as you well know. That is wise, and one of the protections—that it has that link with the GDPR—but because the Bill has that interlink, the provisions in the GDPR are really important. I am aware that there is a draft Bill that has not yet been laid before Parliament

and, again, we—my colleagues in UK Finance—have worked on that Bill. Absolutely key for us in the draft Bill is a legitimate interest for sharing, because that Bill sets out legitimate interests.

At the moment, the GDPR cites only fraud as a legitimate interest, and no other crimes. To be able to make the measure in this Bill work, we need the revised GDPR to have the "prevention, investigation" and "detection" of crime—what the GDPR says at the moment—to be for all crime as a key part, so we can make the interlink. Otherwise, we are restricted only to fraud, but do not include wider economic crime.

Q21 Alison Thewliss: That is really interesting. I want to pick up a little on what you said earlier about receiving banks and where fraud has been against some of your customers. The Treasury Committee, in our report into economic crime, discussed fraud on online platforms, and the level of it. I understand from speaking to some of your colleagues in the past that that has been increasing. If someone tries to buy something on Facebook but is defrauded, the bank of that person will refund them. There is no obligation on the platform to take any action, and the receiving bank of the person who has done the fraud will take no action either. Could more be done in the Bill to break those types of transactions, with fraud being perpetrated on online platforms? What is the wider impact on the banking system?

Nigel Kirby: Your question is specifically about fraud and what we can do in that space. I suggest that tackling fraud is a shared responsibility. When you look at a typical fraud, you have the payment platform, as you mention; you have a sending bank and a receiving bank, and you have the victim. To tackle it, we need to look at the whole ecosystem, as Nick said, and have an approach that works. I am not convinced that there are things that one can put into the Bill for that—it is the wider point of the whole ecosystem coming together for any fraud strategy moving forward, how we tackle that and how we incentivise the right behaviours for tackling fraud in future.

Q22 Alison Thewliss: Would a wider "failure to prevent economic crime" obligation be useful in that regard?

Nigel Kirby: When looking at enacting new legislation, I would go back to the purpose. Putting my NCA hat on, rather than from a Lloyds perspective, I was involved in two pieces of quite significant legislative change: the introduction of asset forfeiture orders in the Global Finance Act, and the change in the sanctions penalty from two years to seven years. That was done very much on an operational need basis. As an organisation, we were able to put out the operational perspective of the gap—the fact that we could not use certain powers because, in the sanctions case, of the length of the sentence. There was a big gap in the ability to seize assets from a civil regime.

In whatever we look at, it is important that we understand that gap from an operational perspective. It is clear and compelling that by having new legislation, that gap gets filled. The other point is that there is the resource and the ability to use the legislation when it comes forward.

Q23 Alison Thewliss: Finally, do you have any comments on the changes being made to the suspicious activity report regime in the Bill?

Nigel Kirby: I would leave those to UK Finance; it is not my area of expertise. Our nominated office in Lloyds feeds into UK Finance so we get the whole industry.

Q24 Jackie Doyle-Price: I want to come back to the issue of GDPR, if I may. The whole ethos sitting behind the GDPR legislation is to defend the subject that the information is about. As you just highlighted, that feels really incompatible with having information sharing for the purposes of combating crime. I just want a better feel from you of how much of a barrier that will be. Is it a barrier or is it tying our hands behind our back to use the issues in the Bill? How much more do we have to challenge the ethos behind GDPR for us to build a system that is fit for purpose?

Nigel Kirby: I can link this to your question on safeguards. Coming from a law enforcement background, I believe that safeguards for members of the public are really important in this space, and I am used to following those. GDPR does not stop us from doing some things. It provides a set of safeguards for what we do.

When you look at what the Bill does on safeguards—I am trying to answer both questions—it makes it very clear that we share this information when certain conditions apply, such as exit or restriction, or we need the relevant actions, which would be the prevention and detection investigations for economic crime. Those safeguards are built into the Economic Crime and Corporate Transparency Bill.

In GDPR you already have safeguards in place. The first safeguard is: do we have a legitimate interest to share? That is precisely my point, Minister, about our needing to have legitimate interests to share—prevent all crime, not just fraud. Then you have a necessity limb to this. Is what we want to share targeted? Is it proportionate? Is there a less intrusive way? From a law enforcement perspective, we look at whether our actions are proportionate and collateral intrusion. There is a balancing act sitting there as a third limb, on ensuring that the legitimate interest of the public is not unduly overridden. I actually support the fact that there are safeguards in GDPR; I think that is the right thing to have. I support the fact that we need to meet those to be able to share information, but in doing so in that particular space, we need to be able to have sufficient breadth to be able to share across all economic crime and not just fraud.

Q25 Jackie Doyle-Price: That is very helpful. It feels to me that we have got to a position with GDPR where the practical implementation has gone beyond that safeguarding, actually, but we could tackle this by, perhaps, a much fuller statement and guidance about how we expect people to respect the protections but also the obligations that exist in terms of tackling crime.

Nigel Kirby: I think it would be very helpful to have, on the obligations, clear guidance from somewhere like the Information Commissioner's Office—it has got good guidance, to be fair—as we move through this. Should the Bill be enacted and become legislation, guidance across the industry and from the relevant Government sectors or law enforcement sectors on how we do this and come together in the same way as we came together through the Bill, would be important and give clarity, because, as I am sure you are aware, Minister, there are

different interpretations of things, different views and different risk appetites. That is normal in business. The views, legal interpretations and risk appetites will always be different, but where there is guidance to help us through this, with a positive intent from Parliament, that is always really helpful.

Q26 Dame Margaret Hodge: That has been really helpful on the information. I think that a slight amendment to what we are doing would help the GDPR issue.

I want to take you back—I could not quite hear what you said to Alison—to the SARs regime, if I may. It may not be your area of expertise, but it is a very important instrument for informing the enforcement agencies of where there may be a problem. The system is clearly broken—hundreds of thousands of SARs are landing on the desks of enforcement agencies. And we had the idea that they could be put into categories—risk categorised. I wonder whether you are able to comment on that at all, because if currently there is just a tick box—you send off your SARs and you have done it—too often the banks then carry on doing business with a suspicious person. Is there room in the Bill for doing something more on that regime, to ensure that the enforcement agencies are more effective in rooting out economic crime?

Nigel Kirby: I think the SARs regime and the Proceeds of Crime Act 2002 itself actually need—well, not necessarily to be turned upside down, but to be looked at as a whole. I think an individual focus just on some aspect of SARs probably would not change the system in any particular—

Q27 Dame Margaret Hodge: So you think SARs are okay.

Nigel Kirby: Just to be very clear, I am here from Lloyds Banking Group; I will answer this question from my former role at the NCA—from that perspective. SARs do have huge value in what they do; the idea that they just go to a box and are not used is not entirely correct. One of the things the UK has done with SARs, which is world leading and others are quite jealous of, is that they are accessible to a wide range of investigators. It is not about following each one up. There is a database. A wide range of financial investigators can see them and they are held there for six years, as legislation allows. So there is a huge use there.

Also, Dame Margaret, we need to think about this. There is the SARs regime and there is the SARs reform work that is being led; investment is going to be put forward there. I would suggest that we need to see what differences the SARs reform makes first.

Q28 Dame Margaret Hodge: Okay, I hear that. I have one final thing to ask. Looking at your background, I see that you have spent a lot of time in the public enforcement realm. From that experience, and looking at the Bill today, do you think that there are any glaring gaps that we ought to be reflecting on?

Nigel Kirby: Reflecting back and particularly focusing on this area, as I am sure you do, we need to build and are building on the public-private relationships we have had. One Member mentioned Singapore and Holland, but actually, from the perspective of a private-public partnership, how we operate together and particularly the joint money laundering intelligence taskforce, we are seen as world-leading in that space. There is something there about building on that as we move forward and bringing in other sectors, which I know the NCA does. In this particular space, the enablers, as they are sometimes referred to—the telcos, the ISPs, the social media companies—being brought into that public-private partnership and building on what we have is important.

The Bill brings forward private-private relationships, and I think that is important. Hitherto, the information-sharing provisions have all relied on the NCA gateways. There is a throttle there, in terms of capacity. Widening that out so that private-private can share and be the frontline, in many ways, to help to prevent and detect is an important way forward.

Broadening out, there are a couple of elements in the legislation that we need to look at. For us, one is about friction in the system. We have a very quick payment system in the UK; when you pay, you press the button and off it goes. That is something we have got used to as a public and as a banking industry. It is unhelpful when you are looking to put legitimate targeted friction into a system to temporarily stop what I will call economic crime, because it is not just fraud, although it includes that.

Q29 Dame Margaret Hodge: So crypto is a bad thing, is it? It goes very quick. There is no friction.

Nigel Kirby: Respectfully, I think that is a different question.

You asked me to put my other hat on, Dame Margaret. Looking at the scale of fraud—you know, you have got it here; you are familiar with it—and the number of victims and the cost to the UK, it is time for the UK and those with the power to do so to either think about fraud as a strategic policing requirement or, going even further, ask whether it is now a national security threat. I do not just mean with that label—that is really important. You can put a label on these things, but if it could be classed as a national security threat and have the available resources brought together from our national agencies and national policing, that might have a greater impact for the public.

Q30 Stephen Kinnock: Thank you, Mr Kirby. You have used terms such as "world-leading" and spoken quite positively about what is happening in the UK. I have to say, as an interested observer, it does not look like that to me. London has generally become known as the laundromat for dirty money, particularly from Russian oligarchs and others. Money laundering prosecutions have dropped by 35% over the past five years in the UK. In March 2022, the budget of the NCA's international corruption unit was cut by 13.5% to £4.3 million, leaving corruption investigators massively outgunned by the oligarchs.

I have two questions. First, I am trying to understand why you have this sense of optimism, because it looks like a pretty dire situation to me. Our enforcement agencies have been starved of the resources and capabilities they need. Secondly, you have had a long career in the NCA and in enforcement; I am sure you are still in touch with some of your former colleagues. If you had to define the resources they need, what extra would they need to be able to turn this situation around? It would be great to hear from you on that.

Nigel Kirby: For clarity, I used "world-leading" specifically in reference to private-public partnerships and what we are doing for voluntary information sharing. Look at the joint money laundering intelligence taskforce and the facts in that space: it has supported 950 investigations that have led directly to 280 arrests, with £86 million secured. There are some hard figures around here that are different. When I was in law enforcement, we had law enforcement from other countries coming to ask how we did it, including Singapore and Holland. I am in the private sector now, and we have private sector colleagues coming to ask us how do we do that part. That is just a part of the ecosystem that is important—

Stephen Kinnock: Point taken.

Nigel Kirby: If I misled you or you took it that way, that was not intended.

On your question about if I were still there, I am sure that Graeme Biggar, the DG of NCA, will have plans for what that could look like. When I was there, we certainly put forward evidence-based propositions such as, "If there were x amount of funding, these are the extra capabilities we could bring and this is the impact we believe it could have." I am afraid my contacts are not close enough now to know the detail of that.

Q31 Stephen Kinnock: Very diplomatically put. Would you agree that the Bill will not be worth the paper it is written on if the enforcement agencies are not properly resourced to do the job?

Nigel Kirby: I fully agree that we need enforcement to be properly resourced with the right capabilities to be able to deliver what it is asked to do.

Q32 Liam Byrne: Just to crystallise this, in your first answer, you described quite a simple layering exercise of money moving through five different banks, and you said that was a difficult problem to stop. Does this Bill help us stop that problem that you just described?

Nigel Kirby: Well, it does not stop that in the UK because our financial system launderers are in there, but what we can do is to prevent them from continuing to abuse the financial system. Take the example I gave with the five other banks—four were sending money—that were involved with Lloyds. The Bill will allow us to have a conversation with the four banks that were sending money into our companies, and to say "In relation to our responsibility for understanding due diligence, money laundering and so on, can we share information on those four companies so we can better understand those flows from those companies?" That is important, because some of them may have been legitimate and some may have been illegitimate, but that will help us to define the good from the bad in that particular space. It will also act as an alert trigger for those other four banks to have a look if they have not done so already.

An intelligence-led approach would say, "Lloyds has a concern about these four companies" and it could look further into the matter and do an investigation into its own relationship with its customer. The other element on all that money that came through to us—it was in the millions—that went out to a fifth bank, which I will call bank F, is that we could alert that bank about our money laundering concerns, provided we had exited those three companies, which we did. If that bank had not already picked it up with its transaction monitoring, it would have an intelligence-led trigger to be able to do its own investigations, and to stop that and report it to the authorities.

The final and important part of this is the indirect part—we call it the utility. The ability to better share this information for others is important because. If all those companies were exited out of the financial system by the five banks involved, it is highly likely that they would go on and open up accounts with other banks. This Bill gives us the opportunity to be alerted to that and to take the appropriate action and due diligence that we need.

Q33 Liam Byrne: The second problem that is often described by banks to me is that they have to spread their compliance resource very thinly across a large customer base, rather than focusing it on a smaller group where they suspect there is more harm at work. Is that a scenario you recognise, and does this Bill help you focus compliance resource on the potential high-harm customers who we should be worried about?

Nigel Kirby: It is an important point in terms of focusing on risk. We are having a conversation at the moment in industry with law enforcement and a regulator about how we can define where the high priorities are and how we can focus our resources on them, while meeting regulatory requirements and the law enforcement perspective. It would be helpful—we refer to it as dial up, down down—in terms of resource to be able to move to a space where our voluntary discretionary resource could be targeted in exactly the way you suggest, because there is a lot of voluntary discretionary resource in this space.

Q34 Liam Byrne: But this Bill does not help you in that squaring of the circle.

Nigel Kirby: Not in the sense of prioritising what the highest threats are and where we should be. That is to the best of my knowledge. Just for clarity, I am not familiar with every aspect of the Bill.

The Chair: We have literally one minute.

Q35 Seema Malhotra: I have a question about automatic strike-off procedures for companies that may have bank accounts with you and where that company may have been involved in economic crime and then is automatically struck off. Do you have concerns about that process and whether there should be reform?

Nigel Kirby: I think, with respect, that "automatic strike-off procedures" are your words, not mine. I used the fact of us taking an approach and considering whether to exit—that might be a similar thing—a customer. We take this really seriously. We look to understand whether we have economic crime concerns about those consumers. There is a range of things that we can do in that space. The ultimate one is about exit. We would exit that relationship, which is contractual, so we are able to do that. But there are other things that we do, and one is actually to speak to the customer and understand that transaction. We see some unusual transactions, but we have a conversation.

Seema Malhotra: It is more about Companies House automatic strike-off—but they might be your customers.

The Chair: Order. I am terribly sorry; we do have to leave it there. I must cut it off on the dot. Mr Kirby, thank you very much for joining us.

Examination of Witnesses

Andy Gould and Arianna Trozze gave evidence.

10.36 am

The Chair: We will kick off. You are very welcome, witnesses. Thank you for joining us. Would you be so kind as to briefly introduce yourselves and your positions?

Arianna Trozze: Hello everyone. My name is Arianna Trozze, and I am a PhD researcher at University College London. I look at detecting and prosecuting financial crime involving cryptoassets, and for the past year I have also been advising the Home Office on a part-time basis on technical aspects involving cryptoassets in relation to this Bill.

Andy Gould: Morning. My name is Andrew Gould. I am a detective chief superintendent with the City of London police. My job is to run the cyber-crime programme for the National Police Chiefs' Council, which is focused on building capacity and capability across policing.

The Chair: Thank you. We will go straight into questioning.

Q36 Stephen Kinnock: Thank you very much. First of all, I have a question for you, Mr Gould. The national fraud policing strategy states that the police's response to fraud is delivered by local forces, but capability across those forces varies widely. It mentions the regional organised crime units being very limited in their capacity. Do you think that that situation has improved since 2019, when the report was published, and could you say a bit about what extra resources the ROCUs need?

Andy Gould: Sure. Fraud is not really my area of responsibility—I am focused very much on computer misuse act offending—but yes. I know there has been significant additional resource put into the ROCUs for fraud in the last couple of years. Is there enough capacity to meet the demand? Probably not. What policing probably needs to do is take a slightly different approach. Rather than trying to investigate those volume crime offences, it should focus more on those organised crime groups or individuals that are doing the most harm. That is the kind of pivot that policing is trying to make, in terms of being more proactive. I know Commander Adams is giving evidence this afternoon, and he will be able to tell you more about that.

Q37 Stephen Kinnock: Thank you. I have a question on cryptoassets. Do you think, broadly speaking, that the enforcement agencies have the expertise that they need to deal with the economic crime dimensions of the cryptoassets issue?

Andy Gould: Yes, I do. I think we have got the capability, but what we lack is capacity. The capability we have got today does not necessarily mean we will be able to maintain that capability tomorrow. We have invested, through the national cyber-security strategy and the programme through Government. We have got about an extra £100 million that has been invested over the last four years or so, building capability across policing. Some of that money we have effectively taken into crypto, so that cyber money is being used to cross-subsidise wider policing. We have created what we describe as cryptocurrency tactical advisers across the whole of policing. There are now officers in every force and every regional organised crime unit who are trained and equipped to do that. We have nationally procured the investigative tools to enable them to progress the investigations, and we have a national storage platform to store that once we have seized it.

We are in a position where we have actually seized hundreds of millions of pounds worth of cryptocurrency assets within the last year or so. The challenge we have is that it is getting harder and harder to do. The assets themselves are becoming more diverse and more technically complex, so our officers are in a bit of an arms race trying to keep up.

On the tools that we use, you might have one supplier that is brilliant on Bitcoin but not so good on another asset class, so we need more than one investigative tool to be able to investigate effectively. That is very expensive. One of the providers is currently quoting $60,000 to $80,000 per licence. That is unachievable, or unsustainable, for policing. We need to procure nationally for everybody, so we have an 80% discount on our current investigative tool, taking that approach.

The big worry for me at the moment is not just the technology changes and whether we will be able to maintain that level of resourcing and expand the capacity across policing; we have created a real staff retention problem. Because crypto is an emerging market, some of the best expertise and understanding of crypto in the UK sits within policing. We have been investigating cryptocurrency since 2015 or 2016. One of my sergeants has just been offered 200 grand to go to the private sector. We cannot compete with that. That is probably the biggest risk that we face within this area at the moment.

Q38 Stephen Kinnock: Thank you. Ms Trozze, I know that you are a specialist on crypto, so would you like to add anything to that?

Arianna Trozze: I would echo Andy's point about the difficulty of tracing certain cryptoassets and investigating certain chains and things like that, and how this is evolving rapidly in competition with the existing providers and the blockchain services themselves. It gets more and more difficult to investigate as time goes on. You need more and more capacity building and investigative tools. At the same time, the crypto companies and the blockchain companies are seeking to develop their technologies in ways that will evade that detection, so it is a constant race between the two sides to be able to effectively investigate and prosecute these crimes.

Q39 Alison Thewliss: Leading on from that question, we are putting a lot of provisions in the legislation. Is the legislation sufficient to keep pace with those technological changes?

Arianna Trozze: One of the key ways that legislation can future-proof itself in the face of this rapidly developing technology is via the definitions. I think that the definition

of cryptoasset in the Economic Crime and Corporate Transparency Bill is sufficient to do that. Probably most importantly, the inclusion of cryptographically secured contractual rights means that the definition will cover smart contracts, which is really the technology that underpins all the major advances in the space of, for example, decentralised finance and non-fungible tokens that have taken place, and that we expect to continue to develop in the coming years. Furthermore, the ability to amend those definitions via secondary legislation is clearly a positive, because in the event that something slips through the cracks and develops in a way that we cannot anticipate, it will make it more efficient to change them.

Q40 Alison Thewliss: Are the measures in the Bill sufficient to protect consumers from being victims of economic crime via crypto?

Arianna Trozze: Because they are very clear that they include cryptoassets, it really makes the rules clear for everyone in the industry. Consumers then know as well what rights they have. My view is that it obviously cannot do everything, but the fact that there are provisions for victim compensation goes a long way to also protecting consumers. Obviously, it does not prevent the crimes from occurring, but it helps them to recover the losses.

Q41 Alison Thewliss: Briefly, how do you feel the measures in the Bill relate to the other measures around regulation in the Financial Services and Markets Bill? I am conscious that the two Bills are going at the same time.

Arianna Trozze: I cannot really speak to that. I am very sorry about that.

Andy Gould: I cannot either—sorry. I have not looked at that.

Alison Thewliss: That is okay. No problem.

Q42 Jackie Doyle-Price: When we talk about things like cryptoassets, it is difficult for lay people like me—I am sure I am not alone—to envisage what exactly we are talking about. I recognise some of the operational sensitivities under which you are working, but would it be possible for you to give us an illustration of how cryptoassets have been used to disguise this activity?

Andy Gould: Probably the most obvious area would be around ransomware, which is if you are an organisation and you get hacked and attacked and then lose access to all your files or systems, and then get a demand from a cyber-criminal saying, "Okay, if you want to get access back, you have to pay"—basically, an extortion demand. That extortion demand will virtually always be in cryptocurrency, because there is a view that that is harder to trace.

Depending on the kind of cryptocurrency, the traceability varies. Effectively, a lot of the technology that sits behind cryptocurrencies is based within what is described as the blockchain. Arianna is much better at explaining this than me, but the blockchain is effectively a public ledger, if we are talking about Bitcoin or something like that. We can see all the transactions. It is like your bank account or NatWest or any other bank doing its transactions in the public space—everybody can look at them. It is effectively decentralised and very public, so there are real benefits in that. The anonymity comes from not knowing who is sending what or who is who, in terms of the bank accounts—the wallet equivalent.

That provides opportunities to follow the money, but, although you might be able to see where the money goes, you will not necessarily know who has sent it or who has received it. There are other investigations you would need to do that. And there are tools—mixing services or exchanges—that will jumble it all up and then send it elsewhere, and you will not be able to see what has come in compared with what is going out. That is why criminals like to use it—because, as they see it, it covers their tracks effectively.

Arianna Trozze: One way to make it a bit clearer is to situate cryptocurrency money laundering in the traditional phases of money laundering. When we talk about money laundering, we tend to talk about three specific phases—placement, layering and integration. In the crypto space, placement may look like someone depositing their Government-issue currency into a cryptocurrency exchange, and exchanging it for cryptoassets, or potentially using what is called a fiat on-ramp to buy cryptoassets using their fiat currency. They may also use something like an over-the-counter broker, which may allow them to buy cryptoassets using cash.

Then, the layering process follows, which is kind of what Andy was talking about, in terms of trying to obfuscate the origin and trail of funds. There are a lot of different tactics that the criminals can use to do that. As Andy mentioned, they may use mixing services, to try to break the chain. They may create thousands of different cryptocurrency wallets and accounts and transfer the funds among them in order to make it more difficult to trace. They may exchange them for various different types of cryptoassets, including privacy coins, which we, again, have a lot of trouble chasing, although there have been advancements in that regard. Finally, they may move to completely different blockchains, using what are called blockchain bridges, and that further makes it more difficult to trace—as Andy mentioned before, different providers have different capabilities and different expertise in terms of which chains they specialise in and which assets they are able to trace. That is something else that they may do to hide that trail of funds.

Finally, we have the integration process, which is criminals using those now-cleaned funds for mainstream economic activity. We know that sometimes they may seek to keep those funds in cryptoassets in an attempt to further their gains, speculatively investing in the market; or they may, again, use one of these exchanges or what is called a fiat off-ramp to transfer their cryptoassets back into pounds or any other currency.

Q43 Jackie Doyle-Price: It is really the complexity that is the barrier, is it not? The actual use of cryptoassets of itself brings an additional complexity, so it is clearly an ideal tool for those who are up to no good.

Arianna Trozze: Yes, and as it is such a quickly developing technology, there are constantly new ways coming out for criminals to use the technology for various purposes. Again, it is a rush for law enforcement and investigative companies to try to keep up with this.

Andy Gould: To give you a sense of the scale of the challenge, there are thousands of different forms of cryptoassets or cryptocoins in existence. We have to

learn to use all the ones that the criminals are using. We can only do it with the private sector. There is no way we can invest in or have the skills in-house to be able to develop all of those tools for all of those different asset classes, so we work really closely with all the big private sector companies to build that capability. It is why we do big open national procurements—because that is the only way it is affordable.

Q44 Liam Byrne: Is cyber-crime and cryptocurrency-based crime growing quickly?

Andy Gould: It is really hard to say, because it is so hard to identify or report at scale. However, I would say yes. If you talked to all of the big cyber-incident companies and the threat intelligence companies about what we are seeing, in terms of reporting, then yes, everybody would say that it is rising. Certainly, the crime survey for England and Wales does.

Q45 Liam Byrne: What is the criminal structure in this market? Is it teenage hackers in their bedroom or sophisticated organised crime groups?

Andy Gould: It is both. There is a real mixture. You can have your sophisticated organised crime groups, with some of those having a bit of a crossover with hostile state actors, which makes that more complex to manage. You therefore have a lot of overseas threat at the higher end, but during the pandemic we also saw a shift of mainstream, traditional—if that is the right way of describing them—UK-based criminals moving into cyber-crime, because a lot of the tools are readily available on the internet and are quite easy to use.

Q46 Liam Byrne: You just said that some of those organised crime groups have connections to hostile states—presumably such as North Korea, Iran and Russia.

Andy Gould: Yes, that is right.

Q47 Liam Byrne: So is there now a blurring of a national security threat and economic crime?

Andy Gould: Yes, definitely.

Q48 Liam Byrne: And are we investing enough in tackling that kind of crime?

Andy Gould: I think that a lot more has been invested. I think—

Liam Byrne: That was not the question. Are we investing enough?

Andy Gould: Well, as a police officer, I will always say that you are never investing enough.

Q49 Dame Margaret Hodge: Lots of us are trying to get our brains around this. I had a session yesterday with a whole load of people in the crypto industry who tried to convince me that there is actually better transparency because it is open—you can go in and see it—and there ought to be a way in which, with the right algorithms, you could follow the money more easily than in other ways. Is that true? Were they conning me, or is that vaguely true?

Andy Gould: No, there is definitely an element of truth in that. If you have a public blockchain, you can see where it is moving, and that is very open—Bitcoin is the most obvious open public blockchain and the most popular crypto. However, that does not mean that you necessarily know who it is that starts and finishes. That is the issue, and with a lot of the different criminal services available, it is becoming harder and harder to manage. It is becoming more tricky. So, the answer to your question is probably yes and no.

Q50 Dame Margaret Hodge: We welcome the Minister's attempts to start bringing this into a regulatory framework. However, looking at the other aspects of money laundering and economic crime, the so-called enablers are often the bad guys. In this world, those who establish a new form for crypto are presumably the ones who, if they are not properly regulated and supervised, could create a system for facilitating economic crime, fraud and money laundering. I do not think that we have proposals in here, really, for the supervision and regulation, have we? Are those badly missing?

Andy Gould: The Financial Conduct Authority has taken on regulatory powers in this space. I am not an expert in that area, but that is looking pretty promising. A lot of UK-based entities that were offering those services are no longer able to do so, so there has definitely been a clean-up of the market in that space, which is positive.

The challenge is that international regulation, and a lot of the recent work we have seen in that space, has driven a lot of overseas exchanges and providers, which might have been operating in a bit of a grey space, shall we say, to suddenly look to become more legitimate and comply because they want to come into the mainstream financial system. I would use the analogy that the tide is going out on a lot of the more criminal providers. They are effectively being left as "clearly not engaging, clearly criminal", and a lot of those that may be operating in the grey space in international jurisdictions are becoming more and more legitimate as they clean up their acts.

Q51 Dame Margaret Hodge: This is really Liam's question, but, because it is digital, the answer must be global, must it not?

Andy Gould: Absolutely, yes.

Q52 Dame Margaret Hodge: And that is really hard.

Andy Gould: Yes.

Q53 Seema Malhotra: I want to follow up on what you were saying about how you can follow the flows, but you do not always know who is sending and who is receiving. I want to understand a bit more about crypto accounts. I understand that you do not need an account in order to make a transaction, but if you do have an account you can see who is making transactions. Is there more that can—or needs to—be done to say that everybody must have an account? Is that practical and how could it happen? Secondly, what is the current level of identification and verification checks when setting up a crypto account, and what level should there be?

Andy Gould: The average member of the public using cryptocurrency will probably be using an account through one of the legitimate exchanges. They will go through the whole "know your customer" process that they would go through for a bank. Regulation pretty much covers that; I think we are in a good place with it. It is

the criminal exchanges and criminal service providers that regulation would not affect. You would not be able to build an infrastructure that stops them being able to create their own wallets, as you could for those accounts with what are effectively crypto banks.

Arianna Trozze: There has been research that some of the KYC processes, especially in some of the higher-risk exchanges, are quite easy to fool with fake documents and other such things. There are companies serving UK customers that are still not registered with the FCA and do not meet its KYC or AML requirements, despite its best efforts. For example, none of the Bitcoin ATMs operating in the UK is registered with the FCA, even though they are supposed to be, and they tend to have quite lax KYC requirements. They may require you to put in a phone number. Some of them have more requirements, but whether it is a rigorous process remains in question.

Q54 Seema Malhotra: What more could be done about that?

Arianna Trozze: In my view, the only thing would be more enforcement efforts against non-compliant companies. I do not know how practical that is, or what kinds of resources there are to address the problem, but to me the only way forward is to make sure that those companies and operators know that it is not acceptable to be working and serving UK customers without a licence.

Q55 Seema Malhotra: What are the consequences for them if they do that?

Andy Gould: I think the FCA has prosecution powers and enforcement and regulatory options, but I could not say what it is doing about that.

Q56 Seema Malhotra: Do you know if there are cases where it has used those powers?

Andy Gould: I do not know. They only came in earlier this year, so I would be surprised if the FCA has got to the stage where it is able to exercise them in terms of investigation.

Q57 Jane Hunt (Loughborough) (Con): Mr Gould, to follow on from that important point, I understand that the Bill removes the need for powers of arrest before you can do search and seizure. Can you explain the impact of that? Will it be useful for reducing the number of victims once you have spotted an issue happening?

Andy Gould: Yes, definitely. That is a huge benefit of the Bill; it is one of the provisions that we have been asking for. Imagine a scenario where you execute a search warrant on criminal premises: you go in and you can see stolen property, but at the moment, if they are not there, they are not under arrest and there is no existing investigation. You then have no power to take that crypto under the Proceeds of Crime Act 2002. So yes, that is a big step forward for us.

Q58 Stephen Kinnock: Thank you for giving me another go. I have two quick questions. If you had a blank sheet of paper and you were able to amend the Bill in the cryptoassets space, what would be your No. 1 amendment to improve it? Secondly, Mr Gould, do you also look at counter-terrorism within your brief?

Andy Gould: No.

Q59 Stephen Kinnock: Okay. I was going to ask something about counter-terrorism, but I will not if that is not your area. So my only question is to both of you: if you had an opportunity to amend the Bill, what would you do?

Arianna Trozze: I need to think for a moment.

Andy Gould: We are generally very happy with the provisions of the Bill. One area that we might want to look at is storage of the assets. Imagine you have £100 million-worth of cryptocurrency. That is really expensive to store, and there is always a security risk around where it is stored. If we were able to turn that into cash straight away at the point we get the restraint from the magistrates court, and that that was a standard power, a lot of that cost and security concern would be taken away. That would be one area where we could improve.

There is an existing power under POCA, where you can go to the Crown court and make that application, but that can be contested by the defendant. There is a cost associated with that. If we had a standard power to do that, I think we would be a bit happier, but we are generally very happy with the provisions in the Bill.

Arianna Trozze: I would echo that I generally think the Bill goes far enough—as far as is technologically possible at this time. I do not think there is anything that I personally would amend at this time.

Q60 Stephen Kinnock: Apart from turning cryptoassets into cash in the way that you have described.

Arianna Trozze: I see both sides of that argument. Obviously, if assets are transferred into cash and then the original assets significantly gain value, and if the person with the assets were then found not to be a person of crime, the Government would be on the hook for the change in value of those assets. There are two sides to the argument but, as Andy mentioned, the storage is quite risky and very expensive. I ultimately agree, but I see both sides of the argument.

Q61 Alison Thewliss: As a brief follow-up, do you have any information on how much that cost is likely to be? That would be very useful to us. I appreciate you might not have that figure in front of you now, but it would be useful to have that detail.

Andy Gould: It is quite commercially sensitive, but it could be a large sum—we are talking hundreds of thousands of pounds.

The Chair: Okay, we have come to the end of this session. Thank you very much for joining us.

Examination of Witness

Jonathan Hall KC gave evidence.

11.1 am

Q62 The Chair: Mr Hall, thank you very much for joining us. Would you like to briefly introduce yourself, please?

Jonathan Hall: I am the independent reviewer of terrorism legislation. I also have a bit of a background in crypto from my practice as a barrister, which is why I

was interested in this whole area. I was asked by the Government to feed into some of the clauses as they went through, and I am here to talk about the crypto aspect.

The Chair: Thank you for joining us. We will go straight into questions.

Q63 Seema Malhotra: I will be brief in asking this question, and then I have to leave. Do you think the NCA has sufficient resources to make use of the new recovery powers in the Bill, and do those powers go far enough?

Jonathan Hall: I do not know about the resources of the NCA, but in terms of whether the powers go far enough, I think there are some areas where they perhaps go too far, or at least where I think, from a fundamental rights and individual rights perspective, some attention may need to be drawn. There is the simple question whether you should be able to seize cryptoassets on the basis of the fact that they might be used by terrorists. Of course you should. Then you have the complicated question of how you bring about a seizure regime where assets are not physical. It is one thing if you seize a jewel or some cash, but it is another thing if you are effectively seizing information. What you have here is a very lengthy set of provisions to allow you to do that.

Generally speaking, I think it works, but there are one or two areas I want to draw to your attention. The first, which I think is acceptable but worth thinking about, is that the power is a power to seize not just cryptoassets but crypto-related items. In practice, you are not seizing a thing; you are seizing a code and that can be written down on a bit of paper or on a computer. What these provisions do, unlike all the other seizure powers that say you can seize the jewel, the cash or the contents of a bank account, is that they allow the police to seize any item, which could be a computer, or a piece of paper. So, it is quite a wide seizure power. I think it is kept effectively within bounds, but it is something that is worth drawing attention to, which is different from other aspects of seizure in this field.

The next point is that you have to be able to convert crypto and there are several reasons for that; one is because the prices may go massively up or down. Individuals whose assets are the subject of seizures may never be prosecuted—and this is a civil remedy—and, in fact, no final application for forfeiture may ever be brought. That is particularly true in the context of terrorism, because often what counter-terrorism police will want to do is disrupt the transfer, but they will not necessarily want to go on and apply to forfeit. The figures from last year show that there is a disparity between the number of accounts that are frozen and the amount of money that is finally the subject of forfeiture.

The Government did listen to my views on this issue. It is important that the Bill has provisions such that both the police can apply to convert the cryptocurrency into, say, pounds sterling, and that it is also open to the individual from whom it is seized, who might say, "Look, I bought this crypto. It's gone massively up in value. You're never going to apply to forfeit this. I don't want to lose out on the rise of value." There is provision in the Bill for the individual to go to court and say, "I'm a person from whom the crypto has been seized. Please can you convert it?" That will be decided by the court, but it is good that that provision is in the Bill; I think it works.

Is this too boring and long? I mean, there is a third bit, which I think is the most difficult bit. It is the power of a magistrates court to require a UK-connected wallet provider to freeze the cryptoassets and, even more significantly, to require that the UK-connected crypto wallet provider should actually pay the money over to the court. It is slightly in the weeds, but what the Government have done—and I understand it—is to try to be quite novel. They are really trying to push the law here, because they realise that many of crypto wallet providers will not be based in the UK, but this comes with a consequence regarding how the Bill is currently worded. I will just give you the bit that I think may need a bit of attention; it is clause 10Z7B—

Q64 Dame Margaret Hodge: Can you give that again?

Jonathan Hall: Yes, I will. It is clause 10Z7B(7).

Q65 The Chair: Have we a page number?

Jonathan Hall: I am not sure I have got the same document; I have got the Public Bill Committee document for 30 September and it is on page 10.

Q66 The Chair: It might be on a different document. I think we might have to move on then.

Jonathan Hall: I will just flag it up to you. It defines a UK-connected cryptoasset service provider. It includes a provider

" which…is acting in the course of business carried on by it in the United Kingdom."

Well, that is completely fair enough; if they are carrying on business in the United Kingdom, they should be subject to court orders. However, it then has this provision:

"has terms and conditions with the persons to whom it provides services which provide for a legal dispute to be litigated in the courts of a part of the United Kingdom".

I will just put the flag up and then allow the Committee to move on. That is quite a wide extension of UK jurisdiction over companies that may be based abroad and potentially over victims who may have claims overseas.

The Chair: Thank you. I will bring the Minister in next, which may be helpful.

Q67 Jackie Doyle-Price: Thank you. Forgive me, but you are speaking very legally, which is obviously why you have been invited here. We want to try to make this live, and you obviously bring considerable counter-terrorism expertise. Can you give us some examples of how the Bill will enable law enforcement to go after and combat terrorism?

Jonathan Hall: Let us imagine that counter-terrorism police have intelligence that there is an Islamic State cell that has been fundraising in Birmingham, and they are going to try to transfer the funds that they have managed to raise to an active cell based in Syria. Their plan is to do that by using Bitcoin. Let us imagine counter-terrorism police had intelligence that that was about to happen. They could raid the premises where the UK-based cell was operating. They could seize a bit of paper on which the crucial key is written down, which would allow the

transfer of the funds to take place to Syria. They could then use that key to grab the cryptoassets—let us say it is £1 million-worth of assets that are about to be converted, or have been converted, into cryptocurrency—and transfer the cryptocurrency to a police-controlled wallet or to another provider who they trust.

That money, which would otherwise have gone out to Syria to buy guns and so on, will then be seized by the police. If the police have evidence to do so, they could in six or 12 months' or up to three years' time, go to a magistrates court and say, "We can prove that this cryptocurrency was going to be used for the purposes of terrorism" or "It was the resources of a proscribed organisation, Islamic State. Can you now please order that the money be seized and transferred to the Treasury?" Does that help?

Jackie Doyle-Price: Yes, not only is that a brilliant explanation that brings this to life, but it is a great plot for a film.

Jonathan Hall: It is real life. There was a man called Hisham Chaudhary who was convicted last year of doing more or less that.

Q68 Jackie Doyle-Price: Exactly, and this is what we are talking about. Do you think that what we have in the Bill will stand the test of time, given that ultimately this kind of criminal activity is always trying to get one step ahead of the law? Can we be confident that what we are enacting here will be future-proof?

Jonathan Hall: We can never be confident it is completely future-proof, but it is necessary and definitely a very strong step in the right direction. As I say, I have one reservation about overseas companies where I think it may go a bit too far. It may just be a question of deleting one part of the provision I read out to you. In general, it is a good step.

Jackie Doyle-Price: We will have a look at that. Thank you.

The Chair: I think the number of the page you are looking for is in the amendment document on page 47 and it is new schedule 1. I think that is what you were referring to, Mr Hall. I am going to move on anyway.

Q69 Alison Thewliss: This is obviously a fast moving area and a lot of expertise is required. Do the enforcement authorities have sufficient expertise to keep pace with this? We heard from a witness earlier that their experts are being snapped up by industry because they are able to offer more money. Does that make it difficult to then enforce the provisions in the Bill?

Jonathan Hall: In the counter-terrorism world, there is an open question about quite how much this blockchain technology will be used by terrorists. There is quite a lot of excitement about the possibility of its use, but the jury is slightly out about how much it is, in fact, being used. I cannot speculate why that would be. Counter-terrorism is a well-resourced part of police business, so I would expect that there would be specialists who would be willing to stay because they are quite highly motivated; outside counter-terrorism, I do not know. I was very struck by the point about the £200,000 transfer fee.

Alison Thewliss: Thank you. I will leave it at that.

Q70 Dame Margaret Hodge: I want to follow on from that, because I am taking it a bit wider than crypto in two areas. After the 7/7 horror, we put our all into counter-terrorism and we now have a strategy that is well resourced, and can respond to and has responded effectively to terrorism threats down the years. When I look at this, I feel that Ukraine ought to be our 7/7 moment in relation to dirty money. I wonder whether we are ambitious or comprehensive enough. I take the point about resources; there is no point doing anything if you do not have the resources. However, are we doing enough here to give you the confidence that we can really start turning around this big tanker?

Jonathan Hall: Do you mean the Russia-Ukraine aspect?

Dame Margaret Hodge: Ukraine gives one a sort of focus on the worst aspects of dirty money, but are we really being as comprehensive as you were when you did the counter-terrorism stuff there?

Jonathan Hall: The one thing that I think would make all the difference would be to resource Companies House. I follow Graham Barrow on Twitter—I think he is giving evidence—and occasionally I look at the overseas entities register, and, as he has pointed out, there are these anonymous chip shops in Barnsley, which have about 57 British Virgin Islands companies attached to them. It seems that that is the low-hanging fruit: having a well-resourced Companies House that can tackle the entries, verify them and prosecute them.

Q71 Dame Margaret Hodge: I will ask you just one more question, which is a little bit off piste. The Bill puts new duties on lawyers to ensure that they can be fined if they engage in work that facilitates crime, or they fail to prevent crime. I gather the Bar Council is a bit iffy about this; I wondered whether they thought it was interfering with access to justice. Where do you stand on that? Lawyers certainly come up constantly as facilitators, giving opinions that underwrite either unlawful behaviour in the tax field or illegal behaviour elsewhere. I do not know if you can help us on that—it is a bit off piste.

Jonathan Hall: The funny thing is that there is a principle in law that, if someone is giving advice to someone in order to commit a crime, legal professional privilege does not apply. It is quite hard to find examples of cases in which that doctrine has been applied, so I do not know whether it is about law enforcement having the confidence, when they have a lawyer who is deeply engaged in advising someone to break the law, to say, "We don't care that you are saying this is privilege because we are going to run the case and say it is for a criminal purpose". Beyond that, I do not know. I am a lawyer and I completely support maintaining access to justice—of course I do. But you are also completely right that lawyers and trust companies are at the heart of this issue, and I am afraid there are professional enablers.

Q72 Stephen Kinnock: This is the same question that I asked our previous witnesses: if you had the opportunity to amend the Bill, what would you do? You have flagged

[Stephen Kinnock]

up one area in which you are worried the Bill goes too far, so obviously we need to look at that, but my question is more about how you would make it go further to achieve the outcomes we are looking for in terms of the role that crypto plays, particularly in financing terrorism.

Jonathan Hall: I have not got an answer beyond the one I gave before, I am afraid. I am sorry; I have not thought of a positive thing. I would just remove that subsection (b) from the definition of UK-connected cryptoasset service provider.

Q73 Stephen Kinnock: I am not sure if you were in for the previous session, but our witnesses talked about the need to be able to transfer crypto into physical assets or cash. What are your thoughts on that and do you have a sense of what the cost would be? Obviously, the disincentive for doing that is how much it could cost the Government for being on the hook. If it is transferred it into cash, and if there has been a rise in the value of the cryptoasset, the Government are potentially on the hook if that person is found not guilty. Do you agree that that "on the hook" argument exists? If so, it becomes a numbers game, because the cost of storing the cryptoasset is high. What is the net benefit to the Government of either transferring it to a physical asset or continuing to fund the cost of keeping it as crypto?

Jonathan Hall: It is quite a bit step to convert it to fiat currency, or pounds, because you are then interfering with the bet that person has placed on the value of the currency going up. I do not know what the figure is in terms of storage. I am interested, too, in the question of potential police liability. I am thinking about the Sanctions and Anti-Money Laundering Act 2018. As you know, before the Government brought in the suite of changes that allowed urgent sanctions, they were very careful to narrow down the potential liability that the Government might have in relation to sanctions, if they were challenged. I have not given it attention, but maybe it is worth having a look at whether there are equivalent protections for the police. The seizures can be very high in this field—they can measure many millions—so the potential liability of the police could be quite high. We would not want the police to be too disincentivised by the risk that they would be on the hook for damages, if everything goes wrong.

In terms of the balance, it may be that ultimately one or other party—the person from whom the assets are seized, or the police—is going to suffer some sort of loss. The key thing is to make sure that people have access to the courts. The courts will have to generate their own sort of expertise and case law over when you should convert a currency. I can imagine that someone will come to the magistrates court saying, "My assets have been frozen. Now is the time for converting them from Bitcoin into Ethereum", and the court says, "What? How do I determine that?" There will need to be a body of expertise. This is a minor point, but it is something that I support: one of the intentions is to allow quite a wide range of law enforcement personnel to be responsible for the court proceedings, precisely so that you can develop a cadre of people who have got that sort of expertise.

Q74 Alison Thewliss: I want to ask about Scottish limited partnerships, particularly given their involvement in sanctions busting and various other things. Do you share my concern that they can exist in the Companies House register in a sort of zombie form and can be reanimated? Is there more that the Bill could do about that? If the use of SLPs is being tightened up, if you were looking to abuse corporate structures where would you go next?

Jonathan Hall: I do not want to say. The key thing is that I am not a Scottish lawyer, and I am not going to try and opine on whether there is a legitimate use of them. The key thing is basic enforcement. You made the point that there are zombie companies. Well, someone in Companies House needs to follow these things up. I am sure they will, but the resourcing of Companies House is where I would put my money.

Q75 Liam Byrne: We have just heard some very powerful evidence about the relationship between organised crime groups operating in this sphere of crime, and state threats. Have you any other observations about the relationship between economic crime and national security threats as we face them today? Is that a serious problem that we need to be worried about?

Jonathan Hall: It is a serious problem. I would say that the reason we have not faced the wave of mass casualty terrorist attacks in the UK, in contrast to America, is the lack of readily available firearms. That is the key thing. It is why the growth of the extreme right wing and all these ideologies that inspire mass killings, the obsession with Columbine and so on, have not resulted in mass shootings. From a national security perspective, the real concern is the alignment—if it happens—between terrorist organisations and those in organised crime, who do have the capacity to source firearms. That is a really important point.

The Chair: That brings us very nicely to the end.

11.24 am

Ordered, That further consideration be now adjourned. —*(Nigel Huddleston.)*

Adjourned till this day at Two o'clock.