



Industry and Regulators Committee

Corrected oral evidence: Compliance costs in the financial sector

Tuesday 6 July 2021

10.15 am

Watch the meeting

Members present: Lord Hollick (The Chair); Lord Allen of Kensington; Lord Blackwell; Baroness Bowles of Berkhamsted; Lord Burns; Lord Curry of Kirkharle; Baroness Donaghy; Lord Eatwell; Lord Grade of Yarmouth; Baroness Noakes; Lord Reay; Lord Sharkey.

Evidence Session No. 1

Virtual Proceeding

Questions 1 - 23

Witnesses

I: Steve Elliot, Managing Director, Business Services UK & Ireland, LexisNexis Risk Solutions; Nick Van Benschoten, Director, International Illicit Finance, UK Finance.

II: Christopher Woolard CBE, Chair, EY Global Financial Services Regulatory Network, and former Interim Chief Executive, Financial Conduct Authority.

USE OF THE TRANSCRIPT

1. This is an corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.
2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.
3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Steve Elliot and Nick Van Benschoten.

Q1 The Chair: Good morning. Today's hearing is a one-off inquiry into the cost, complexity, efficacy and efficiency of the anti-money laundering and "know your customer" processes, and whether there are ways of making these processes more effective in the pursuit of crime, but less onerous so as to enable companies and individuals to comply more efficiently.

In its report in February, the Kalifa review recommended that the Government facilitate and mandate the sharing of data across various sectors, with open finance as a priority. That recommendation was echoed in the recent report on innovation from Iain Duncan Smith's committee, which also called for a review and an update of GDPR. We would like to look at those two issues today.

I am delighted to welcome our two witnesses for the first session. Steve Elliot is managing director at LexisNexis Risk and Solutions in the UK and Ireland. He recently wrote a report, *Cutting the Cost of AML Compliance*. He is joined by Nick Van Benschoten, director of international illicit finance at UK Finance.

In your recent report, Steve, you state that the annual cost of anti-money laundering compliance for UK financial institutions is £28.7 billion. How did you arrive at that figure, and what makes up those costs? In summary, what is your assessment of the value that we get for those costs in reducing crime?

Steve Elliot: The review itself is one piece of work in a series of reviews where we are trying to understand the impact of regulation on markets in the UK and around the world. That particular review focused on the UK. To get the findings, we interviewed 301 leaders across financial services in the UK: chief compliance officers, money laundering reporting officers and the like. We asked them a range of deep questions about the financial crime and money laundering arrangements in their firms. When arriving at the number, we actually took the median number. We dragged the total costs down to try to truly represent the cost rather than to pick up on the outliers. There are a number of different ways of measuring it, but we took the median.

We found that the costs were extremely high. Our responders came up with a cost of £28.7 billion for the financial crime arrangements that they implement in their firms. We extrapolated across the industry to get to the £28.7 billion. We compared it with the cost of financial crime. We found that the National Crime Agency was reporting that £37 billion is the cost of money laundering in the UK. The cost of complying is very high compared with the risk that is being mitigated. In our opinion, that needs to be changed to allow firms to target more cost-efficiently the true risk that they are trying to address.

The Chair: What is your estimate of the value for money? Did you make an appraisal of that?

Steve Elliot: Value for money can be measured in a number of different ways, but the value for money, in our opinion, is relatively low. Again, you can look at different metrics. The amount of money laundering that has been detected in the UK markets is often quoted as being as low as 1%. The industry is spending £28.7 billion or so to identify about 1% of the money laundering activity. There is a whole host of reasons for that, which I can go into later.

The Chair: Thank you. Nick, would you like to comment?

Nick Van Benschoten: Yes. Thank you for the opportunity of contributing to the inquiry. It is very timely, and it is an important topic. I echo what Steve said. The review included a number of our members in its interview sample. We definitely recognise the billion-pound scale.

We did a narrower review of our members a number of years back, and that was also at the billion pound level. One of our members with a large retail base in the UK estimated that its total cost of financial crime compliance is now equivalent to the total cost of its branch network in the UK, which as an illustrative example echoes some of the points that Steve raised.

With regard to value for money, it is important to look at the opportunity cost. A lot of the cost of these regulations is for activity that is of relatively low utility. Reallocating those costs for better outcomes and more effectiveness is another important part of the debate.

Q2 **The Chair:** To what extent is the problem caused by legacy systems that have not been updated or, if they have, it has just been new software on top of old software?

Steve Elliot: That is a significant issue for the larger firms. They have a number of systems in place against legacy policies or accounts, depending on which part of the market you look at. They struggle to bring all of that together to get a single view of who the customers are. Without that single view, it is difficult to understand the true risk that an individual poses. It is also difficult to run external "know your customer" and money laundering checks against it. The risk is large for large firms, but it is a lot less for smaller firms that have built much more modern and progressive systems. The large firms are seeing their market challenged by the smaller firms, which are a bit more dynamic and able to progress.

The Chair: Steve, if you had done this survey 10 years ago, what would have been the cost then?

Steve Elliot: The cost would have been a lot lower. For various reasons, the market has seen significant increases. There have been increases as a result of the complexity of the regulations that people are now seeking to cope with, and the desire within firms to ensure that they meet compliance obligations. They are giving that greater weight than actually trying to address the outcome, which is to drive down money laundering in the market. They are forced to comply with ever-increasing, complex

regulations, and that is having a significant impact on the cost of compliance.

The Chair: Are you saying that there is more box-ticking but less actual vigilance?

Steve Elliot: I am saying that firms are obliged to evidence the extent to which they are compliant against obligations, and, as the range of obligations increases, more evidence needs to be gathered in order to provide that confirmation. There is very little freedom and flexibility for firms to target money laundering, as opposed to confirming and evidencing compliance.

The Chair: Do you recognise that description, Mr Van Benschoten?

Nick Van Benschoten: I am afraid I do, yes. A number of the recent regulations that Steve referred to were introduced over the last number of years, and they restrict the flexibility of firms to follow the data and to follow the money and target their efforts.

To give you an example of some of the problems we are dealing with, the systems and the monitoring set up by the financial sector produces roughly 20 million alerts of potentially suspicious activity every year. That translated most recently into 460,000 suspicious activity reports to the UK Financial Intelligence Unit. That is only a 2% conversion rate. Once it actually went to law enforcement, the estimates from a number of bodies are that only a very small number of those suspicious activity reports actually contribute to the disruption of organised crime.

Europol's estimates are, overall, that less than 10% of reports by the regulated financial sector are of value to law enforcement. Recently, the director-general of the National Economic Crime Centre, Graeme Biggar, estimated that maybe 10% to 33% of all UK suspicious activity reports were of no value to law enforcement. There is a real problem with the outcomes from this process. The cost of the inputs is a very important point, but the outcomes are increasingly of low utility.

Q3 Lord Allen of Kensington: Good morning, everyone. Steve, I am keen to get behind your report on the difference between the larger and smaller companies, and the impact on costs. I want to understand whether the costs are disproportionately borne by newer and smaller companies, and therefore whether the impact of that affects competition and consumer choice. From your report, with £100 billion of assets under management, the costs are 0.019%. If it is under £100 million it is 2.12%. It looks as though it is 11 times more expensive for the smaller companies as a proportion of their assets under management.

Secondly, what are the unintended consequences of these rules on consumers in bureaucracy and their ability to get good financial services? Are competition and consumer choice affected by these regulations and costs?

Steve Elliot: Thank you, Lord Allen. On the first point about the costs across different scales of firms, all firms, regardless of scale, need to build knowledge of the regulatory environment. Even small firms have to build compliance functions that identify, evaluate, interpret and implement very complex regulatory obligations. That is where a lot of the cost bites for some of the small firms. It is difficult to enter the market from a compliance perspective.

In the larger firms, it is more difficult to change the compliance obligations, because you are steering a much larger organisation and you are wedded to much more expensive and more deeply embedded controls that operate across more complex systems. So, yes, from an understanding of regulations perspective, the cost for small firms is significantly larger as a proportion of their revenue than it is for the large firms, but the picture changes across organisations when it comes to complexity.

To your second question—what it means for consumers—having a lot of barriers in place across operational processes disrupts the consumer experience. If the controls are not effective, it makes it increasingly difficult for individuals to get access to markets, because there are a lot of preventive controls in place. It makes their experience, as they move across organisations, less easy, because there are more disruptive controls at different points across the organisation. Consumer experience is poor, because a lot of the KYIs—the “know your customer” controls—are repeated at multiple points rather than just being done once. So there is poor experience and high cost.

Lord Allen of Kensington: Nick, do you agree?

Nick Van Benschoten: I echo the point about the duplication of checks. The regulatory system allows a degree of reliance between firms that are regulated for anti-money laundering, but that reliance has been successively narrowed to the point that consumers often get repeatedly requested for the same information. Obviously, we will move on to this topic, but technology is one solution, although technology quite often requires quite a lot of complex legal analysis and interpretation of regulatory guidance, which is an area that our industry and Steve and his colleagues are working hard with the Government to improve.

We definitely recognise the complaints from smaller firms that they lack the capacity to keep up with the rate of change. There has been extensive regulatory change management on financial crime for a number of years. The pace has not slowed down. In the UK, there is the added complication of all the institutional and legal change following the exit from the European Union. That has been a particular challenge for our smaller members, but there is also a question about the allocation of costs across the wider ecosystem. The regulatory perimeter for anti-money laundering does not cover all the sectors that bring risk into the system. The anti-money laundering costs do not fall in alignment with the actual risks that they are supposed to manage.

Lord Allen of Kensington: Has the industry looked at a shared services model, or is that prohibited by legislation or regulation? Clearly, the smaller companies do not have the economies of scale, so their unit costs are substantially higher. Is there a shared services model anywhere else in the world? As a consumer, you are giving the same information again and again. If there were some way in which that could be streamlined, it would take cost out of the system and would be much more efficient from a consumer perspective.

Nick Van Benschoten: Yes. The issue has been looked at a number of times. I believe there have been a few attempts in other countries. There are obviously challenges to try to make sure that the system delivers the right outcome. I believe that in the UK one of the current discussions is that DCMS is taking forward a consultation on digital identity. That will aim to reduce a lot of the duplication and improve the reliance framework so that it improves the customer experience. Steve's organisation may have more direct insight into current efforts in other countries.

Steve Elliot: Lord Allen, there are a number of conversations happening in a number of different countries to try to build utility models that sit across multiple organisations in a particular sector. Instead of each organisation running its own "know your customer" checks and controls, it is done centrally. The shape of the future regulatory markets could help that by allowing firms to make more use of trusted identities. When there is a confirmed trusted identity, firms can utilise it across a range of services they provide rather than having to redo the checks. To answer your question directly, there is certainly interest in building that, but it then creates commercial models in the middle for firms to provide that service.

Lord Allen of Kensington: Thank you.

Q4 **Lord Burns:** You have explained something about the drivers of increasing compliance costs. Is there anything more that you want to say about the drivers and what the main factors are? Secondly, what kind of changes do you suggest might be made? What are the priorities in addressing the problem of increasing compliance costs?

Steve Elliot: On increasing compliance costs, a large part of it relies on the regulations. It is firms trying to do the right thing by the regulations, but when you look at what they are doing, it is not particularly effective.

We have mentioned "know your customer" a few times. What is it? We have all experienced it when we have tried to open a bank account. We have to provide a passport or a utility bill. That is doing very little other than generating a lot of paperwork. The risk that I pose to an organisation is dependent on the network I interact with. Who else am I engaging with? Who else is in my household? Who else am I engaging with in my commercial life, and so on?

Two people could appear to be the same because they have a very similar passport and utility bill, and live in the same street, but actually

the risk that they pose for money laundering, for credit risk and for all sorts of other risks is very different. You only see that when you access a much broader range of identity attributes and monitor that across the expanded network. Cost is being created by ineffective controls that gather paperwork rather than actually seeking to understand the true nature of the risk.

Lord Burns: You are saying basically that it is designed to chase down one avenue with increasing ferocity, and not to redirect efforts towards areas where there might be greater returns.

Steve Elliot: Exactly. The risk is in the network, not in the individual. I can provide a passport and a utility bill, but you do not know the risk that I pose in relation to money laundering or fraud. If you can see all the interactions I am having through the devices I use—mobile phone, tablet, iPhone or computer—and my commercial transactions, you can see the true nature of the risk that I pose.

You could also see vulnerability. You could see how vulnerable I am as a customer. The ability to see all that data and have that insight is available today, because technology and big datasets allow firms to get far more insight than is available using a utility bill and a passport.

Lord Burns: Are you suggesting that basically the whole set of arrangements for AML and “know your customer” has been driving us down an increasingly deep and rather pointless hole?

Steve Elliot: I am, yes. There are a whole range of benefits that are available to be gained by industry that are not being accessed at the moment. I could go into them in some detail, but your point is well made and I agree with it.

Q5 **Lord Burns:** How do we get more value for money from the alerts and reports that both you and Nick spoke about earlier? It is some years since I was reasonably closely involved with this, but at that point a major concern to me was the use that was being obtained from the enormous amount of material that was being hoarded. Do you have any proposals for how one might get greater value out of those alerts and reports, or is it all about the direction in which the investigations really should be going?

Steve Elliot: The reports, as they stand today, do not have the value they should have. You could get more value from today’s reports by using more data science to evaluate or get data insight from what already exists, but what exists is not particularly valuable.

For example, having been a money laundering reporting officer, I have been obligated to report people in the past because they have a passport and a transaction that comes from what appears to be a high-risk territory that we could not necessarily explain. There was no substance necessarily to confirm that they were involved in money laundering, but they were suspicious to a point that we could not validate. A whole load

of information is being reported that does not add value to the regulatory regime or the attempt to drive out money laundering.

Lord Burns: Nick?

Nick Van Benschoten: I would like to draw attention to the work we are currently doing with government law enforcement and regulators under the economic crime plan. That work has shown a way to improve on the status quo. It includes getting much better outcomes for joint intelligence sharing and analysis with law enforcement through the information-sharing gateway from the Joint Money Laundering Intelligence Taskforce. That has definitely proved the value of taking a new and different approach, and trying to make sure that the industry looks at problems as a network.

As Steve says, part of the problem is that the regulations are addressed to individual firms, but criminal organisations address the industry as a whole. The problem we have with a lot of the work under the economic crime plan is that the direction of travel is right—we know that it works and adds value—but it is reaching the limit of what we can do without fundamental law reform.

One of the examples I would note is the vulnerabilities of the system. Nearly every regulated firm is trying to look at whether companies are true companies with legitimate activity or whether they are shell companies that have been taken over by criminals. The problem is that, unlike passport data, the UK Companies House registration system is hobbled by a legal duty and lack of powers to check. We have a key vulnerability in the system.

We know through our work with Companies House and other government agencies that, when the Government are able to share data to help the regulated sector as a network to scope its investigations, we get much better outcomes. That is very hard to do under the current legal regime. We are still waiting, and we look forward to the next Queen's Speech to see fundamental Companies House reform to close that vulnerability.

Likewise, the information-sharing restrictions that Steve referred to are preventing firms piecing together the different networks they see and helping law enforcement to direct further inquiries and close down vulnerabilities. Instead, law enforcement gets fragments of intelligence from fragmented firms.

We know that the JMLIT model works, but it is very hard to scale up without legal reform. A lot of the technological options are there, as Steve said. We are able to use them in some areas such as fraud, where we have a technological solution for identifying and tracking money mule activity, which is a form of money laundering across the payment system, but that is very difficult to do at scale without fundamental law reform. The economic crime plan gives a very good indication of what we want to do. It is just how we scale it up. I think the answer is fundamental law reform.

Q6 Lord Burns: I have one follow-up question. To what extent have the costs on financial institutions been excessive relative to the costs of enforcement activities? Maybe they should be bearing more of the costs. What you are suggesting is that there is no point, if I have interpreted it right, in doing that without law reform that enables it to be a more effective activity. Are we not investing enough in law enforcement?

Nick Van Benschoten: It is a bit of a mixed answer, if I am honest. You are quite right: you need a properly capable public sector response to these organised crime networks. You need a network to defeat a network. We now have the National Economic Crime Centre, and we have a number of economic crime co-ordinated committees, but they need the capabilities to respond. They need to invest in analytical technology. They need to respond in terms of investigatory headcount. That is happening. There are commitments in budgets. We look forward to seeing that continue. You are right: at the end of the day, we need bodies such as Companies House not just to be given some extra money but to allow their digital transformation to be supported by fundamental legal reform.

A final point is that the private sector at the moment is not able to share intelligence among the industry. If we exit a customer because of anti-money laundering suspicions, they can go down the street and enter another bank. We are not able to share that intelligence freely or even under a directed instruction. That is an area of reform that would provide much better intelligence for law enforcement.

I am afraid it is a bit of a mixed answer. There is a bit of investment going on, and we welcome that, but I think it will reach its limit without further law reform.

Lord Burns: Thank you.

Q7 Baroness Donaghy: Good morning. What impact has the UK's withdrawal from the EU had on anti-money laundering compliance costs for UK financial institutions? The report we read indicated that they felt that there would be increased costs. Is that correct?

Steve Elliot: It is correct. There are two questions in your question. One is about the impact. The industry does not know yet what the impact will be, because we have not yet seen enough detail on the future state of law or regulation. That uncertainty is causing some nervousness, because firms need to prepare and plan for the future, and they do not yet know what that future is.

We have seen some increase so far. There is a UK sanctions list, for example. That means that firms operating in the UK and across national boundaries have to comply with another list in the regulatory environment in addition to the ones they already have. At a very basic level, it is creating additional cost because there is more checking to be done. The end answer is not yet known, because we do not have the detail.

Baroness Donaghy: Nick, do you have anything to add?

Nick Van Benschoten: I echo that. Obviously, the withdrawal is a major change management process. There has been a lot of regulatory change for financial crime, and this was another bit. We have worked with our members, as well as with other industry associations and law firms, to help try to manage the process. As I mentioned before, a number of our small members are struggling to keep pace with the change.

I note, however, that as regards the end of transition we are now in a standstill period, with the Financial Conduct Agency waiting until next April before the full effects of the changes come through. Some of the changes will definitely have a significant impact on certain regulatory obligations—for example, correspondent banking. We are still working through the impact, and we are discussing it with the regulator. As Steve says, we are still waiting to see the full impact. We are still, as it were, half way through the process before the end of the standstill direction.

Q8 **Baroness Donaghy:** Thank you. On a slightly different issue, I was interested in the costs of staffing and training, and the fact that the market seems to favour them so that people can hop around from institution to institution. That seems to be a management issue. If there was more co-operation between the companies—rather than poaching, presumably—that issue could at least be mitigated, if not solved. Is there any thought about co-operating on levels for the cost of staffing?

Steve Elliot: It is a very difficult thing for firms to co-operate on, because they are commercial entities. They need to deliver a service to their commercial customers.

Staffing is a real problem. When firms have a new regulatory obligation, or when they are doing retrospective work to improve some of their anti-money laundering controls and arrangements, the easy quick fix that they often see is to bring more people in to do more manual processing.

To give you a practical example, in previous consulting roles I have been in I have seen large UK banks do remedial pieces of work on high-risk customers to try to truly understand how they risk-rate high-risk customers and how they update the controls and paperwork—the KYC records—to ensure that they are adequate. In one case, the bank brought in 200 people to manually process the records, transferring data from about 12 spreadsheets on to one spreadsheet to produce the record. It then had to employ another team of another 200 people to quality-check the work of the first 200 people.

All that work could have been done by machines using processing and AI to pull data from one spreadsheet to the next. Then you could use people to do the intellectual work, to evaluate the outputs rather than to do the manual processing. Firms use far too many people to solve problems that should be solved for the long term using data and technology.

Nick Van Benschoten: On the training and awareness-raising aspects of regulatory change, we work extensively with our members trying to share good practice to reduce the extra duplication of investment that they may

need to put in. Additionally, the industry in the UK has the Joint Money Laundering Steering Group, which produces guidance on best practice. That, hopefully, helps to reduce the added investment that people need to put in. I know that is of great benefit to many of our firms, both large and small.

As Steve says, a number of the processes that firms need to implement have changed. Historically, there have been fairly rigid requirements. Some of the requirements in the implementation of the fifth money laundering directive have required new red flags to be raised on certain high-risk sectors. That is a process that is very hard to flex at the moment. Those are the examples that drive additional burdensome requirements.

Q9 Lord Curry of Kirkharle: The picture you have painted so far, gentlemen, is quite depressing. Compliance costs are very high and customer experience is poor, and current regulations do not address the risk. We need to find a solution and a way forward.

Nick, you have already mentioned that law reform is necessary, in your view. You also referred to technology. Steve, you have talked about the sharing of data. What role can data and new technologies play in helping to address the problem? Are there opportunities that we are not seizing at the moment?

Nick Van Benschoten: I think Steve will have a great deal of professional insight on this. From our members' perspective, technology is a great opportunity. The statements from the Financial Conduct Agency during the early stages of lockdown on remote onboarding and the use of biometrics were a good example of how regulatory guidance can encourage and assist firms in taking on new, innovative approaches. That is an important aspect of the point we are making about regulatory change. Regulatory change does not need simply to be through legislation. It can also be in statutory guidance and other statements by the regulator.

I mentioned the DCMS consultation on digital identity, which is an important aspect of the debate. When I say that we are concerned that it delivers the outcomes it is intended to, we are very keen to understand how that will interact with the money laundering regulations and the rules about reliance on other regulated firms, how that will interact with the regulators' perspective on what firms should be doing, and whether duplicative activity is still required.

Technology is very useful. It is, however, sometimes difficult to implement without the right guidance or regulatory underpinning. At the moment, the key point for us is working with the Government. We know that this is part of a global trend; it is not just the UK. The international anti-money laundering body, the Financial Action Task Force, published a number of reports over the weekend about the value of innovative technology, including collaborative analytics and data sharing, and set out a number of cases where this can be supported by joint public and

private activity. The UK is pretty well placed in the tech experience and in money laundering and other innovations, but, as I said, this is a global initiative; there is always more good practice to be picked up on.

Steve Elliot: Lord Curry, if I may add to that and give it a practical flavour, one point worth bearing in mind is that firms find it very difficult to innovate because they have to do tick-box compliance against current regulations. If they want to find better ways of driving outcomes that provide better customer service, or drive down money laundering or even fraud, it is an additional cost. It is very difficult to redeploy cost from already high-cost areas to innovate and drive solutions. It is also difficult for them to do, because they are not given regulatory and legal protections when they seek to innovate and drive towards better outcomes. The focus for them is ensuring compliance and evidencing compliance. If they want to drive innovation and get better, they do not have the same protections that are afforded against their compliance checklist.

Our current position is not at all depressing. I am where I am, having been a practitioner for many years, because the value in data is phenomenal. We are at a point in history where we are able to use data and technology to make life much more difficult for money launderers and real fraudsters, and to make life far easier for trusted members of society who should be able to move across the ecosystem far more effectively.

I can give a practical example. We are running algorithms against large datasets across multiple firms at the moment. We can see money laundering and fraud networks starting to appear before the individual firms can see them. Individual firms are looking only at their customer, but we can see the full network that those individuals and firms are operating in. We have a great opportunity to drive down fraud, financial crime and money laundering across the market, but we need to use data and technology effectively to do so.

Lord Curry of Kirkharle: But, Steve, you said earlier that the current legislation is preventing that.

Steve Elliot: Again, I can give you a practical example. We have to explain, when we use AI and machine learning, how we got to the outcome that it drove, which means that we have to reduce the effectiveness at the moment, and reduce the capability of AI and machine learning engines, so that we can explain the decisions.

We are being held back in a way the health sector is not, and in ways the industrial manufacturing sectors are not. The aeronautical sector is using AI and machine learning at the moment to try to build lighter and stronger fuselages for aircraft. It is able to do that, because it can put a whole range of attributes and design criteria into AI models, and that produces the model, but the human cannot explain how they got there. The health sector is using AI and machine learning to try to solve cancers and to find cures. You take outcome data and reverse-engineer back

through lots of attributes to find what you should have been looking at in the first place, so that you can then treat it before you get to the cancer.

In financial services, we cannot do that. We have to explain all the analysis that has taken place, and that matters when we are looking for suspicion of fraud or money laundering. When we are looking for credit risk profiles or when we are trying to allow people to access the markets, we have to explain all the decisions. We are already in a great time, but the regulatory environment needs to allow us to go further to get to the outcome that we need to achieve.

Lord Curry of Kirkharle: Thank you.

Q10 **Lord Reay:** Continuing the technology theme, what is currently preventing financial institutions in the UK from taking advantage of these technologies? To what extent do you think changes to GDPR could be helpful in that regard?

Nick Van Benschoten: On prevention, as Steve and I have mentioned, there are a number of areas where the regulatory permission to explore new technologies comes with a lot of caveats, and those caveats often require quite a bit of legal interpretation. As Steve says, they are additive; they are on top of existing requirements.

Most financial firms will be looking for ways to streamline case-by-case assessment of individual customers. It is important for reasons of financial inclusion and fairness that we treat customers fairly, but that has to be done at bulk. When you start to look at those additional requirements on top of the challenge of scale, it becomes increasingly important that we get guidance on what is an acceptable approach to managing risk indicators and sharing intelligence. At the moment, a number of our members are finding that these requirements, on top of other regulations, are making it both prohibitively costly and quite prohibitive in terms of regulatory risk to innovate in that way. As Steve says, firms still need to meet minimum legal requirements. If they are doing this on top, sometimes there is an opportunity cost or requirement to reallocate resource.

On GDPR, we are lucky in the UK to have quite a mature debate about the need for public policy to be balanced in the round, and for people to take a proportionate approach to all sorts of risks against individuals' data, including account takeover and fraud against them. We are working very closely with the ICO and the Government looking at new ways in the approach under UK law on data protection for industry to set out its own path on how we can move a bit more into the collaborative network approach. Again, that is work that is referenced in the economic crime plan. It would be helpful if there was more regulatory guidance and legal reform to support it, but we are lucky in the UK that we can have a constructive and mature debate on that.

Steve Elliot: GDPR has been invaluable. I have been a practitioner and I am now a service supplier. GDPR has forced firms to tidy up and clean

their data. That was a long overdue exercise that has benefited the industry, because it now has more accurate data that it can run checks from. There is nervousness about personal data, but there is a benefit in sharing data. People want to protect their data and prevent it being shared, but by sharing it we can protect people better.

I gave the example earlier of us being able to see fraudulent networks starting to appear. We can see account takeover and identity impersonation starting to appear. We can see that, because data is being shared and accessed across multiple firms and industries. If that was not available, we could not see it, and the individual would be less protected. I think data sharing actually helps to protect individuals, but that is not often seen when individuals are looking at GDPR and personal data.

Lord Reay: In the past, I have found setting up an account at one of the fintechs much easier than with traditional banks—for instance, Revolut or TransferWise to transfer currencies. Could you comment on why that might be?

Steve Elliot: It is really interesting. A lot of the fintechs, and particularly the regtechs that are coming through, are starting to challenge some of the bigger banks. Open banking has been invaluable to the industry. It is a piece of progressive legislation that has allowed firms to access data in a way that previously they could not do. The smaller firms, which have more efficient operational processes because they have designed them in the current environment and designed them around the customer, are able to run algorithms against data and access data assets very quickly and efficiently to embrace the current regulatory environment. The larger firms have a bigger organisation to re-steer and benefit from some of those changes.

- Q11 **Lord Blackwell:** Listening to this, you could form the view that the industry is spending a huge amount of money—£28.7 billion—employing mostly humans, as Steve said in his report, who are going through capturing myriad customer data from lots of small customers and small businesses that are inherently low risk and of very little value. Is the impact of what you are saying that we ought to consider simply abolishing all that and investing some part of it in building an intelligence-led network so that we can focus on the higher-risk areas and customers?

Steve Elliot: Absolutely.

- Q12 **Lord Eatwell:** That is such an enormous question and it has absolutely hit the button right on the head. We have heard about a major failure, in the sense that Steve says that only 1% of money laundering is found. That is a huge failure for all this money. He has sketched out the three components of what needs to be done: the regulatory perimeter, the identification of beneficial ownership, and networks. If you take that, the question Lord Blackwell asked is: where do we focus with respect to the regulatory perimeter, beneficial ownership and networks? Is it all three?

Steve Elliot: I would start with number one and number three, because the network would give you the beneficial ownership but you need the regulatory and legal environment to allow you to embrace the data and technology that allow you to explore the network.

To go to Lord Blackwell's question, I would say that, no, it does not help us to keep fixing an environment that does not get us to the outcome that we need. I think we need to embrace the new, and allow firms to utilise data and technology to target fraud, money laundering and a whole range of similar activities.

Nick Van Benschoten: I echo that. It is important to remember that the anti-money laundering regime is an international standard. We have a lot of legacy legislation from implementing EU directives, but the standards come from the international body, the Financial Action Task Force. There are other more flexible and outcome-focused ways of implementing those standards, as Singapore, the US and others are doing. The EU is undergoing its own fundamental reform of its anti-money laundering regime. I think now is a timely opportunity to look at what other fundamentals we are trying to achieve.

As to how we would eat this elephant, the first few slices should be threat driven. We should be looking to where we know there is a problem. Again quoting Graeme Biggar, the director of the National Economic Crime Centre, he said that his organisation's analysis of the global laundromat schemes for Russia and Azerbaijan noted that over half the transactions were connected to UK companies, but that those companies were not banked in the UK.

As regards vulnerabilities, we know that a number of sectors are undersupervised. Trust companies and service providers in the UK have submitted only 31 suspicious activity reports, which, when you look at the 460,000 for the banking and building society sector, is odd. There has been a very welcome increase in supervision by HMRC of accountants, letting agents and trust company providers, but it is from a low base. HMRC increased the registration from 7,000 to 15,000 recently, which suggests that it may have been undersupervising in the recent past.

I think a threat-based approach would be the first step. As Steve says, there are a lot of exemplars overseas of best practice opportunities for implementing these international standards. We can do better.

Q13 **The Chair:** Just a quick, one-word answer, Nick. Are the Government seized of the need to react to the pressure undoubtedly coming from your members?

Nick Van Benschoten: I believe so. We have a joint commitment to respond to it. I think now is the chance to implement that through fundamental legal reform.

The Chair: Thank you very much indeed. That was a very lively and illuminating discussion. The problems are rather larger than many of us thought them to be. Thank you for that. That brings this session to an

end. We will have a few minutes' break before our second session.

Examination of witness

Christopher Woolard.

Q14 **The Chair:** Chris Woolard, welcome to the second session of today's discussion on anti-money laundering, "know your customer" and its effectiveness in catching criminals, the onerous cost that it brings with it and, of course, the onerous paperwork that customers have to endure.

We heard in the previous session that the outputs for the £25 billion-odd that this costs the industry are disappointingly low, and that there are better ways of dealing with it. It would be very helpful to hear from you what the FCA thinks about this whole area and what reforms it is pressing for.

Christopher Woolard: I am very happy to do that. Perhaps I should briefly introduce myself. I am now a partner at Ernst & Young and have been for a number of months. Obviously, I cannot answer on behalf of the FCA, but I am very happy to give you what was my view when I was there.

In particular, there is the question of how you strike the balance between the costs and benefits, and what might be done better about financial crime. Certainly, in terms of how I used to think about it as a regulator, in the UK the estimates of what it costs UK industry in compliance vary quite considerably. The figure that we used from an FCA perspective was around £4 billion a year. That was seen as a reasonably reliable number that quite a lot of different sources agreed on, but there are varying estimates. To put that in context, although you have to be careful because clearly it is not quite comparing like with like, £4 billion is roughly the same cost as the UK prison system every year. It is a very significant sum of money, whichever way you look at it.

As to the benefits—if you can describe them as benefits—first, clearly there is an attempt to deal with financial crime, organised crime, counterterrorism financing and those kinds of questions. It is important absolutely to try to do our best as a nation to deal with that.

Secondly, for many of the firms that we are talking about, the standards that they would be dealing with in any other part of the world, certainly in any other part of the G7, would be very similar. This is absolutely part of playing in a global financial system. One of the particular issues that we might end up returning to in this session is the fact that often standards set in the US guide many firms into thinking about their approach overall towards financial crime.

At the same time, there are two very significant issues in dealing with financial crime. The first, if you look at it globally, is that even if you can create a hostile environment in the UK towards financial crime, and I

believe that that is an important part of London's wider appeal, about 1% of global illegal money flows are estimated by the UN to be intercepted by regulators and other law enforcement authorities each year. The vast majority of this is finding its way through illegal sources to other parts of the world.

The second issue is that financial crime has become increasingly asymmetric. When they originated, a lot of the controls, particularly sanctions and "know your customer", were very much geared to the idea of terrorism or state sanctions being levied against multimillion pound transactions and entities. Increasingly, what is being sought in terrorist finance now is a matter of a few thousand euros. There is a real asymmetry in where the targets for trying to discover beneficiaries of financial crime have gone over the years.

The final point I would make in response to the opening question is that I certainly always took the view that there were better options for finding ways in which you could make the system cheaper in its overall cost burden and far more efficient in identifying bad actors. One of the things that the FCA has pursued historically is how you can use greater technology to begin to work into that space and try to find a solution that achieves that.

The Chair: In his report, Steve Elliot says that the cost of compliance is £28.7 billion. You are saying it is £4 billion. How do you arrive at that?

Christopher Woolard: I am afraid I do not know where Steve's number comes from. There are various ways of cutting it. During my time at the FCA, historically the numbers used by a variety of institutions—the City of London, TheCityUK, and others that commented on this—put the price for compliance somewhere between £2 billion and £4 billion annually for the UK. All I can quote is the number that I used as a regulator, which was £4 billion as a reasonable estimate.

There are higher estimates. It rather depends on what you include in the calculation, how many countries you look across, and those kinds of things. Within the UK, that was the number we used. Whichever number you adopt, and speaking with my new EY hat on, however you look at the issue and however you cut it, the cost is very large indeed.

Q15 **Lord Blackwell:** Whatever the cost to the industry, the front line of our AML protection is this very indiscriminate attempt to man the whole of the "know your customer" information requirement across every individual customer and business. The rewards from that may be questionable in terms of the risks associated with those individuals. It also creates friction and inconvenience for customers and small businesses trying to go about their business and having to deal with the bureaucracy involved. At the FCA, were you and others concerned about the scale of the costs imposed on consumers and small businesses?

Christopher Woolard: Absolutely. You can think of those costs and inconveniences in a number of different ways. The first is obviously on

the individuals. That could vary as to who it most affected. At one end of the scale, and I imagine a number of the members of the committee might have come across this, you have the question of PEPs, politically exposed persons. That is a reasonably broad category of people who have to go through some sort of additional checks.

At the other end of the scale are people who have very little interaction with the banking system and who are often some of the poorest in the country. They find it quite hard sometimes to prove their identity the first time they come in. Historically, that was something that we tried to pay some attention to: how could you widen the range of things that can be used to prove identity there?

The other place where this bites, and where there is a lot of concern in the market, is the wider effect on competition. In particular for individuals, it poses a friction. It creates potential discouragement for switching between banks or between other service providers if you think that you have to take half a day off to bring in a passport or some other document and physically identify yourself. Are there better ways in which that could be done?

Also, are the controls being applied on a blanket basis by banks to certain categories of other firms, whether payment firms or other providers in the market? One of the things that keeps coming back, and indeed was even mentioned recently in Ron Kalifa's review, particularly for fintechs and other high-growth firms, is that often one of the hardest bits is not getting regulated but getting a bank account after you have been approved. There are clearly frictions that hold back competition from working as well as it could.

Q16 Lord Blackwell: Given those frictions and the costs they impose on consumers and small businesses, are the benefits from reducing money laundering from that kind of regime worth it? Would you say that there are opportunities now to reduce the complexity and scale of that intervention? Are there more focused ways of reducing the risks?

Christopher Woolard: First, proving the benefits and disbenefits in this space is particularly hard. You are looking at an illegal activity, which by its nature is very hard to measure in a conventional way.

Clearly, for most firms that are going to plug in somehow to a wider international banking system, particularly where they will touch the US or other parts of Europe or wherever it may be, all those countries are operating on very similar standards to the UK and will expect that kind of reciprocity. I think there is almost a cost of playing for financial institutions and a necessary hygiene factor.

I think there is more scope than necessarily thinking, "Which rule do we take away here or there?" It is always a worthwhile exercise to step back and think about the proportionality of anything, and that is fine, but the bigger wins may be in the way you think about a number of issues. The first is the application of technology. One of the things on which the UK

led the way in experimentation but which others are now following is homomorphic encryption and no-proof identify: in other words, you do not have to create massive central databases to exchange data about an individual's identity between banks. You could invest in that and do it far more smoothly.

The wider question about digital ID is really interesting. I know that it has had a chequered history in the UK, but if you look at countries like Sweden or Canada and what they are doing there, they are reducing a lot of friction through being able to have a digital identity that at least you can use within the financial sector.

There is then a question of whether there are fundamental issues that might be holding people back—for example, how liability is addressed in those systems, who has done the identification, and those kinds of questions. If you could get to the heart of those, you could take out quite a lot of friction.

Lord Blackwell: Thank you. Others will want to come back on the technology issue, so I will leave it there for the moment.

Q17 Baroness Bowles of Berkhamsted: Hello, Chris. I am interested in exploring a bit further where there are differences between the UK's anti-money laundering rules and those in other jurisdictions.

We all know that the principles are handed down internationally from FATF, and we have inherited a lot from the EU. I remember only too well that originally the anti-money laundering directive was done by the civil liberties committee. When we were doing AMLD IV under my chairmanship, ECON got a look in, and we had a lot of fights with the civil liberties committee over things that we wanted to do and things that it said offended civil liberties.

How much will that change after Brexit? Obviously, GDPR comes into all this. Have some of the new measures overcome that? What are they doing in other countries, such as the US and Singapore, that might not be so careful over the information as in the EU precedents?

Christopher Woolard: What is going on globally at the moment varies a bit. There are obviously some nuances. When it comes to penalties, for example, I think the EU standard is roughly four years' imprisonment as the maximum criminal sentence. It is about 10 years in the US and up to 14 years in the UK. There are nuanced differences such as that, but the broad principles that are applied are very similar between countries.

On how you apply technology to the question, how you use large datasets and how you use systems like no-proof encryption, probably the UK and Singapore are the most advanced in thinking about those right now, although no one has actually got to the point of implementation yet. In the US, quite a lot of what has to be done is quite prescriptive. In primary legislation, the sort of paperwork that needs to be done is often set out. In many ways, it is far more prescriptive than in the UK and in the EU on certain kinds of topics.

If you look for differences, historically the UK has had a far more dispersed money-laundering regime, with many bodies and agencies able to apply it. The EU is now thinking about a single anti-money laundering body. Other jurisdictions—Australia and other places—have had them for years.

On what needs to be done to establish identity, the underlying principles are pretty much the same everywhere. As you know, FATF not only sets an expectation but benchmarks different countries and inspects against those standards. So I do not think there is an awful lot there. Where you might see a bit more scope, because the UK can now set its own standards and laws for this, is in how you think about information sharing in a different way. That could be on the table, but the regulations are driving at pretty much the same thing, in whatever country they come from. Broadly, they are pretty much the same.

- Q18 **Baroness Noakes:** My question broadly follows on from Lady Bowles'. You rightly said that now we have left the EU we have the opportunity to set the rules for ourselves, but you seemed to imply that there is really relatively little scope. The EU is famously rules-driven rather than principles-driven. I wonder whether there is scope to look more radically at whether we are shaping our rules and legislation to attack the real problems, identify where the risks are and focus effort on the risks, and rather than just saying, "We've got this big body of rules. Can we take away one here or one there?", re-engineering it quite significantly. Would we not have scope for that, even staying within FATF?

Christopher Woolard: The point you make is really important. I think the focus has to be on how you are trying to drive at the underlying problem, and how you are attempting to tackle the harm at the bottom of it, as opposed to necessarily taking one rule away or substituting another. I think that point is entirely right.

The reality for most banks is that the really big player is the US. One of the things they have to have an eye on is the US standards. As I said, some of them are very prescriptive when it comes to what information needs to be produced. There has been dialogue in the last couple of years between the UK and the US about how you might move much more to concentrating on the underlying effectiveness.

My personal opinion—this is not EY's opinion or the FCA's opinion—is that if you look at what a combination of digital identity and greater encouragement for collaboration between financial institutions coming from government and regulators would do, with the right technologies underpinning it and dealing with some of the really thorny questions about liability you could make some significant advances in this space. Some of that would require legislative underpinning. Obviously, the UK now has the opportunity to do that legislative underpinning for itself. That is the territory where you could get significant gains in efficiency and effectiveness, rather than thinking about designing a completely different regime. For most firms, a completely different UK regime, when they

operate in Europe or in the US, would just be a further regime to have to try to comply with, with the cost attached to that, if that makes sense.

Baroness Noakes: Could I just explore that? When you say that they are being driven by what happens in the US, is that just for sanctions, or are we talking about the whole range of AML requirements? The AML requirements are bearing down hugely on small and medium-sized entities in this country, and there is a lot of the cost for financial institutions in dealing with that. That cannot have anything to do with something that impacts the US. Are we just not taking a sufficiently risk-based approach to how anti-money laundering is implemented and enforced in this country?

Christopher Woolard: There is a question about how you set risk appetite and proportionality. Historically, the FCA sought to do that, but you might want to address that question to the current management of the FCA as well.

Many large institutions, if they are operating across multiple jurisdictions, usually want to try to find ways in which they can have systems and controls that work largely for all those jurisdictions rather than making lots of individual ones inside firms. To some extent, you get highest common denominator-type standards just because of that pressure to say, "How do we control our wider costs and those sorts of issues?"

To give you a practical example, in Sweden there is essentially a bank-led digital identity, not a government-issued digital identity. Everyone has one, effectively. One of the big questions is: the first time you are identified, is that good enough for the system as a whole, or does every individual actor in that system have to re-identify you each time, in which case the benefits of a common digital identity are nullified because you have to prove who you are all over again? There, the fact that you have gone to one bank—your bank—and identified yourself once to that digital system is deemed by all the other financial institutions in Sweden to be good enough. That is an agreement that has been reached largely just between the banks, although I think there is some kind of regulatory underpinning and recognition for it.

Something like that would have the potential for very significant cost and friction reduction. Whether it needs to be underpinned in UK legislation is a matter for others to think about, but those kinds of things would make a real practical difference for many people.

Baroness Noakes: Does that work for companies as well as individuals?

Christopher Woolard: I think you can apply the same thinking to small firms. One of the big lessons from the whole BBLS and CBILS-type packages that were put in place for Covid is a far better understanding across the system of what very small businesses actually look like in financial services terms. Often, they look very like individuals. I think that, with some development, you have a space where you could certainly apply that to SMEs.

Baroness Noakes: Thank you.

Q19 **Lord Sharkey:** Good morning, Chris. The existing regulation seems to create obviously unnecessary costs. For example, Iain Duncan Smith's TIGRR report suggested that account information services and payment initiation services should be removed from AML scope on the reasonable grounds that they could not possibly be used for money laundering. That is already the case in Denmark, as I understand it. Do you agree with the TIGRR proposal? What else could be removed from scope?

Christopher Woolard: First, in the overall thrust of where some of the TIGRR report goes, particularly how you use innovation, sandboxes and those kinds of things, there are many points that are very worthy of consideration.

On the particular point about AIS and PIS, just so that we are all operating on the same definitions, an AIS is an account integration service that allows you to put a number of your own bank accounts together and see all that information in one place. A PIS is a payment initiation service that allows you to move money between accounts.

This is a debate worth having, in the sense of what an AIS could actually do with regard to financial crime or money laundering. It is a perfectly reasonable debate to have, because you cannot do anything once you have seen that information. With a PIS, it is more difficult, because you can use it to initiate payments moving between accounts. Depending on how those accounts have been aggregated, there can be a potential financial crime risk within them.

There is also a question about how those institutions dock with the wider mainstream financial system—the classic incumbent high street bank—and the level of confidence that can be had both ways. It is worth having a debate about. Given that most of the business models that certainly I saw that really worked and had the chance of making money needed to be both an AIS and a PIS, whether you take out one or the other might be quite an academic distinction.

There is also a question about how you think about the system holistically and about the confidence of new firms entering it. Clearly, I am not the regulator now, so that debate is with a slightly different audience. It is a reasonable conversation to have, but in practice I am not sure that it would deliver huge benefits to AISs and PISs.

Lord Sharkey: Is there a simple explanation of how we assess the effect of AML measures on the volume of laundering?

Christopher Woolard: Sadly, no. You can obviously look at some of the global figures that are prepared by the UN, but in reality—a bit like other forms of crime—the fact that people, by the very nature of it, will try to hide it means that it is an incredibly difficult thing to assess.

Q20 **Lord Eatwell:** I have two information questions. The first arises from what you have said already. I am very puzzled by your references to the

United States. Company registration in the United States is an issue of the state, not the federal government. If you register a company in Delaware or Wisconsin, the level of beneficial ownership information is negligible. I do not understand what you are talking about, in the sense that Delaware and Wisconsin are both black holes as far as securing information is concerned. Could you explain?

Christopher Woolard: Yes, of course, I would be very happy to. We have been talking less about individual company registration necessarily and more about the wider requirements that are imposed, particularly on banks and other institutions, largely by federal law—obviously some state law is involved where banking and insurance are concerned—and what money laundering and counterterrorism controls may be imposed and—

Lord Eatwell: Yes, but identification of beneficial ownership is fundamental. It is one of the three pillars in attacking money laundering. Given that it is a state responsibility in the US, as far as this investigation is concerned federal law is not relevant.

Christopher Woolard: In the sense that it is the US Treasury that sits behind most of the policy—it is the owner, if you like—in the States, and the SEC, the OCC and a number of other agencies take responsibility to some extent for the overall sets of measures. When we are talking about those, and certainly when we are talking about the risk to firms posed by financial crime, sanctions and impositions, most of which come from the Department of Justice in deferred prosecutions, those are the kinds of questions that the UK banks have had to face. That is the set of standards I am referring to.

Clearly, there are very variable company law standards within the US, as you point out, but the requirements on banks to try to establish, for example, beneficial ownership in the US, which the US Treasury would set, are not too dissimilar from UK standards.

Q21 **Lord Eatwell:** Okay. Thank you. The other information issue is: to what extent would changes to GDPR reduce the compliance costs that we have been referring to and perhaps increase competition in financial services?

Christopher Woolard: The first thing to say on this is that I am absolutely not an expert on GDPR.

Lord Eatwell: I know the feeling.

Christopher Woolard: I have obviously encountered it in my career, but I am probably the wrong person to put this question to. I have a couple of quick observations, though. The first is the degree to which GDPR has become almost a de facto global standard. Even a number of US websites use GDPR-type disclosures now, because they are doing business internationally.

Secondly, the prize here is how you ensure that you have a really safe global system for processing data and moving it potentially between jurisdictions processing that data. There are some things where GDPR is

becoming in effect a global default, so how far do we want to be part of that in the future?

Finally, on data and competition, there are initiatives that government, BEIS, seems to be coming forward with now, such as the use of smart data, and there is the degree to which you can have so-called digital sandboxes. We set one up just before I left the FCA. You can assemble very large datasets where people can experiment and launch new products. Some of those can be incredibly important. Whether there is an interaction with GDPR that might need to change in the future is for others who are far more expert than me to comment on and explore.

Lord Eatwell: Thanks very much.

Q22 **Lord Grade of Yarmouth:** I want to pick up on the sandbox question. Hello, Chris, I have not seen you for a few years. You are looking younger than ever.

Christopher Woolard: Obviously.

Lord Grade of Yarmouth: Are the sandboxes really critical in driving innovation in this area, or are they just a peripheral?

Christopher Woolard: I will be biased on this question, because obviously I founded the FCA sandbox and saw it copied in 50-odd countries. So I will speak from the position of being a massive proponent of sandboxes.

I think they matter, because regulators are often placed in a position where authorisation or licensing is a yes/no question. Often, when you are dealing with the newest technologies, the simple answer is that you do not know. A sandbox provides a regulator with a means of learning how a new technology will really work in practice.

The other piece is that where they have been evaluated, and certainly the UK one was evaluated, the firms that have been through that process have greater resilience. They last longer as new firms on average. They are also a very clear signal, particularly to the venture capital market, to invest. The firms that go through sandbox processes find it significantly easier to raise capital in the future, because they have a proven model.

I think that kind of experimentation is incredibly valuable. It should not become the only route to market. If people have good ideas that they think are ready to go, that comply with existing regulations as they stand, and they are confident about that, in all sorts of markets—not just financial services—there should still be a way of getting to market without having to do six months in a sandbox. That aside, I think they can play a very valuable role.

Q23 **Lord Grade of Yarmouth:** Listening to all the evidence this morning, the thought occurs to me, as a complete amateur in this area, that essentially this is about crime prevention and crime prosecution: catching criminals and trying to prevent it happening. We seem to be taking a

huge swipe at it in every direction.

Given what technology is available, and if the data was shared properly between the different authorities, could we not move towards a system that was driven more by anomalies and suspicion than by the data that is collected? At the moment, we are collecting data that nobody knows what the hell to do with, by all accounts. Would we not be better off spending our resources looking at where there is prima facie evidence or suspicion of wrongdoing?

Christopher Woolard: In fairness, that is what the existing system tries to do now. There is a system of suspicious activity reporting that tries to pick out, from the mass of transactions, where there are things that are flagging. There are a number of drawbacks to that process. One is the sheer number of false positives that you get in any of those kinds of systems. The other is the volume for the police and other authorities that might have to be investigated at any point in time.

The reality is that technology is becoming available. Some of it has only been available for the last five years or so, so it is relatively recent stuff. You can do a far better job of finding, predicting and spotting outliers. You can also do a far better job of spotting patterns of behaviour that might have otherwise been very easy to hide because it was all very small transactions.

I suppose the thrust of the evidence I have given so far is that I think there is a lot that can be done in this space, with a mixture of government, regulator and firms, to ask how you could begin to join up some of these things more and what the barriers would be to that. Often, they are the discomfort and liability that individual firms might feel about the handling of their data and what they are promising to the rest of the system in terms of "I know this person's identity" or not.

There must be better ways of doing it. You come back to the overall figure of 1% worldwide being intercepted. That tells you that there is a huge amount of room for improvement yet.

Lord Grade of Yarmouth: Is anything standing in the way of using technology to innovate in this area and increase successful outputs, prevention and all the things that this is designed to identify and prevent?

Christopher Woolard: There are probably three big things. The first is the sheer scale of investment required. We need to remember that, not just in the UK but internationally, almost every large financial institution is building on a massive brownfield site when it comes to technology. There are some huge resource issues there.

Secondly, the liabilities in anti-money laundering are significant and proper risk factors that banks and others need to think about. To go back to my Swedish example a moment ago, if I identify an individual and I am now doing it to a common system rather than just my own bank,

what liabilities do I take on at that point? That issue would need to be solved.

Finally, we are still in a world in which the US has made some really promising shifts of tone. In particular, there is willingness to think about whether there is technology that can do a better job than the existing systems in the last couple of years, but we still do not have complete international consensus of what this should look like in the new world. That is something that government regulators will have to keep concentrating on.

Lord Grade of Yarmouth: You talked about the up-front costs for firms investing in innovative technology and so on to manage this. If you can demonstrate that their annual savings over five to 10 years will at least equal what they had to put up front because of high costs currently, do you think that that equation might work and that the return on investment might stand up to scrutiny, or is it a sunk cost that they will get back, which will obviously prevent a rollout?

Christopher Woolard: My personal view is that that equation would work out pretty well for most institutions. I think there would be a significant saving over time. One of the things you have to bear in mind with the technology piece is that, right now, an awful lot is manual. In the very largest banks there are tens of thousands of people, in some cases, doing financial crime in some way, shape or form. I think the cost-benefit analysis would stack up for an individual bank, but it goes hand in hand with the question about international standards and liabilities. There is no point me having a very high-class technological system if, in the major jurisdictions, the law still requires me to do something manually or to have the paperwork available literally as physical paperwork.

It is those kinds of questions that the leadership of major banks will want to see solved: "I'm prepared to invest, but am I going to have not safe harbour but at least assurance that I will meet the standard if I make that investment?"

Lord Grade of Yarmouth: Many thanks indeed.

The Chair: Many thanks, Chris. That was very helpful and illuminating for all of us. I am still perplexed by your estimate of the cost. It would be good if you put your head together with Steve Elliot and worked out where the other £21 billion went. Your last answer was very helpful: that in fact there is a cost-benefit analysis but only if everybody is playing to the same rules. That is a challenge.