House of Commons

Treasury Committee

Oral evidence: Economic Crime, HC 940

Tuesday 9 October 2018

Ordered by the House of Commons to be published on 9 October 2018.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Simon Clarke; Charlie Elphicke; Stephen Hammond; Catherine McKinnell; Wes Streeting.

Questions 263 - 339

Witnesses

I: Colin Bell, Group Head of Financial Crime Risk, HSBC; Stephen Jones, CEO, UK Finance.

Written evidence from witnesses:

– [Add names of witnesses and hyperlink to submissions]

Examination of Witnesses

Witnesses: Colin Bell and Stephen Jones.

Q263 **Chair:** Good afternoon. Thank you very much indeed to our witnesses for being here for this next session of our economic crime inquiry. I am going to ask you both to introduce yourselves briefly, because we have people watching online as well as in the room, to know who you are. Then we will start with some questions.

Stephen Jones: Good afternoon. My name is Stephen Jones. I am the chief executive of UK Finance, which is the trade association for UK-based banking payments and cards businesses.

Colin Bell: I am Colin Bell. I am the group head of financial crime risk for HSBC.

Q264 **Chair:** Thank you. We have a series of questions. We are very grateful to you for coming in. I wanted to start with a question about whether the banks have got the message about the importance of economic crime and their role in dealing with this. In a recent article in *Private Eye*, Tom Keatinge from RUSI suggested that recent fines on banks for anti-money laundering breaches have changed their perceptions of financial crime risks. Do you think banks have got it in a way that other sectors have not?

Stephen Jones: I am not going to make a comparative comment with other sectors but, in terms of focus and attention, in terms of time, money and indeed personal accountability, as a result of the senior managers regime as well as the regulatory oversight to which banks are subject, I would strongly suggest that they do get it. They are also doing everything they can to help Government, in a co-operative and collaborative way, through public-private partnerships, in order to make sure that the UK is as safe and transparent as it can be, as a place to undertake financial services businesses.

Colin Bell: I will obviously give you an HSBC perspective. It is clearly well known that we have been through a transformative effort over the last five years, with a huge amount of investment. I joined the firm in the middle of 2016, and I was hugely impressed with the effort, not just in terms of resource. In terms of technology investment, we have spent over $1 billion since 2015 on AML-type technology, but there has also been a whole-firm effort in terms of training. Millions of man hours have gone into training. For an institution to tackle this really well, you have to really understand the risk. That is training and education. You have to be able to operate your systems at scale. That is technology investment. You have to recognise that it is a continuous process, because the threat environment continues to change.

For our institution, making a decision back in 2012 to apply the highest and strictest of standards, and apply them globally so we have a consistent standard, has given us a really objective way of assessing this risk. In terms of the level of understanding, the fingertip feel across the organisation for financial crime risk, I think that has been transformative.

Q265 **Chair:** Sorry, what was the figure you gave us just now? How much have you spent?

Colin Bell: On technology since 2015, we have spent over $1 billion.

Q266 **Chair:** That is a phenomenal investment for an institution to make. To drill down a little more, we are looking at other sectors, and I understand you will not be able to comment on other sectors, but it has been clear that the banks have a more sophisticated approach to this than other sectors. From an HSBC perspective, what was it that, in your view, made them realise this was something that was worth or needed $1 billion of investment in technology?

Colin Bell: We are a big organisation. The events, which were obviously very public, back in 2011 and 2012 that led to the DPA were a catalyst for the organisation to really tackle this risk, and to understand and tackle it at scale and comprehensively. If you look at us as an institution, we have reshaped the business over the last four to five years. We have exited a number of countries, as we have reshaped the business, according to a risk appetite. We have exited around 20 countries, just over 20 countries, and a number of lines of business.

In order to manage an institution of 233,000 people across now 60 countries, the scale of the exercise for us is that we process 550 million transactions a month. If you think about monitoring that volume of transactions, that requires a huge investment in technology, because you have to be able to automate those systems. Of those 550 million transactions a month, we will alert, so we will get an indicator of potential concern on, around 450,000 of those. Then we will have to process all of those. There are a huge number of false positives. Part of our effort, as we look at continuous improvement, is focused on how we develop a better use of analytics to try to reduce that false positive rate.

The scale of that particular challenge requires the type of technology investment I have talked about. It is not just the monitoring capability. If you think about the client due diligence that we do, as I have said, we apply a global standard everywhere, in terms of the assessment we make of a new customer who comes on board. That requires systematisation. We have to have a central system that is common across our lines and businesses, and that collects data in a common way. Hopefully, you get the sense of why we need the scale of technology investment that we have put in place.

Q267 **Chair:** You mentioned the DPA. That is a question both from an HSBC perspective, but also from a general sector perspective. Is it the actions of regulators, the threat of fines, the threat of reputation risk, that have concentrated minds in the financial services sector, in the banking sector, to persuade that this level of investment is needed?

Colin Bell: We would take the position that this is the right thing to do. We have a legal, regulatory and moral obligation to protect the financial system against use by criminal actors. It is the right thing to do. We need to be able to manage this risk. In the past, it is clear, given events, that the risk was not managed as well as it should have been. We have now made the type of investment, the type of training, et cetera, to be able to do it. Fundamentally, this is the right thing to do. As we look to grow the business, we have to be able to manage this risk through a growth phase and manage it really well.

Q268 **Chair:** What would you say has concentrated minds?

Stephen Jones: From an industry perspective, to give a UK-based industry number, the last number we have collated in terms of investment in economic crime prevention, technology and compliance is about £5 billion a year, broadly, across the whole range of anti-money laundering, fraud, sanction, counter terrorism and slavery measures, et cetera. In terms of concentration of minds, you are right to say that the more the regulator focuses on it, the more that it becomes consciously embedded in the day to day. I would agree with Colin that people want to do the right thing. They do not want to serve the bad guys; they do not want to facilitate crime, whether that is fraud or otherwise. There is no such as high-volume, low-value fraud. Most frauds ultimately flow back into organised crime. No one working in a bank wants to be facilitating organised crime. From a money laundering perspective, I cannot think of why one would be tempted, as a banker, to facilitate money laundering. It is not why a bank exists.

Having said all that, the complexity of banking, the high volume of banking, means that we have to be very careful to look for where the problems might be. There is a risk, if you become too restrictive in terms of onboarding and then processing the transactions to the clients, that you slow down and make it inconvenient for perfectly legitimate customers. There is always that tension in terms of getting the balance right between ensuring that every onboarding decision is correct, that every transaction and payment facilitated is free of fraud and there is no victim, and doing what customers expect, which is transmitting their money through the faster payments system in 0.17 seconds up to the tune of £100,000. You are managing those tensions on a day-to-day basis as well.

Q269 **Chair:** Before I hand on and we look at some of the risks in more detail, Mr Bell, in your role at HSBC, how often do you have to intervene to persuade people within HSBC that either something they want to do, or somebody they want to accept as a customer, is just too risky?

Colin Bell: Rarely, a handful of times.

Q270 **Chair:** Is it literally less than half a dozen per year?

Colin Bell: Let me go back and talk about the process. We articulate through our policy in terms of our risk appetite. The lines of business understand that they have to work and implement systems to work within that policy. My function provides subject matter experts to sit alongside them and help guide those decisions. What I tend to see is where there is a difference in opinion, so where issues of judgment—and it is normally a judgment—get escalated to me because my team and the business have a different view. I would probably see only three or four of those per month. It is not that I am stepping in; the system is such that it has escalated a difficult judgment for me to take a look at.

Q271 **Rushanara Ali:** I want to focus my questions on Russia. There has been lots of discussion about dirty money flowing through London. The NCA estimates about £90 billion. You both express the fact that much more is being done by the banking sector, but the fact remains that, if it is £90 billion, that is £90 billion too much of dirty money flowing through our banking system. Does Russia pose a unique risk or are other countries in a similar position?

Colin Bell: I will take the second part of your question. I will take the NCA's number as the NCA's number. It would be difficult for me to comment on that. Let us talk about illicit flows. The reason I talked about the fact that, as an institution, we take a global standard, we apply it everywhere and we have a consistent standard in the way we think about customers, when we review current customers and when we look at new customers we want to onboard, is that we have to consider the risk that they present to us.

We think about that risk through a number of components. We think about the country of origin. We think about the type of business that they are in and whether that business poses more or less risk. We think about the products that they want to use. We look at that collection of considerations and we take a view on the level of risk. We use that determination, if we think somebody is higher risk, to look at how much scrutiny we subject them to. It could be an enhanced due diligence process. It could be additional monitoring once they are on board and we are looking at their activity, because we clearly want their activity to be in line with what they say.

As you go through that process, at the heart of it is transparency. As an institution, we are looking for a sense that we know where the funds originated from, so how you got them; the people who have control over them and whether we are comfortable with those individuals; and then where they are going and whether we are comfortable that they are being used for a legitimate purpose. That is not a Russia-specific view of the world; that is a risk view of the world. When you look at Russia, you would apply exactly the same lens to a Russian business or client as you would to somebody from any other country.

Q272 **Rushanara Ali:** You would.

Colin Bell: Yes, because we apply a global standard.

Q273 **Rushanara Ali:** I suppose I am trying to get at whether you have much more of an intensive risk management process for certain countries, like Russia, given those facts. Even if you disputed the NCA number of £90 billion—let us say it was half of that—would you be applying much more intensive scrutiny for a country like Russia, given what we know about the amount of money being laundered through London, or are you saying it is a general approach across different countries?

Colin Bell: It is a consistent approach, to which the risk presented by a country is one input. We would look at a country and think about its potential risk based on a number of eternal indicators. We have the Financial Action Task Force, for example, which provides guidance for the international community and does some really good work on assessing implementation of standards in countries. It will have comments on countries. We have Transparency International, which provides us with a corruption index. Then we have a general view of the geopolitical environment, transparency, the news, et cetera. We look at all those factors.

Q274 **Rushanara Ali:** Where do individuals sit in that analysis?

Colin Bell: They would sit in the general assessment of a country. Certainly, we consider some countries to be higher risk than other countries, but primarily around the transparency piece. We would consider the risk posed by a country to be one input when considering a customer who either had a business incorporated in that country or was domiciled in this country. It is an input. It is an important input, absolutely.

Stephen Jones: There are other externalities that are relevant across the industry. National risk assessments are important in terms of raising sensitivities, as is the imposition of sanctions. There is no question that the UK's risk appetite to Russia in general has changed over recent months. That is an important factor that goes into individual institutions determining what their risk appetite is. There are well-known individuals who have previously lived in London happily, and until six months ago were given visas to do so by the Home Office, who are no longer able to do so. That reflects through, and our members are working closely with the authorities as requested in order to help them understand the quantum and nature of the potential risk in relation to Russia since Salisbury, which has definitely changed risk appetites.

Rushanara Ali: Another question I had was in relation to the subject of the origin of wealth. I think they are called UWOs.

Chair: Unexplained wealth orders.

Q275 **Rushanara Ali:** Unexplained wealth orders, yes. Perhaps, Mr Jones, you could say something about that. What are your thoughts on whether those could be useful in terms of the armoury that banks have?

Stephen Jones: I started the day with the director-general of the National Crime Agency and her deputy, so I think they are incredibly powerful and useful tools. They have started to be applied. The intention, if they were here—and obviously I am not the NCA—would be that they intend to use them appropriately, judiciously and fairly, particularly where political corruption and/or organised crime is suspected, and wealth that is unexplained has ended up in the United Kingdom. The first orders, as you know, have started to be applied.

Q276 **Rushanara Ali:** Not many have yet.

Stephen Jones: Not many have yet, but the industry will certainly co-operate as and when they are used as a tool by the authorities.

Colin Bell: I agree wholeheartedly.

Q277 **Rushanara Ali:** Did you have any further comments about the role of other professions, such as accountancy or the legal profession, and their contribution, which the Chair referred to earlier, in helping to deal with the risks around money laundering? Is there sufficient joined-up working across the sectors? So far, the banks have had to act; HSBC has had to act, given what happened five years ago, related to the high-profile case where there was a big fine. Could there be more pressure applied and more work done at the regulatory level, or in any other sense, to ensure that this happens and that they step up to the plate?

Colin Bell: We know from the industry statistics that the vast majority of reports of suspicious activity come from banks. Almost self-evidently, more could be done by other parts of the regulated sector in terms of reporting. It is also clear to me that we will be most effective in fighting financial crime when we have a consistent view and consistency capability across the whole of the regulated sector, not just in terms of standards and a consistent view of how we think about risk, but also a consistent view on reporting. That comes through the frequency of reporting, but also through information sharing, our ability to share information between groups and our willingness to do that within the correct legal framework. That can only help us get better in fighting financial crime.

Stephen Jones: Collaboration not only between regulated sectors but also between the public and private sectors is critical in winning this battle, and it is a battle, with a very sophisticated opponent. There are examples of where that public-private collaboration, and across multiple private sectors, has worked, such as the Joint Money Laundering Intelligence Taskforce, but it is tactical. The Joint Fraud Taskforce is tactical. These initiatives need to be scaled up. One of the areas where information sharing could help the battle is private sector to private sector. At the moment, there are legal gateways that allow information sharing with the public sector to happen, but the Criminal Finances Act did not take the opportunity to make it easier for banks to share information with one another or with other regulated sectors, like lawyers and accountants. As a tool, with a basic threshold that has to be met, that could be extremely useful in allowing institutions to collaborate in the fight against economic crime in general.

Q278 **Rushanara Ali:** I have one supplementary on this and then one on derisking. I am very intrigued by this £90 billion figure from the NCA. Mr Jones, do you have any sense of which institutions that £90 billion is going through, in terms of a breakdown? Perhaps HSBC can give us a sense of what proportion of that relates to your bank.

Stephen Jones: I do not have precise data. I would just reiterate the point that I think was made by the Prime Minister or the Chancellor, which is that not every Russian is a criminal.

Q279 **Rushanara Ali:** I am not suggesting that. I would like to understand where that £90 billion is going through, and whether you are allowed to tell us that, or whether it is top secret and we are not supposed to know, because £90 billion is a seriously worrying figure if it is money laundering, dirty money, money through trafficking, sex slavery and the rest of it. We all know very well the consequences for people's lives of that kind of dirty money. Does anyone know—if you do not, is it something we should be asking the NCA—where this money is going to and who is laundering that money, if it is not the banks?

Stephen Jones: I do not know; that is the honest answer. We would need to go to the NCA to ask how they calculated the number, basically. They have certainly illustrated a point that large sums of Russian money continue to come through London. Some of that comes through as investment in real estate or other assets. Some of it is legitimate; some of it is not. I do not know how they have calculated it.

Colin Bell: If the NCA felt that part of that money was flowing through HSBC and had an indication of that, I would hope they would come and tell me and we would do something to stop it happening.

Q280 **Rushanara Ali:** I have one final question about derisking. HSBC had to pay a fine of £1.9 billion in 2012 following alleged money laundering of £881 million from Mexican drug barons and a number of other countries in relation to sanctions. This is well documented. As a consequence of that, a number of banks stopped banking with certain charities, with money transfer businesses. I think yours might have been among them; certainly Barclays was. This was the subject of a major campaign, because money could not be sent to developing countries, particularly during the east African famine. It was identified that, in an attempt to try to derisk, a sledgehammer approach was taken to deal with a bigger problem that HSBC and others were responsible for, and a whole series of people were being punished when they had done nothing wrong.

Can you say a bit more about whether your approach is now more proportionate, so that innocent people do not suffer as a consequence of HSBC and other banks needing to prove that they have got their act together and cleaned up their act in relation to sanction busting, rather than what we saw over the last few years?

Colin Bell: Yes. I mentioned earlier, going back to the events of 2011 and 2012, the reshaping of the business and the firm, exiting 20 countries and over 100 lines of business in various countries. We need confidence that we can manage the risk in the footprint within which we operate. Through that process, there is obviously a need to look at the customers you currently bank and make sure you are still comfortable with them, and to set the standards that I have described in terms of new-to-bank customers. They are difficult conversations, in some cases.

At the core, it comes back to transparency. Every time we work with our customer to determine the relationship that we have with them, the core of the conversation is transparency. Do we understand where the money has come from? Do we know who can direct where it goes? Are we comfortable with the transparency as to where it goes? Clearly, in some cases, the firm could not get comfortable with that conversation and exits took place. As far as charities specifically are concerned, we take the work that we do with charities really seriously. We work with the Charity Commission. We provide banking services to 32,000 charities and 106,000 not-for-profit organisations. We have a meaningful relationship with a range of charities, and we work, as I said, with the Charity Commission.

With the work we are doing today, it is a continuous improvement, partly because the threat changes as criminals get smarter, and they are relentless in their attempts, partly because the environment is changing, but partly because we want to be much more nuanced and precise in the way that we understand risk. The work we are doing around data analytics, information sharing and the need for close partnerships, as we have talked about, will help this discussion. It really will help. It will make a difference, because we will be able to get greater insight into activity and transactions, et cetera.

Q281 **Rushanara Ali:** Mr Jones, can you comment on the wider banking sector, if that approach is being taken? Have we learnt from that experience?

Stephen Jones: A very important and delicate balance needs to be struck between ensuring that criminals cannot access the financial system, on the one hand, and being able, as a legitimate person, whether you are a charity, a corporate or an individual, to operate your bank account and have access to it. Certain sectors become targets and are in the spotlight as a result, for example, of national risk assessments that are put out by the public authorities. It is very important that banks are particularly careful. You mentioned money remittance businesses. They have in the past been targeted in warnings to the banks as potential vehicles through which funding passes, for example, to terrorist organisations. We need to get the balance right.

Q282 **Rushanara Ali:** With respect, that was not the case with a number of money transfer businesses, including one in my constituency, that had banking facilities taken at a time when they were playing a very important role in getting money, through organisations like the Mo Farah Foundation, to east Africa. It is quite worrying that they all end up being tarred with the same brush.

Stephen Jones: For humanitarian aid to countries, whether the subject of sanctions or not, there is now a fast-track process that allows banks to explicitly bypass sanctions in order to ensure that humanitarian aid, for example, arrives in areas that, on the one hand, might be the subject of sanctions but, on the other hand, desperately need those remittances to flow quickly. In terms of access to banking, it is very important that, if someone is de-banked, they understand why they have been de-banked, why the institution has derisked, and we are working with the FCA on better communications around that. We also, as UK Finance, support the Government's action group on remittances to ensure that customers in the UK can access legitimate money transfer services.

We have worked with a number of roundtables for other industry groups that have had problems, across sectors such as pawnbrokers, crowdfunding, money service bureaus and e-money institutions. All of those have been subject to enhanced scrutiny, because there have been some bad actors in those sectors and that has been highlighted by the public authorities. We are working with the Payment Strategy Forum at the moment to take forward work for payment service providers that have indirect access to payment systems, to make sure that they get easier access to payment systems. That may well also touch on money remittance service providers. There is a lot going on to make sure people are not inappropriately derisked and de-banked across the sector, but I recognise your comments.

Q283 **Chair:** Rushanara was asking about other sectors that banks have to work with. Mr Jones, you mentioned real estate. We heard evidence previously from the National Association of Estate Agents, which recognised they were a weak link. On the flipside, other regulators may not be as tough on this as the banks' own regulators. In your written evidence to us, you mention HMRC, for example, as potentially being a regulator. We have already heard evidence that it might not be quite as focused on money laundering. You say, "In addition, less stringent supervision by other regulators has seen banks increasingly expected to act as a de-facto regulator. So, one Government regulator (the FCA) can act against a bank who has an MSB as its customer even if the failings are within the MSB which is regulated by another Government regulator (HMRC)". Is there anything you wanted to expand on about the different approaches of regulators?

Stephen Jones: We end up navigating public policy conflicts in lots of different areas, and that is an example in this particular space, which we referred to because we think it is relevant. Money service businesses were used as a specific example there, but there are multiple other regulators that we and our regulators need to be capable of working with on a co-ordinated basis. It is a very complex patchwork of regulators, private institutions, bodies such as the Joint Fraud Taskforce and CMORG, the Cross Market Operational Resilience Group. There are many. Actually, sometimes it is a bit of a patchwork. Sometimes there are gaps in terms of how all these organisations, with all their legitimate objectives, come together. An overarching economic crime strategy that holds all this together and paints a picture that is a little more consistent would help us all, frankly, in the battle against economic crime.

Q284 **Charlie Elphicke:** Mr Bell, I was looking at the comments that the former head of Europol, Rob Wainwright, made earlier this year before he left the role he had. He said, "We have created a whole ton of regulations […] the banks are spending $20 billion a year to run the compliance regime […] and we are seizing 1% of criminal assets every year in Europe". Does that strike you as accurate and do you think it is good enough?

Colin Bell: I have heard those numbers before in a number of forums. In fact, I have discussed them with him. The case he makes is that we need to be more effective in the fight against financial crime. The work we are doing at the moment, as we look at potential improvements to the way we tackle financial crime, is focused on getting a number up, whether or not it is that number, and putting improvements in place. The industry over the last few years, has put in place a layered control framework, so we conduct due diligence on clients; we have transaction monitoring; we screen them for sanctions; and we produce reports that we hand to law enforcement. Through that process, we deal with a huge number of false positives.

There are two major improvements we are really focused on. One is better use of data. At the moment, our monitoring systems just look at the transaction. Of course, if you are looking for a transaction and you see an alert, it is an individual piece of data and you have to conduct an investigation. The false positive rate across the industry is between 95% and 98%. It is a huge amount of expenditure to document false positives. We do find risk, absolutely. We do find risk, so it is good from that perspective.

We want better use of technology. We have machine learning, artificial intelligence and more processing power coming online. We are building prototypes now that would be far, far more effective at finding suspicious activity more quickly, and finding it more precisely, which of course is helpful then in terms of reporting. If we can complement that with information sharing—Stephen talked about bank to bank, but Government to Government as well—and look at international information sharing, we have an opportunity to take a step change and make a big difference, a big dent, wherever that number starts, whatever the baseline is, and to have some meaningful improvement.

Q285 **Charlie Elphicke:** You talk a good game, but I have constituents who suffer push payment fraud, who think they are buying a car and get nothing whatsoever. This continues unchecked. The banks seem to spend billions and billions on compliance and all these wonderful systems that you say are working so very well, and yet my hard-pressed constituents, many of them pensioners, are completely taken for a ride by fraudsters. It is not working, is it?

Stephen Jones: May I take the APP-specific question? APP is a very, very unfortunate crime, and a crime is what it is. There are three parties to that crime, typically. There is the victim, who has instructed their bank to make a payment, the recipient bank to which that payment is ultimately made, and the paying bank. The supposition with authorised push payment fraud is that either the paying bank or the recipient bank must have done something wrong. Typically, the supposition is that the recipient bank must have done something wrong for allowing the fraudster to open a bank account.

The evidence we have seen and the work we have done suggests that, in the vast majority of cases, accounts are opened through perfectly well-undertaken KYC processes, that a significant proportion of receiving fraud accounts in the UK are opened by British passport holders aged 16 to 25. A number of them are students. They open their account perfectly legitimately and are then compromised. It is very, very hard for banks' systems to detect when an account that has been legitimately and properly opened becomes compromised by a fraudster who uses that account as the vehicle to which monies are transmitted mistakenly by the victim.

The work we have done over the last six months with the consumer groups on APP fraud has resulted in the issuance of a draft code. That draft code essentially seeks to formalise standards of reasonable behaviour that a paying bank and a receiving bank should evidence in order to demonstrate that they have done everything that is reasonable for them to do to in facilitating a payment, which is after all what the customer has asked them to undertake as banks within the payment system.

Q286 **Charlie Elphicke:** You are saying responsibility should rest with the victim.

Stephen Jones: No, I am not. I am saying that there are circumstances where the paying bank has done what it is supposed to do according to this standard, and the receiving bank has done what it is supposed to do in accordance with this standard, including issuing warnings to customers about whether they are really sure they know who they are paying the money to. My own bank has warnings coming up to me when I make an electronic payment asking whether I am being pressurised. Do I really know the person to whom I am paying the money? Is this the first time I am using these bank account details? All of those are deliberate warnings that are put in the system to make me step back and think twice about the payment I am about to undertake.

The code codifies this for both the sending bank and the receiving bank, and suggests that there may be circumstances where the banks have actually done everything that they should do. In those circumstances, there was originally a suggestion that the bank should nevertheless pay money back to the victim. In some circumstances, banks will pay money back to the victim even if they have done everything that is reasonable, particularly if the victim is vulnerable. There is a broad public policy conversation we need to have about who should pay for a victim of crime, which is what we are describing here: your constituent who has been conned into making a payment. Is it the banks that should pay or is it, for example, as in the case of a crime resulting in an injury, a public compensation fund? How should that fund be constituted and how should funds be found in order for those payments to be made? Where banks have not complied with the standards that are determined in the code, the code suggests that the banks should pay the victims back.

Q287 **Charlie Elphicke:** Mr Jones, this is a shift in position. Previously, UK Finance put a lot of pressure on the regulator not to make any change in the rules. Previously, UK Finance used to engage in, frankly, what I would describe as victim blaming. Now you are saying, "We are not blaming the victims, but it is just not our responsibility; the risk should be socialised". Do you really think that is good enough?

Stephen Jones: I do not think we have ever blamed victims. I would be very surprised if anything has come out of UK Finance to suggest anything other than a victim—

Q288 **Charlie Elphicke:** You fought tooth and nail against the change by the regulator. We have been through this in this Committee. Your organisation, your trade union, effectively, UK Finance, fought against changes by the regulator to protect victims. The regulator is now pushing those through, thanks to pressure from this Committee. Is that not the case?

Stephen Jones: I do not recognise the statement you are making, but if I have made a mistake in doing that I will write back to you.

Q289 **Charlie Elphicke:** Can I also take issue with this? If the risk is socialised, the banks will continue as they have done, without any incentive, any financial incentive, to sort out the system. Is the right thing not for the banks to take the risk of this kind of fraud, because that will make sure that the banks are much more cautious about account opening and, indeed, interbank transfers overseas, particularly to other parts of Europe?

Stephen Jones: You risk setting very, very perverse incentives that could be exploited by organised criminals if you create a system where a responsible bank at either end of the transaction and a responsible customer have all done what is supposed to be done and the bank pays in all circumstances. In our view, you will end up attracting more fraud into the system, not reducing fraud.

Q290 **Charlie Elphicke:** Moving on, let us look at the wider remit of Europol. A study by Europol, Mr Bell, indicated that, in 2014, financial intelligence units received almost 1 million reports of suspect transactions, 65% of them from the UK and the Netherlands. First of all, is there an issue that a lot of countries do not seem to be taking this kind of reporting seriously? On the other hand, is there a risk that, in the UK, we have a checkbox, tick-box culture where we just file a report, and it means it is impossible to find the needle in the haystack?

Colin Bell: From an international perspective, I go back to the decision that we made as an institution to apply a common standard, because we want to be comfortable that we are consistent in the way we assess, identify and report financial crime, irrespective of the jurisdiction within which we operate. From an HSBC perspective, we have that level of consistency. If you look across Europe, a joint working group was recently put together by the European Union to look at consistency of implementation of AML legislation in countries. I think they have identified some shortcomings that are going to be addressed by the working group. No doubt, further information will come through that process.

In terms of the volume that we get in the UK, I would take a slightly different position on that. It is about what we do with that volume. It is about how we consume it and how we analyse the information that they present. If I take the US as a comparison, five years ago, maybe, in the US they went through a big upgrade of the way they ingest suspicious activity reports. They introduced electronic filing, something called a common data model, so it all arrives in a common format that allows law enforcement to query the data, to have direct access to it, along with regulators. It allows FinCEN, which is their financial intelligence unit, to run proactive analytics over that data. It has enabled them, in that particular case, to become slightly volume agnostic, if I can put it that way. The analytics that they can run allow them to find things in that large amount of data that have not been found before.

We have an opportunity to do something similar in the UK. It is less about volume, because financial institutions will be conservative if we have a suspicion. The threshold is that you know, you suspect or you have reason to suspect. If we cross that threshold, we will file. If we file with standard information and we can interrogate that data in a way similar to the way I have described, we have an opportunity to see things in that data that we have not seen before, which is why we are hugely encouraging of the SARs reform programme that is ongoing in the UK.

Q291 **Charlie Elphicke:** This is my last question, if I may. Mr Bell, you are a large international bank. You have lots of experience of systems all round the world. How do UK systems for combatting economic crime compare with other jurisdictions such as the US, and what do we do better? What do we do worse? How can we up our game?

Colin Bell: Inevitably, jurisdictions do different things well. JMLIT is a standout example. Stephen made the point that it is tactical. It is still the best example we have as we look around the world for information sharing. We recognise within JMLIT the steps we can take to improve. The UK has been a really strong voice at FATF around information sharing. We have led that discussion with the US. That has been hugely influential in some of the additional guidance that has come through FATF.

Looking at areas to improve, we talked about the SAR process and our ability to look at the SAR. There is an opportunity for simplified and common governance between the public and private sectors. That is built partially on information sharing, and Stephen has made the points on information sharing. We could have a simplified public-private partnership with closer governance.

The National Economic Crime Centre is a real opportunity for us, if we land it right. Really, it is about political leadership and then dialogue between private and public sector to really land the NECC. If we get that right, the UK has a real opportunity to take a lead internationally in the way we tackle this.

Q292 **Wes Streeting:** Good afternoon. Mr Jones, in your written evidence, you said, "Firms also note that whilst the financial sector has increased resource on economic crime, there has been a reduction in public sector resource in this area. We have also seen banks, as a highly regulated sector, being increasingly required to deliver functions to supplement that of the state". Are you still worried about this imbalance? Perhaps you could elaborate on which particular functions you think banks are currently performing that should be properly conducted by the state.

Stephen Jones: We have been talking about the SARs reform programme, which is a very good example of private and public sector partnership coming together in order to build a system that is more effective, more substance based, better resourced, makes greater use of the technologies Colin has mentioned and ultimately, at the end of the chain when all these SARs have been submitted, has investigative resource that is there and available, and is able to interrogate the SARs in a manner that potentially leads to arrests, because ultimately we want the bad guys locked up as well.

At the moment, with the SARs reform programme that is proposed, at least for 2019-20, the ask of Government is that that be funded by the private sector. The suggestion is that, over five years, rebuilding a fit-for-purpose SARs programme will cost somewhere in the realms of £500 million. Again, the suggestion of Government is that that should be largely funded by the private sector.

The private sector is also increasingly being asked to provide human capital and expertise to public authorities. Of course, that is welcome because working together will hopefully make economic crime and the fight against it more effective. But there is no question that there is substantial pressure on public resources and, increasingly, the ask therefore comes from the authorities to us, the private sector, to fund that. The Dedicated Card and Payment Crime Unit, which is a joint venture between the Metropolitan Police and the City of London Police and targets the organised crime end of card and payment fraud, is funded by UK finance, i.e. our members, the banking sector. The Banking Protocol is training police forces up and down the country to work with bank staff to spot the signs of individuals being coerced to withdraw large amounts of cash at bank branches. Both programmes, DCPCU and the Banking Protocol, have been enormously successful. They are funded by the private sector.

The point we are making is that we need to find a way of understanding what the resourcing model is together, in order to enhance economic crime protections. It may well be that, for the no-blame scenarios in APP fraud that we were discussing with Mr Elphicke earlier, and for other SARs reform investment programmes, we need to think about some form of central pool, which could be a levy, for example, on payment transactions. We need to have a debate about whether there is a funding mechanism we can create where a small amount is charged against each transaction, in order to put money aside to be used for public-private investment in enhanced economic crime systems. That is the debate that we think is worth having at the moment.

Q293 **Wes Streeting:** That is really interesting. I had always thought that the financial service industry was quite resistance to transaction taxes, particularly where they were applied unilaterally by one nation state, as opposed to nation states acting together. Even when a Tobin tax was proposed on a European level, there was heavy resistance. We were warned that this would be a disaster for UK financial services and the City of London. Have you changed your view on that?

Stephen Jones: I am not talking about a financial transaction tax in the wholesale markets, which I think is the context to which you are referring. I am talking about the payment system. For example, we have a very unique opportunity at the moment because the payment services operator is designing a whole new payments architecture for the payment system in the UK, and all payment service providers will be required to build to that specification. It may be that, in the building of the architecture, we could put a tiny levy on each payment that goes through the architecture, in order to provide an insurance pot that can be used, for the circumstances we are describing, to make the system more effective against economic crime.

Q294 **Wes Streeting:** We will try to get customers to pay a bit more, not just the banks. Is that the argument?

Stephen Jones: Customers will pay if the banks have to pay. There is no such thing as a free lunch here. The question is how the cost can be fairly distributed across the system.

Q295 **Wes Streeting:** Do you accept that the Government are right to ask the private sector to pay more to tackle economic crime?

Stephen Jones: We need to have a debate about how that is funded. There are circumstances where the private sector can and should pay. As I mentioned, we estimate that it is paying about £5 billion per year in the UK in the fight against economic crime. There are also circumstances where there is a public sector requirement as well. Sometimes it is very important that both sides see each other investing in a programme, to demonstrate that both sides have skin in the game in making the system more effective.

Q296 **Wes Streeting:** I totally understand that point on principle. To be kind to the Chancellor for a moment, because not many people are, if you are asking the Treasury to find this money, it has to be found from somewhere. The Chancellor has already made a £20 billion pledge to the NHS, and we are not really clear about how that is funded. Community policing, in my community and countless others across the country, is at the lowest level it has been for some time. Do not get me started on what is happening with people in terms of the universal credit rollout and disability benefit.

In the grand scheme of things, I appreciate the enormous financial contribution that financial services make to the UK's tax base, without which we would not fund our public services. Those are debates I have in other parts of Parliament. At the same time, whether it is quantitative easing or bank bailouts, the financial service industry has also been one of the biggest beneficiaries of state benefits. It is not unreasonable in this area that we are asking financial services to cough up because, if it is not you guys who are paying, it will be our constituents or cutbacks in other areas of public services. No one is going for that at the moment. By the way, my voters are certainly not going to pick you over the Chancellor in this argument.

Colin Bell: From our perspective, we have talked about the amount that is spent by the financial services industry to combat financial crime. We have implied through a lot of that discussion that we can be more effective in that fight, and I have talked about some of the ways that we might be able to do that. With that effectiveness, hopefully, comes more efficiency and that provides the foundation for a discussion on a sustainable funding model. That sustainable funding model conversation needs to take place without details about what it might look like. It is a core part of the discussion, as we look at this economic crime review programme.

Q297 **Wes Streeting:** The point that you and Stephen have made is well made and something we will take up with the Treasury. Finally, I am keen to get your views on how you think the National Economic Crime Centre is taking shape and what kind of interaction you have had with it so far. Secondly, you talked about having a clear model in place in terms of the funding to tackle economic crime. Are there merits to having one body in

Government taking sole responsibility for AML and anti-economic crime defences, rather than the patchwork system we have today? We are constantly told that agencies are working well together, but I am interested in your views about whether there should be agencies, plural, or whether this would better rest with one body.

Stephen Jones: It is always hard, because there is a regulatory function and there are multiple different areas that need to be regulated, so the regulators need to be expert in what they are regulating. Therefore, there are multiple areas that are relevant here. There is an enforcement function. You have the police, the National Crime Agency, the security services. They all have a legitimate place. You have the private institutions and how they all come together. Then you have fora that exist where those bodies come together to co-operate in order to make themselves work more effectively together.

The NECC is a very important initiative because, as a tasking body within the NCA, but with the support of, for example, the Financial Conduct Authority and others, it should provide a very good vehicle to, in a sense, task those many bodies that you describe as to where the focus should be, where the priorities are, the overall strategy for economic crime, today's No. 1 thing that everybody should be focused on, and what may need to be deemphasised in order that the resource and the focus can go on that one area. At the moment, that strategy and that overarching piece—"SARs reform is what we are all going to go after now"—is sometimes missing. At the moment, we are focusing very hard on SARs reform, to make that system more effective in the fight against anti-money laundering. We hope not to dilute any other form of counterterrorism, sanctions or slavery activity in doing so. Having a tasking body at the top of what is a complex architecture, but one that is quite difficult to change, is a good thing.

Colin Bell: It is really important to understand those three constituents: law enforcement, regulators and the private sector. They are three legs of a stool that all have to talk together. When I talk about how we land the NECC, if the head of that organisation has a co-ordinating authority or a tasking authority across the three elements and we can have a shared set of priorities, that will be a significant step-change improvement in terms of the way we tackle this at the moment.

Q298 **Mr Clarke:** Thank you both for coming in today. Mr Jones, in the written evidence to us, RUSI, the Royal United Services Institute, gave some really devastating commentary about the Office of Financial Sanctions Implementation. Specifically, it said, "There is no evidence that OFSI acts as any sort of deterrent to UK-based sanctions violations". Is that a fair characterisation?

Stephen Jones: It is an important body. We work with it very closely.

Q299 **Mr Clarke:** You disagree with the RUSI.

Stephen Jones: We work with it closely on drafting and issuance of industry guidance. Equally, sanctions implementation is as much a matter for individual institutions as it is for a central tasking body. The area of sanctions, as you know, is very complicated. There is a lot to be understood. There is a lot to then be implemented within individual firm risk appetites. Often, there are significant cross-border conflicts, which global institutions have to navigate when they are dealing with, for example, Russia and Iran, where different parts of the world in which they operate have different standards or requirements for sanctions.

The EU blocking regulation at the moment is seeking to ensure that European institutions do not stop their banking activities in Iran, while at the same time the United States, as you know, has withdrawn from the Iran-related nuclear deal and has re-imposed sanctions on Iran. Anyone who operates in both Europe and the United States has a very unenviable tightrope to walk. I do not think OFSI is necessarily going to be able to help in those circumstances. That becomes a decision for individual firms about whose rules they are going to breach, fundamentally. Typically, they will err on the side of caution. Colin can talk about that as a global organisation in terms of HSBC's context.

Q300 **Mr Clarke:** In terms of the performance of OFSI within the constraints that exist and trying to navigate a range of different regimes, are you confident that it is, in fact, fit for purpose?

Stephen Jones: Yes. We have had no problem with OFSI in terms of the work it is seeking to do. We work very closely with it in terms of, as I say, drafting of new legislation, ensuring it is functional and capable of being implemented, and providing guidance to members.

Q301 **Mr Clarke:** Mr Bell, is that your experience?

Colin Bell: I personally have not had a huge amount of direct contact with OFSI. Our UK teams see the relationship as an important one. It is an important provider of guidance. We have had comments internally about the licensing regime, because there are quite often some very practical elements in how we manage assets internally. For example, when you ring fence, you sometimes need to move assets from one side of the ring fence to the other. That is a technical violation and you need a licensing regime. The agility and the response of that licensing regime is something we have been discussing with OFSI to improve.

Q302 **Mr Clarke:** In an earlier answer you gave to Mr Elphicke, you referred to the fact that the UK has had a really strong voice at FATF. Is that the right pronunciation?

Colin Bell: Yes, the Financial Action Task Force.

Mr Clarke: What have we secured and what should we, as a country, be seeking in terms of further gains to try to make sure that OFSI's interaction with other agencies is as smooth and effective as it can be?

Colin Bell: Do you mean in terms of OFSI specifically or information sharing more broadly?

Mr Clarke: The question is probably both: specific and general.

Colin Bell: In terms of the work the UK has been doing on information sharing, we can have situations as a global institution where we have identified networks of criminal actors, and they are transnational in nature. Criminals are entirely unconstrained by international boundaries, entirely unconstrained by data privacy laws. We may have identified suspicious behaviour and filed reports in multiple jurisdictions. In many cases, our ability to tell other jurisdictions that we have filed a suspicious activity report somewhere else is restricted by law. We are not able to do that. Even intra-group, sometimes it is difficult for us to share the information internally between jurisdictions.

The UK, as I said, has been very vocal in this. The work with FATF is about introducing guidance within the FATF principles that seeks to find a middle ground, and we recognise how difficult that middle ground is, between data privacy, which is obviously what nation states are trying to protect, and the fight against economic crime and how we do that internationally. It is an incredibly important debate and one that we feel very keenly, as an international institution.

Q303 **Mr Clarke:** You touched a moment ago on licensing regimes. It is worth taking you to another point I wanted to raise, which is that, in your evidence, from HSBC's perspective, you said that you would welcome discussions on improving our licensing regime, which would reduce unintended consequences, including by removing barriers to the NGO sector's ability to move humanitarian aid within the financial system. Is that something you could expand upon?

Colin Bell: Yes. When we are trying to move resource in and out of countries that may be subject to sanction but are being served by NGOs, an agile licensing regime that allows us to release the funds that support medical, education, et cetera, is clearly for the common good.

Q304 **Mr Clarke:** Is it not very agile at present?

Colin Bell: It is a developing capability. Let us put it that way.

Mr Clarke: That is a very tactful way of putting it.

Q305 **Chair:** Mr Jones, I think you were saying earlier on that there is now provision in place.

Stephen Jones: Yes, it came across my desk last week. I think it related to Indonesia.

Chair: It is very recent.

Stephen Jones: It was very quick. It was an order that was issued. It was saying, in relation to the tsunami damage there, to the extent that there were any restrictions, "Boom, no, it is fine; money can go to NGOs that are operating in this area". I saw it come across my desk and thought, "This is good. This is fast. It is timely". Maybe it is getting better.

Q306 **Mr Clarke:** Did that catch your eye because it is unusual, though?

Stephen Jones: Well, possibly. Colin makes a good point. We need to be agile and fast in these circumstances.

Q307 **Mr Clarke:** In terms of how sanctions implementation can be improved from the wider perspective of financial institutions, what would be your top asks of Government?

Stephen Jones: Do you mean in terms of improving the overall sanctions regime?

Q308 **Mr Clarke:** Yes. We are hearing that it has significant flaws, some of which are perhaps unavoidable, given the constraints.

Stephen Jones: I would like to write back to you with the details of what we are doing. There is an awful lot going on in terms of the Sanctions and Anti-Money Laundering Act and its passage through Parliament. We are seeking to brief and inform to the extent that there are lacunas in that Act that have been left by the wayside. Can I write back to you if there is anything missing?

Q309 **Mr Clarke:** I would be delighted. That would be really helpful. Thank you. The NCA, which of course has a pivotal role in all this, given that state actors start to get involved as well, notes that the scale of financial sanctions breaches is unknown. However, the expanded use of high-profile international sanctions, strongly backed by the UK, against regimes such as North Korea, has increased the risk to the UK of sanctions evasion. How have financial firms reacted to that warning?

Colin Bell: We apply sanctions—UK, US, EU, UN, et cetera—as a matter of policy, but always have to be aware of the primacy of local laws in particular jurisdictions. It is a self-evident truth that, when you put restrictions on groups or countries, et cetera, they will look for ways to evade that.

Q310 **Mr Clarke:** Has that manifested itself?

Colin Bell: We see increasing sophistication of methods as sanctions go in place. When you are looking at state-level actors, you are dealing with some of the most sophisticated capabilities, in terms of creating shell companies and layers of shell companies, using conduits and third parties, and being able to move money off shore. An institution like ours is experienced in looking for those typologies, so seeing the methods they use, but they evolve over time.

Again, the most effective way that we tackle this is where we share information, particularly with Governments. Governments have information that the private sector does not have. We have information

Governments do not have. We have tackled those most sophisticated of actors most effectively where we have brought those two pieces together. Over the last couple of years, sanctions have been an area of real intense focus when it comes to that public-private information sharing.

Q311 **Mr Clarke:** Do the two dovetail well? Sometimes they are two very different worlds coming into contact with each other. Are there mechanisms in place?

Colin Bell: It is difficult to discuss in too much detail, for reasons I think you would understand, but over the last two or three years we have really developed the mechanisms for that targeted information sharing between public and private, so we can take action quickly and we can ensure that we close down potential evasion wherever we see it.

Stephen Jones: To reiterate the earlier point, the legal gateways tend to exist between the private sector and the authorities in order to do that under the Crime and Courts Act, for example, but bank to bank, or private to private, they do not currently exist. We need to keep thinking about that and keep thinking about what the safeguards need to be, on the one hand to preserve data privacy, and, on the other hand, to increase our effectiveness. It sometimes causes real problems. In the case of fraud, the ability of a receiving bank to slow the money down, to stop it, to freeze it without a court order is quite limited. Many of our members are starting to do that, but they do so at their own legal risk at the moment.

Q312 **Mr Clarke:** It is not a risk they should have to bear. They are trying to do the right thing. This is my final question. It is not on sanctions; it is regarding your answer to Mr Elphicke about who bears the balance of risk in the event of malfeasance. You said the industry's view is that, were the industry itself to bear the risk of losses in those circumstances, that would increase the risk of crime. Is that a fair summary? Can you just explain why that is? I do not understand why criminals would care.

Stephen Jones: I was speaking specifically about the no-blame scenario. We have set up a code. The code establishes an evidential burden for the consumer and an evidential burden for the paying and receiving bank. All three parties have done what they are supposed to do under the code and the consumer is still a victim of fraud. Fraud has got through the system. They are the victim of a crime. Who should pay? Our concern is that, if there is an automatic presumption that the banks will pay in all circumstances, the likelihood is that you will have organised fraudsters focusing on an indemnity, effectively, that exists in the system, which is underwritten by the banks, because of the existence of that indemnity. It is easy money, basically.

Q313 **Mr Clarke:** Is there not the state indemnity at the moment, though, in that the taxpayer picks up the tab?

Stephen Jones: No, not in those circumstances. There is no question that they are unfortunate circumstances. There are victims of crime here who are bearing the associated cost, but the state is not picking up the bill in those circumstances at all.

Q314 **Mr Clarke:** There is no right for compensation, necessarily.

Stephen Jones: Not at the moment, no. There are circumstances in which victims of authorised push payment fraud who have been conned, and therefore have been the victim of a crime, are required to bear the cost of that crime. The example I used as an alternative in other parts of the criminal justice system is the Criminal Injuries Compensation Authority, where, if you have been injured as a result of the crime, money is made available for recovery. The emotional injury associated with financial fraud, particularly for an elderly or vulnerable person, is very significant, and many banks, on an ex gratia basis, will refund where a vulnerable person has been the victim of that kind of fraud, but it is not organised at the moment.

Q315 **Chair:** I should just say that a lot of this particular part of the economic crime inquiry is looking at the high end: money laundering, sanctions and everything else. We are going to return to what you might call retail banking, authorised push payment and crimes like that at some point. I am sure that Mr Jones at least will be back before us potentially giving evidence. I am sure he will be delighted to hear that.

I just want to ask one question. Mr Bell, in your evidence you talked about criminals entirely unconstrained by international boundaries, which I think we would all agree with, and the need for international co-operation. Earlier on, Charlie talked about Europol. I am sorry to bring in the Brexit word so early on in proceedings this autumn—it is not that early—but do you have any concerns? Perhaps, Stephen, you might have concerns in terms of the sector. Does the UK leaving the EU cause concern in terms of information sharing, operation of Europol, or is it the case that all that has to happen is at such an international, global level that Brexit does not have the impact you might think?

Colin Bell: In the short term, we have been informed that the Government intend to implement the fifth money laundering directive. That would retain parity in terms of the standard we apply, so we would not see an impact in the short term. Obviously the detail of the deal—

Chair: We are looking at that too, so do not worry. We have that delight to look forward to, later on in the autumn.

Colin Bell: It is a key element of that. Anything that hampered the sharing of information between institutions as a result of Brexit would clearly make it more difficult to fight financial crime.

Stephen Jones: I have nothing to add, Chair. It is incredibly important. There are negotiation tactics at play in other aspects of the financial services negotiation that are preventing co-operation and memorandums of understanding being put in place between supervisors. I would very much worry if that were also to pervade action between criminal justice authorities working with the private sector to prosecute economic crime. Economic crime is a borderless crime. Many of the bad actors are not based in the United Kingdom.

Q316 **Stephen Hammond:** Gentlemen, good afternoon. In the National Strategic Assessment of Serious and Organised Crime earlier in the year, the NCA noted that money laundering using corporate structures and financial markets continues to come to the attention of law enforcement. In the NRA, it noted that there is a significant emerging risk of money being laundered through capital markets. I wonder, Mr Bell, if you have detected that or attempts to do so through your bank. If so, could you give the Committee some flavour of how it is presenting or exhibiting itself?

Colin Bell: I will give you the most high-profile example, which is not an HSBC example, which is mirror trading. We have seen, with recent enforcement actions, the use of mirror trading to essentially move currency from one country to another through the buying and selling of securities and that transfer of value. That is not an HSBC example, but it is a good example of the challenges of capital markets.

At the moment, our focus is on monitoring our capital markets intensively for market abuse, so insider dealing, mispricing, front running, all the types and terms that people will be familiar with. Our focus is on ensuring that, where we see that type of thing happening—so it might be mispricing; it might be insider trading—we do not just look at it as a market abuse event, but we consider it from a financial crime perspective. We look at the parties that might have been involved in that transaction, the customer, their connected parties, and we think about the financial crime element. Where we consider there to be suspicion, we will file the necessary report with the authorities so it can be acted upon.

It is about making sure that the link between well-established market surveillance capabilities in the capital markets, and financial crime and reporting, is robust and comprehensive. We are also—again, it is part of an onslaught of new technology— looking at whether we can do more in the back end to monitor particular transactions, particularly if you think about the foreign exchange market and other high-volume markets like that, as to whether we can see activity. That work is pretty early days.

Q317 **Stephen Hammond:** In your judgment, are all or most of the participants in capital markets taking the same sort of view, with the same sort of governance to ensure that is detected, as you are?

Colin Bell: The FCA published a guidance note at the end of Q1 this year. It was a consultation note, but we all assumed that it was due to go live in October. It requires institutions to take that approach, so yes, on the assumption that people have implemented it.

Q318 **Stephen Hammond:** Mr Jones, in the written evidence UK Finance provided to the Committee, you noted what the NRA had said about laundering through capital markets. The written evidence UK Finance provided said that has been made without sufficient detail or supporting analysis provided. I wonder if you could detail to the Committee where you think those gaps are. Also, have you spoken to the Government or have you tackled the Government on the need to have this evidence if they are going to make that statement?

Stephen Jones: The fact that the FCA has come up with a consultation paper in the interim, recommending practices, is quite helpful, whether or not there is evidence of large-scale usage of capital markets. We have seen examples in other jurisdictions, in peripheral European Union states, where those mirror trades have been more prevalent in facilitating the movement of money. We have to be very careful, wearing a parochial UK hat, rather than a European Union hat, to ensure those practices do not move into the UK. It may well be that the NRA was looking at other EU states and reflecting a concern that that those practices are transmitted into the UK. We have not specifically raised with the NCA, or with the authors of the national risk assessment, where the evidence of those capital market practices in the UK came from.

Q319 **Stephen Hammond:** Should I take it from the evidence you have supplied that the view of UK Finance is that, broadly, the UK capital market structures are less susceptible to this crime than peripheral EU states?

Stephen Jones: It would be wrong to be complacent in any circumstances or to assume that what happens elsewhere could not happen here. I have great confidence in both our capital market actors and indeed the regulators, and the FCA guidance is welcome.

Q320 **Stephen Hammond:** A corollary to this, but slightly separate, because it goes into mainstream money laundering, is the formation of companies, the activities at Companies House and the register that is kept there. Can I ask three basic things? First, how much are you seeing, across your range of activities, the formation of shadow, false companies as a feature of economic crime? In your experience, do you think Companies House has the resources, both financial and knowledge, to detect this? Third, there is a great cry for a public register, but a public register is as transparent as it is monitored, on the basis that "Mickey Mouse Enterprises" could register as a company. Might we not do better to concentrate on signing up to the international regulation standards that some of the overseas territories have signed up to, and yet we criticise them?

Stephen Jones: There is no question that we support the work of Transparency International in this space. It is very important to have, in our view, good beneficial ownership registers that are not only good at the point of incorporation but are then maintained through a corporation's life. A robust company registration and beneficial ownership structure significantly enhances the KYC obligations of a bank opening a bank account for a corporation.

Q321 **Stephen Hammond:** Do you not agree that a public register is not enough, that we need both a public register and to be signed up to the sort of standards we see elsewhere in the world, which others have signed up to?

Colin Bell: We take a very simple position on this. We absolutely support public registers. They are best when they are accurate, verified, accessible and comprehensive. You can apply those four principles as a reasonable test to any public registers. I am not sure—I think long and hard about this—whether there is really a best practice example of a public register at the moment.

Q322 **Chair:** Anywhere in the world?

Colin Bell: Anywhere in the world. Transparency International does an analysis of this.

Q323 **Stephen Hammond:** I understand the pressure for public registers. It seems to me, to your point about verification, that there needs to be adequate verification of what is going on the public register. It is fine to have a public register, but there are other standards that certain people have to sign up to. Their registers are not necessarily public, but they are at a higher standard of verification. Surely in the UK we should be aiming for both.

Colin Bell: As I said, those four principles applied to a beneficial register would be a best practice, no question. On the use of shell companies, absolutely, shell companies are a well tried and tested mechanism for high-end money launderers. They create layers of them through a layering process within the financial system to try to obscure the origin and source of funds. It is something that I think all major financial institutions have developed various techniques and indicators to try to look for. Not all corporate service providers are bad. Some of them provide a good service, but there are those that are serving shell companies. Understanding the distinction is something that, as financial institutions, we get better at, but it is an arms race.

Q324 **Stephen Hammond:** You have touched on my final question. Given the state of the resourcing at Companies House and the state of the UK register, how easy is it for you to identify companies you wish to query? How easy is it for you to make the adequate investigation into the companies you wish to query?

Colin Bell: Companies House is one input for us. If we are looking to make a judgment on a company, we will want to understand beneficial owner through to natural person, so you cannot have a trust owning a trust, et cetera. We look for beneficial owner through to natural person. We can start with Companies House, but we will always then work with the company and additional information to verify that data. It is an input and it is, in the vast majority of cases, a helpful input, but it is not a deciding factor for us. We go further than that information.

Q325 **Catherine McKinnell:** That leads quite helpfully into what I wanted to ask you about in relation to information sharing, because you have referred to it a number of times in your evidence today and in the submissions that you provided to us. You have asked for greater permissiveness about information sharing in order to combat this sort of economic crime. What in particular are you looking for, in terms of information, and what are you hoping to achieve from the increase in its flow?

Colin Bell: There are maybe two aspects, from our perspective. One is what we have termed pre-suspicion information sharing. I described the threshold that we have to pass before we file a suspicious report, so knowledge, suspicion or reason to be suspicious. At some point before that, we will be conducting an investigation. That investigation will be triggered either by an alert from our monitoring systems or by a member of staff who has indicated that they have seen something they did not like. At that investigatory stage, before we have made the decision, it would be helpful, where we had an indication that there was a link to another institution, if we could share that information, and if we were then able to have a cross-institution discussion about whether we felt there was suspicion. That is one particular piece.

The second element is the international information sharing that I have talked about. That is to try to overcome—again, we appreciate the delicate balance between privacy of personal data and cross-border sharing of information—some of the restrictions we have, so we can inform other jurisdictions where we have seen suspicious activity that may originate in one part of the world but then flows through, cross border.

Stephen Jones: In certain circumstances, which Colin has outlined, we would also like the ability to slow payments down. Perversely, the payments system works so quickly that at times we cannot trace the money as quickly through legal gateways as the money is physically moving between multiple accounts. The ability to share information but also to temporarily pause the movement of money across multiple accounts would be extremely helpful in terms of, on suspicion, making the act of tracing a victim's funds through to the end account less difficult. Typically, money will move through multiple accounts, not to a single account.

Q326 **Catherine McKinnell:** Why do you think this level of information sharing is not currently happening? Are there data issues with it? Is that the big challenge? What is stopping this from happening now?

Colin Bell: It is the legal framework. It is the law. As I said, on the international stage, it is a criminal offence to tell someone outside that jurisdiction that you have filed a SAR. Again, domestically we are not allowed to share that information at the stage of pre-suspicion. Once we get to a suspicion stage, we have the JMLIT mechanism. That is why JMLIT is so effective.

Q327 **Catherine McKinnell:** I guess what I am wondering is how you get to that level of pre-suspicion. The point is that you report that information and then that becomes part of an organisation that is looking at the picture more globally. Why do you need that additional information in order to report your suspicions?

Colin Bell: Partly it takes us back to the richness of reporting and the quality of information we want to give to law enforcement, because a single bank may see only part of the picture. As I said earlier, we will be conservative. If it is a judgment, we will file, but if we can have that conversation with another institution we can put together a much richer picture of the network that we may think is at work, so what goes to law enforcement would be that much more effective. Otherwise, we are passing half the puzzle to them, and they have to pick up the SAR and add all the bits together by going out to other institutions.

Q328 **Catherine McKinnell:** Is that the thinking behind the current framework? Is there any resistance to changing the current legal framework in order to enable banks to carry out some of that pre-suspicion communication, rather than handing it over to an external organisation?

Stephen Jones: We made suggestions and moved amendments in Parliament when the Criminal Finances Act was going through that would have enabled greater certainty regarding that information sharing. For whatever reason, they were not taken through, so the Criminal Finances Act did not implement the kind of information sharing that we were suggesting at the time would have been helpful.

Q329 **Catherine McKinnell:** We are here to be convinced, in terms of how we change that legislative framework and how we make the case for changing that legislative framework. You have no views on why it has not been changed.

Stephen Jones: Perhaps we will write back to you, in terms of the amendments that we moved and what we know of the reasons why those amendments were not taken forward on to legislation. We will write back to you on the specifics of what we know about that. Obviously there may be internal Government legislative aspects that are not public, that we are not aware of, in terms of why they were not taken forward. We are very happy to write back to you on that.

Chair: The Minister is coming before us, so if you are able to write back before that session that will be helpful. We can share the date with you. We can follow it up with them.

Q330 **Catherine McKinnell:** On a slightly related issue, the Serious Fraud Office has also suggested reforms to the law to make corporate criminal liability easier to establish, and reforms to the current legal framework around being able to attribute corporate liability for economic crime. Have you looked at some of those proposed changes? Where do the banks sit, or where do you sit, in terms of the proposals?

Stephen Jones: We have looked at the changes and would like to understand a little more about what the SFO sees is required. From what we know within individual institutions, there is a huge amount of alignment of interest in preventing economic crime. There is a personal alignment of interest to the officers of banks in preventing economic crime, as a result of the senior managers and certification regime, where personal accountability is attributable. Dear Colin here can go to jail if he gets it wrong, and it is Colin specifically who is responsible for this at HSBC, and then ultimately up to his board. There is an awful lot at stake.

There is an awful lot economically at stake as well. If I look at the £358 million of unauthorised fraud that was successfully perpetrated in the UK in the first half of this year, the vast majority of that was reimbursed by the banks to their customers. That is a cost to the banks. They want to stop it. It is not economically in their interest to be seen to be lazy on preventing economic crime or the fraud end of economic crime. Obviously, we are talking about sanctions and anti-money laundering as well.

If you overlay on that the overall fit and proper tests that the regulator, the Financial Conduct Authority, applies, the general principles that the regulator applies, and its ability to supervise the effectiveness of institutions, an awful lot of mechanisms already exist to attribute responsibility to individuals and institutions, which have severe financial, personal and licensing consequences if you get it wrong. I do not really know why the SFO wants more powers, but maybe it does not feel there are enough out there. I would not mind understanding better from the SFO why it thinks more powers are required.

Q331 **Catherine McKinnell:** You will understand that we had the financial crisis in 2008. Numerous scandals and numerous failings have come out since then.

Stephen Jones: There is criminal liability now attributable as a result of that. The law has been changed. In circumstances where an institution is brought to its knees by an individual, an individual can explicitly go to jail now. I would agree with you; in 2008, that was very difficult.

Q332 **Catherine McKinnell:** Quite often, the individuals who are held to account are at the lower levels of the institutions, and often the institutions themselves, or those in charge of those making the decisions, are not seen to be held to account.

Stephen Jones: It is not possible anymore, I do not think.

Catherine McKinnell: That is something I think the public struggle to understand. The Government rightly have an interest in making sure it is addressed.

Colin Bell: As an approved person under the senior managers regime, with accountability for financial crime risk within HSBC, I feel that accountability very keenly. I feel bound by that statement of responsibilities. I think my colleagues and peers feel the same way. There has been a sea change in the way that is tackled, and we feel it. We really do feel it.

Q333 **Catherine McKinnell:** That is reassuring to hear and that is how it should be. In terms of whether there needs to be additional change within the framework to ensure that it is working as well as it should do, that is something as a Committee we will continue to look at. In terms of legislative reform, not just in terms of information sharing but in terms of liability, is there anything that you would like us to consider, in terms of how things could be improved and your ability to tackle these issues?

Colin Bell: For us, the information sharing element is the key one.

Stephen Jones: On top of that, the other thing we would like to leave with the Committee is the idea of working hard, public and private together, to come up with an overarching set of priorities and tasking, so that we are extremely organised across all these multiple agencies, bodies, regulators and the private sector in what we are doing, why we are doing it, how we are funding it, to what timetable, to just be a bit better organised, frankly.

Chair: And to avoid those gaps you talked about earlier on, yes.

Q334 **Catherine McKinnell:** I have one final question for you, Colin. I do not know if you have recently googled "HSBC money laundering", but it brings up approximately 1.6 million results.

Chair: They are not complimentary, I should not think.

Catherine McKinnell: No, and some of them, I am sure, will not have all the facts. Many may not be accurate, but obviously it is of significant public interest. I just wondered if you were in a position to give the Committee an update on the current investigation into the money laundering controls and any money that might be set aside to deal with that.

Colin Bell: Anything material from an enforcement or investigation perspective we put in our litigation, so that is available publicly.

Q335 **Chair:** In terms of culture, we spend a lot of time in this Committee looking, and we will continue to look, at banking cultures. Is there anything that you see? I appreciate you only joined HSBC—you will be able to tell us; I have it here in my notes—in July 2016, so after some of the events had happened. What is your impression of the culture, the seriousness with which HSBC takes this, the way it trains people internally? Do you detect, from people who have been there longer, that the culture has changed in respect of economic crime or money laundering?

Colin Bell: Yes, to almost all of that, in the sense that this is an organisation that takes it incredibly seriously and has invested huge amounts of time in training. I think about culture as a pyramid. Whenever you go into an institution, you think about it in the sense that you are trying to change behaviours. To change behaviours, you have to get people to understand what the issue is. If you have enough people with the same behaviours, you get habits and those habits pervade the organisation. Then you can say you have a culture.

One thing that HSBC has done really well, in terms of its training and education, is to start building those foundations of behaviour through hours of training, education, case studies, examples. Really importantly, that is across the business part of the organisation, so not centred in financial crime risk or the control functions. It has done it across the business part of the organisation, and is then constantly updating, constantly checking, constantly reviewing. I describe it internally that the people who face off to our customers need a fingertip feel for this risk. In the same way that they have developed over 20 or 25 years a fingertip feel for credit risk when we are lending money, we need a feel for whether we are looking at the indicators of financial crime.

The firm has come a huge way, even in the two-odd years I have been in the organisation. It has really made some significant progress. You see it cascading down the leadership. If I think about the chief executive we have in Mexico, for example, one of our most difficult locations, he is one of the most driven, eloquent, persuasive people on financial crime risk I have met. His knowledge and level of understanding really gives me heart in terms of the understanding of the organisation.

Q336 **Rushanara Ali:** Mr Bell, I wanted to pick up on what has changed. Obviously, HSBC has struck gold in hiring you, given your distinguished career, and you are applying the militaristic zeal in changing culture and the rest of it. I bank with HSBC, so I am reassured. Picking up on Catherine's point earlier, a US congressional report referred to banks like yours as being "too big to jail". Obviously, I do not wish that on you, given what you are doing. In terms of the wider culture, is it still an issue for major banks? Despite the changes Mr Jones referred to, despite the post-crisis lessons, is it still a major challenge?

For both of you, in relation to this point, is the temptation to make big money by busting sanctions and laundering money still there in the banking world, or has it radically changed? If it has not, please suggest ways in which we can promote ideas to ensure that happens. That picks up on wider points you have made earlier. For the interests of the banking sector, which we remain dependent on in our economy and for jobs and the rest of it, we need to make sure this happens.

Colin Bell: I will go back to some of my earlier comments. As an institution, our starting position is that this is the right thing to do. We have had events in the past where the organisation fell short, but there is a fundamental understanding that this is the right thing to do. We have that legal, regulatory and moral obligation to protect the financial system against use by criminal actors. It is also a very complex thing to do. I have talked about scale, in terms of volume of processing, the sophistication of the criminals who are seeking to exploit the sector, and the fact that they continue to innovate and are unconstrained by many of the issues that we deal with. Institutions, HSBC being an example, but also others, have invested huge amounts of money, effort and time in understanding this risk and how to tackle it.

It is a continuous battle. I do not think there is a point where we will sit back and say, "We are done", partly because the environment continues to change, but partly because, as I mentioned earlier, as technology comes on, as our understanding of methodologies of criminal activity gets better, we will continue to push. We will continue to push the boundaries. Getting something that is absolutely watertight is unrealistic, but we have to be able to find it quickly, report it, and then the ultimate test of effectiveness is whether we can convert that, from a law enforcement perspective, into people in jail.

Q337 **Rushanara Ali:** What about the temptation point?

Colin Bell: Again, if you have an institution that says, "This is the right thing to do", growth is about growing safely, and growing safely is about managing risk. If this is one of the principal risks an institution has to manage, it will grow safely and in a prudent way. I sit on the group management board and have input into the strategy of the firm. As we are discussing growth agendas, we are discussing the financial crime risk agenda, and how we develop particular activities and capabilities to support that growth. I see nothing that suggests that is the case, certainly within my institution.

Q338 **Chair:** I have one final question, which is close to the hearts of people in this building, I suppose. How easy is it for banks to determine whether someone is a politically exposed person?

Stephen Jones: We realise that is a dominant feature in your postbag, particularly when someone in or around this estate has difficulty with accessing financial services. I do not know whether you want to—

Colin Bell: I thought you might hand that to me.

Stephen Jones: It is only because of the number of times I am here meeting MPs and Ministers who say, "By the way, I have these 10 letters in my postbag. Can you help sort it out please?"

Colin Bell: The definition of a politically exposed person has developed. I think it was the fourth money laundering directive that applied it to domestic and foreign. The definition, as people may well be aware, is a senior Government official, domestic or foreign, in a country. That is a pretty loose definition. You have additional guidance in some countries. Some, for example, will consider town mayors to be PEPs. Others will say, "No, it has to be at national Government level". It makes it very difficult for banks. We have our own set of guidance. We looked at the

UK, the EU, Hong Kong, the US, and we came up with our own definition of what we think a politically exposed person is.

I looked a couple of months ago at a list from a vendor that can provide lists of politically exposed people, and there are a million names on that list now, as a global institution. You are absolutely right; we make our own determination in terms of what a PEP is, against that rather loose guidance. We try to apply that consistently globally. More precise guidance would be welcome, recognising that it is quite a difficult topic to get hold of.

Q339 **Chair:** You have had to set your own internal rules. Rushanara asked earlier on about Russia in particular. Do you have a tendency to regard Russian oligarchs as politically exposed persons?

Colin Bell: It depends on what positions they have held. When you look at a politically exposed person, you also look at connected parties. If there is a strong connection there, they would be swept up by the PEP process.

Chair: That is very helpful. Thank you both very much indeed for your time this afternoon and for the evidence. As I say, Mr Jones, I suspect you may be back before us at some point on the basis of your role, either for the second part of our inquiry or for something else. We are very grateful to you for your expertise this afternoon.