



Treasury Committee

Oral evidence: [Treatment Of Financial Services Consumers: Cybercrime and Fraud, HC 631](#) Wednesday 5 November 2014

Ordered by the House of Commons to be published on 5 November 2014

[Watch the meeting](#)

Members present: Mr Andrew Tyrie (Chair); Steve Baker, John Mann, Jesse Norman, Alok Sharma, John Thurso

Questions 125 - 232

Witnesses: **Dr Richard Clayton**, Computer Laboratory, University of Cambridge, **Dr Alastair MacWillson**, Special Adviser, PA Consulting Group, and **Jeff Day**, Senior Security Consultant, British Computer Society, gave evidence.

Q125 **Chair:** Thank you very much for coming to give evidence this afternoon. I am sorry that this session may be relatively brief. We have another session immediately following and you have already met the people who will be participating. There is a risk, I am told, of a vote at 4.00 pm or shortly thereafter, and so we are going to see if we can obtain enough evidence on these subjects in the time available. Can I begin with you, Mr Clayton? Do you think we know the scale of fraud in banks?

Dr Clayton: We know the scale of lots of fraud, particularly that touching consumers, because the banks collate this information and break it down by different sorts of fraud, whether or not cards have been lost in the post, whether or not it is “card not present” fraud, whether or not it is online banking fraud, and they publish the figures for how much money is lost, as in they have to recompense consumers for that amount. Insiders tell me that the going rate is about twice that amount of money goes walkies out of people’s accounts.

Q126 **Chair:** Sorry, that is £2 for every one that they pay out?

Dr Clayton: Yes. But that money they are able to recover because moving money out of a bank account is relatively straightforward, moving it out of the banking system in a way that cannot be undone is quite difficult and not all criminals are as skilled at that as they might be. They also measure internally to the banks but do not collate, as far as I know, basically money at risk. When they see evidence that bank accounts have been accessed by

unauthorised people, they look at how much money was in those accounts and they scare their boards by adding up the totals of how much money might be moved if the criminals were better at their jobs.

Q127 Chair: What you are describing is a serious concern. In fact what you are saying is it amounts to a serious allegation that banks are systematically understating the scale of the fraud in the banking system. Why would they be doing that?

Dr Clayton: Because they do not want to frighten people. If your account has been accessed without your knowledge and you change your password and everything is then just fine; it is obviously a scare for the bank but it is not a problem to you and no money goes missing, so it is hard to call that fraud. It is obviously criminal but it is not fraud per se. You have not lost money.

Q128 Chair: This is very concerning if you think there is twice as much fraud out there than is being publicly reported. Three times as much

Dr Clayton: The other way of looking at it is that even when your money is stolen the banks are very good at returning it and half the time they manage to do so. It is a good news story as well as a bad news story.

Q129 Chair: How is it that you have been able to come upon this information, Mr Clayton?

Dr Clayton: Because I talk to bank insiders. I have done a lot of work on phishing, when phishing was a big problem for banks. These are setting up fake bank websites, not something that is a big problem to UK banks as of today because of the way they have changed their systems. But I used to talk to bank insiders to understand what the figures were because we were able to produce estimates from our academic workers on how many accounts were being compromised, and making these figures tally with what the bank published was difficult until they explained these other factors.

Q130 Chair: These insiders have been prepared to blow the whistle to you but it might be helpful if they blow it, at the very least, to the regulator, if not to us, do you not think?

Dr Clayton: I would hope that was the sort of thing the regulator would probe.

Q131 Chair: Is there anything, Mr MacWillson or Mr Day, you want to add on this or do you disagree with the evidence that you have just heard on this point?

Dr MacWillson: Part of the challenge is that although the banks could declare how much fraud goes on in terms of real hard money lost, a lot of the attacks are taking place where

extraction of value, that is money, does not happen. Recently there was a big attack on JP Morgan Chase, for example, where there was data extracted and there is a fair chance that that data will be used for subsequent fraud by matching other data obtained from other sources. So it is very difficult to quantify, and that is one of the challenges, so banks are obviously reluctant to air the fact that they have had a problem but equally they cannot talk about things when they have an incomplete picture. There is no mechanism to share that sort of information.

Q132 Chair: Anything you want to add, Mr Day? Do not feel a need if you agree, particularly if you disagree.

Jeff Day: Probably not worth me adding to that.

Q133 Chair: At the moment the amount being spent to clamp down on this is a function of trade-off between the extra amount being spent and the amount that they are having to pay out in compensation and in lost reputation as a bank, and also the potential damage to switching between online and offline banking because banks want us to go into online banking. Is that the right way that we should be deciding how much should be spent on clamping down on fraud? Who would like to go first?

Dr MacWillson: This may surprise you, but I don't think that many banks do a return on investment of the nature that you are talking about.

Q134 Chair: So they do not treat it as a business cost?

Dr MacWillson: No, they do the fraud aspect of it but the actual cost of breaches is a very grey and difficult area because of the complexity. A lot of the countermeasures and the measures for redress are done simply on the basis of normal IT type spend in a lot of, but not all, banks. But there is a change in awareness, which is changing that behaviour. Some banks are looking seriously at consequential loss and the indirect losses because they are significant, and some of the recent events have proven that. I do not know whether you have a view.

Jeff Day: All I would add to that, my personal view, is that the financial institutions are masters of maths and I would have thought if anyone should most effectively be able to determine the true cost of anything it should be the financial institutions.

Q135 Chair: What you have said to us this morning so far will be of considerable concern to a wider public. Fraud is, first of all, extremely concerning for members of the public because it does damage and causes concern well beyond the sum of money involved. It creates uncertainty, a loss of confidence, and a loss of trust. In that sense, it has some characteristics of house burglary. People feel their house is no longer safe, people feel their bank account is no longer safe or might not be safe. It sounds as if we

have a much bigger problem than is currently being admitted. What policy prescriptions do any of you have for addressing this?

Dr Clayton: The first thing to say is that fraud on credit cards and on bank accounts and so forth is now the volume crime. It is more prevalent than house burglary. You are more likely to see some strange transactions on your credit card or your bank account than you are to get burgled. That is from the figures from the existing surveys. The way in which we fix it—we have already done this—is to tell the banks that it is their responsibility to carry the loss. If the security measures they put in place cannot be operated correctly by normal people, so that normal people are impersonated to the bank and their money is moved around, then the bank must carry the cost and they must redesign those security measures until they are suitable for use by normal people.

Chair: I can take this much further but in the interests of time I am going to hand over the questioning to Jesse Norman.

Q136 Jesse Norman: Is the antiquated nature of many of the IT systems within banks responsible or a cause of many of the attacks? Does it facilitate many of these attacks or, in a funny way, does the fact that some of these systems are very antiquated render them relatively more immune to attack?

Jeff Day: The dilemma that the banking industry have is the fact that they have systems that are, in computing scales, old and they are trying to bring them forward into the modern day but because of the complexities of the whole industry and the technological complexities it is extremely hard to do and extremely costly and complex, so I can quite understand their reluctance to, at times, throw things out and start again because that is a huge impact.

However, the problem is that if you do not make top to bottom renewal what you end up with is a hotchpotch of new technologies being added on and added on and added on and, in the same way you can start with a little bungalow and put an extension on here and a roof extension there, you get to a point when the thing looks like a mess, and ideally you would want to throw it away and start again, and they cannot do it. So the banking industry is in a dilemma here but because there are so many interconnections and so many old technologies trying to work with new technologies, it leaves what you might call a large attack surface potentially accessible to the hackers.

Dr MacWillson: If I may, I would add to that. I agree with what we have said. These are challenging times for banks. They have a massive legacy base, which they have been trying to catch up and secure in a housekeeping sense. Ever since they got them they have always been behind. But what has come in in the last three years, as well as the sophistication of attacks, is the desperate need for banks, particularly retail banks, to change their business, the whole dimensions of it, to be digital, to be online, mobile and so on.

That fact, the innovation and the pace of innovation of technology that allows them to have a new business model, is so fast paced that not only can the banks not catch up, they cannot change their legacy systems while at the moment they cannot necessarily retire them.

More to the point, the regulators cannot catch up with what is going on, so they cannot even mandate standards that are appropriate.

Q137 Jesse Norman: So the banks may not know necessarily how to fix the ones they have. They may not even know what the true scale of the problem is and the regulators cannot track themselves what the true scale of the problem is for that reason as well.

Dr MacWillson: That is exactly right. So banks are pretty good at operational risk analysis usually, but I would say that for many banks this new world that they are entering into is putting all of their risk and compliance mechanisms to a real test through stress.

Q138 Jesse Norman: Okay. There is an area I want to go very quickly to, but just before that: presumably one effect of standardisation around things like internet protocol is to increase vulnerability because so many systems are interlinked and therefore if you get an attack it can go that much further.

Dr MacWillson: Yes, the monolithic culture of following the herd and doing the same as everybody else is not only dangerous but it is also, from many banks' perspectives, counter to their wish to differentiate, to provide different services to their customers, so there is a competitive aspect to it as well.

Q139 Jesse Norman: Can I just pick up on the question you raised then about the quality of the regulations going on or the regulators? Have any of you looked at the Bank of England's systems, their vulnerability? Do you have a view on whether or not our financial regulators are themselves potentially vulnerable to attack as well as relatively less capable of being able to—

Dr MacWillson: I have but—

Jeff Day: I have not, no.

Dr MacWillson: If you are asking is the Bank of England a best practice it possibly is but I will question whether best practice is an appropriate term because nobody really knows what best practice is against a set of threats that you cannot foresee at the moment. All of that is necessarily rear-view looking.

Q140 Jesse Norman: Do they have obvious areas of vulnerability, to put it that way?

Dr MacWillson: No more so than any other organisation of their stature in the banking and financial community. They have challenges like anybody else in terms of having appropriate resources and understanding the scale of the problem. But they are at the leading edge with initiatives like CBEST, which is testing cyber readiness and putting it to the test in real life situations. They have some pretty good baseline standards on which to operate from but it is very hard to say whether they are better or worse than anybody else.

Q141 Jesse Norman: Final question: there are two issues—there are many issues—there is fraud and theft of information on one side but there is also potentially wrecking attacks, damage to the plumbing of the monetary system, things like that. Presumably that is also a significant area of concern for you.

Dr MacWillson: If I may, that is a completely different subject, the whole financial stability of the entire—the whole financial system is one integrated network and is as dependent on stronger links in the chain as any other supply chain, so the challenge for the financial stability question, which is possibly the background to your question, is that—and the challenge across the industry is—although there is, in the last couple of years, much more co-operation between the government institutions and the banking institutions as well as the regulators—

Q142 Jesse Norman: How frightened should we be?

Dr MacWillson: It is not joined up—for me the biggest worry is the financial stability question, not the citizen or customer centric focus that was the line of your earlier questions.

Jesse Norman: And that is a very serious worry.

Dr MacWillson: That is going to lose banks money, the customer centric stuff, but it is not going to bring down the system, whereas the real worry in the profession is whether there are events that could be catastrophic to the entire system.

Chair: We have taken quite a bit of evidence on catastrophic risk already but there is no reason we should not take more. The point is though, for the millions of people out there with bank accounts, these risks are very real, even if it is not so catastrophic to the home economy, which is why we have been asking questions.

Q143 Alok Sharma: Gentlemen, good afternoon. I do not know whether you are aware or have seen any of the “Die Hard” films, the franchise; “Die Hard” with Bruce Willis. In “Die Hard 4”, there was a case where the US was under attack by cyberterrorists and basically were bringing down the whole system in a fire sale; happy to say that Bruce solved everything. But the question goes to the point whether or not in the UK we are open to a cyber attack, which could lead to effectively a meltdown of the financial crisis next time round. How high is the risk that cybercrime, cyberterrorists shut down our financial system?

Dr Clayton: This is an unanswerable question. There are a lot of people whose day job is preventing that happening, detecting malware, designing systems so that they—

Q144 Alok Sharma: Can I put it differently? What are the threats? Can you highlight two or three big threats that you think could be a huge risk for the system as a whole?

Jeff Day: Significant global events could change the level of risk. If Britain goes to war with another nation; time and time again you see this when nations go to war or there is significant friction between them, you start getting denial-of-service attacks on the various significant institutions in those countries. They are lobbing denial-of-service attacks on each other.

Q145 Alok Sharma: Are you saying then that the biggest risk to the financial system is effectively from other states as opposed to individuals?

Dr Clayton: It is sometimes hard to tell individuals from states in that a lot of times individuals act as they do because their state tolerates them and because they will get a warmer cushy job if they are successful rather than because they were being paid upfront by the state.

Denial-of-service attacks are not a big issue. Frankly, whether or not the No. 10 website is up or down is not a major issue in terms of whether or not the country is safe.

Alok Sharma: It probably is for No. 10.

Dr Clayton: Perhaps so, and it will make the evening news as lead story that they cannot keep the website up because of a denial-of-service attack, but it is not a big problem. What is a big problem is if you get malware in cybersystems and that malware starts either extracting data or manipulating data so that when you look at your screen to see how much money there is in the vault it is misstating that.

Dr MacWillson: “Die Hard” was all about manipulating market pricing and even attacking hedge funds so that you can manipulate money flow. Acknowledging that the banking industry themselves think that a near catastrophic situation is inevitable at some stage, whether it succeeds or not, whether they have the tools, is an important point to consider. But the BBA—the British Bankers Association—did a survey and thought that seven out of 10 CEOs believed that that was the highest operational risk that they would have to deal with. Normally it is about liquidity and so on, but the new boy in town is cyber. There is real worry both in the banking profession and with security professionals about the potential for that, and the fact that it has probably happened in several circumstances. There has not been mainstream awareness that it has happened with cascade ATM failures and so on.

Jeff Day: May I pick up a point that Dr Clayton made about getting something like malware into the system? These days huge amounts of trading in the City and stock markets is done at extremely high speed through automated systems—although I am not an expert in that area. I bet in recent years they had quite a few twitchy moments when those computers have pushed the boundaries of what us humans are comfortable with in the stock market. If those are compromised that could wipe the stock market out for hours, days: what happens to the City then?

Q146 Alok Sharma: Just two quick questions, I know we are pressed for time. The first is to do with what individuals can do to mitigate cyber attacks. You talked about—the

chairman's question—the scale of fraud and the bank's understating the scale of the fraud. Should we be having league tables, somehow, of financial services firms, which are kind of the safest as opposed to least safe when it comes to cybersecurity?

Dr Clayton: Personally I think so. The banks have decided not to compete on security as a policy decision. The upside of that is it means that their security teams can co-operate with each other without it being an issue for the bank chairman to consider what they are saying to each other. Since many actual frauds involve moving money from one UK bank to another UK bank in order to make the money look suitable for moving outside the system, there is a lot to be said for the security teams being on first name terms with each other, being able to ring each other up and say, “We just saw a big flow of data to one of your accounts, can you stop it please?” That makes a real difference.

Q147 Chair: Do you have a league table in your back pocket?

Dr Clayton: No. What I do know is that when the banks first came together to put together the figures that they had overall, one of the banks suddenly realised that 90% of the loss was theirs and concentrated their minds on improving their situation.

Dr MacWillson: Although there is no league table, as we said, in some countries, say in Canada and some of the US, there is informal social web reporting on—not on how well the banks do security but on how well they redress a problem after you have lost your identity or lost money out of your account. That for me is telling in a bank that has their act together, how well they have sorted that out.

Q148 Alok Sharma: Maybe we should have that here. Final question: Dr Clayton, you have put together a presentation that I think you made in 2012, where you said that cybercrime figures are often grossly inflated, and you have just told the chairman that banks understate the scale of fraud: which is it?

Dr Clayton: Both, depending on the subtlety of how you ask the question. But one of the things we drew attention to in our paper was that our fraud, which was now cyber, did not used to be. Things like tax fraud, VAT fraud, benefit fraud, all of which now involve computers, are basically costing a first world citizen somewhere around £100, dollars, euros, per year. Things like bank fraud and so forth, which used to be offline and have now gone online, are costing around £10, dollars, euros per person per year, whereas cybercrime, the new fancy thing, which everybody gets excited about, is probably costing around 10 cents or 10p. That is the scale of the thing. So banking fraud comes in the middle.

The real thing that we found was that the actual cost was spending in order to defend ourselves against this cybercrime, which is costing us 10 cents a year. We are spending \$40, \$60, \$80 a year on various security measures in order to keep ourselves safe, and that did not seem a very sensible trade-off.

Q149 Chair: How much are we spending on the high level fraud, the one that is costing individuals a lot?

Dr Clayton: Basically round about 10% of the loss. If you look at the figures for how much we spend on investigating tax fraud, VAT fraud, benefit fraud, it is around 10% of what is lost rather than 10 times.

Q150 Chair: So we are misallocating our antifraud, anticyber response by putting too much into cyber and not enough into fraud; that is what you are telling us, is that correct?

Dr Clayton: No, what I am saying is we have been very inefficient in the way in which we are dealing with cyber. We are hardly investigating it at all. The police have almost no money. We are looking at this as a result of which it becomes a big issue. We are almost scared about it, and we spend the money defending ourselves rather than relying on the police to defend us.

Q151 John Mann: Is there a technical possibility we could wake up one morning and no one can draw money out of any ATM in this country?

Dr Clayton: Yes, it has happened.

Dr MacWillson: It has happened. There is a very good example—I think it was about 18 months ago—of the ATMs being taken down in Boston in Massachusetts over a bank holiday weekend. One of the things that shocked the US authorities was that it caused riots because it was a hot summer day. People paid attention to the fact that that was a limited scale. It was surpassed in the headlines because it was at the time of the marathon in Boston where the bomb went off, otherwise it would have played for some while. But it is a good example of attracting attention to the scale of a much bigger problem.

The difference between the US and the UK is that our banks have a much higher level of interlinking on the ATM network through third party providers. The possibility of cascade failure that I mentioned earlier is probably higher here than maybe in some other countries.

Q152 John Mann: You mentioned in relation to JP Morgan, Dr MacWillson, that an attack of that level can only be done by nation states.

Dr MacWillson: I did not say that. I do not believe I said it. I am sorry if I did but I did not mean it that way.

John Mann: That was a quote of you saying that. Can it be?

Dr MacWillson: It can.

Q153 John Mann: Outside of NATO, which nation states have the capability of doing that?

Dr MacWillson: Quite a few. In actual fact, of the several high profile banking attacks in the US the recent ones were thought to be originating from Iran because of the pressure Iran is under from a nuclear perspective and also the whole Middle Eastern equation. I believe that equally you could say that it is maybe Russia, China; so a lot of nation states have the capability.

I said I did not mean that for JP Morgan, but we do not know, nobody knows. It is always very difficult to realise who it is that is doing it. You can possibly make assumptions but in that case it could have been a criminal gang in the JP Morgan case. So criminal gangs are becoming incredibly sophisticated and it is hard to tell the difference, as Dr Clayton said, between individual attackers, hacktivists, criminal gangs, and nation states.

Q154 John Mann: Dr Clayton, considering it has been said—and by the governors of the Bank of England—that our banks are too big to fail, looking at the size of the banks in this country and the small number of large banks, are we more vulnerable than other countries?

Dr Clayton: It depends what you mean by “fail” in this case, because if the cash machines do not work then you will be able to go inside and get the money from over the counter. What I think you are worried about is not that but the computer systems not working so the bank does not know how much money you have in your account. That is really the problem, at which point, if that happens to all the banks, that is obviously going to be extremely disruptive. It is not the same as being invaded by a foreign army. Cyber scares people because they do not understand it.

Q155 John Mann: My question is: wherever the source is we have seen a concentration of banking, a reduction in competition in this country, and we have seen banks—RBS would be a good example—taking great kudos and credit for merging systems together. We had a go at the Co-op and some of its mergers for not doing it sufficiently or sufficiently well. With integrated systems in bigger banks does that mean that there is more of a vulnerability here in this country as opposed to other banking systems elsewhere in the world?

Dr Clayton: To the extent that, if one of the big banks failed to operate for a few days—and we have seen some of the banks in the UK failing to operate for a few days recently—that obviously affects a lot of people. In the US, banks are basically regional. Although there are a lot of banks, there is still a very large number of people in any particular town banking at a particular bank.

Dr MacWillson: I would slightly challenge that thinking, the assumption that if you have a bank made up of five smaller banks and you whack them all together that the system must be more vulnerable. That is possibly true in theory. But I would argue that one well-constructed, well-architected organisation is much better than five disparate systems in organisations that are not very well secured and not very well designed.

Q156 John Mann: Final question: what should we be recommending to citizens, to consumers, in order they can be better protecting themselves against cyberfraud? I do not mean what detail but what should be the principle, who should be doing it, how should that be done to ensure that the citizens of this country can better protect themselves against cyberfraud?

Jeff Day: That is an enormous question. Yes—

Q157 Chair: Do you recommend online banking?

Jeff Day: Yes, per se.

Dr Clayton: If you are good at complaining, some people are not, then online banking is just fine. Have a look at your account every month. Do not leave it six months to have a look. If there is a problem then complain.

Jeff Day: Which is the same as a traditional paper account. On the whole question of education of the end consumer, if you could educate to some degree, get the thinking of the average person in the street to think safely and securely online—in the same way they think safely when they walk out the door and cross the road—if you could get them to think a little bit about security when they operate online you will probably hit the 80/20 rule. You will resolve 80% of the problems by the consumer thinking about what they are doing.

Q158 John Mann: But my question is: who should do that? You are experts in the field. Who should be doing that: banks, Government, educators, internet providers?

Jeff Day: It needs to be driven by the Government and pushed out across the various business institutions and pushed all the way down, right down to education in schools. All the way down.

Q159 Steve Baker: As I listen to you, I wonder once again whether in cybercrime conversations we are having the right conversations at all, or whether we should be having several quite separate conversations. You have just been talking about consumer behaviour and getting a little bit more thinking. Earlier the subject of distributed denial-of-service attacks came up. I have read about traditional crimes, the banal but expensive stuff like fraud, transitional crimes, platform crimes, making available new tools, and then the new crimes themselves, which are only characteristic of cyber. Are we having the right conversation or should we be having several conversations about several quite different kinds of cybersecurity? Dr Clayton?

Dr Clayton: Yes, because there is not all that much in common between DDoS and malware getting on your machine. The way forward here is to stop seeing cyber as something terribly important that has to be separated out and dealt with completely

separately and you just pick up cyber in terms of what the risk is that you are looking at. Because asking whether or not the banks are going to collapse due to a cyber attack and asking whether or not your bank account is at risk if you don't choose a strong password are very different questions.

Q160 Steve Baker: Good. I am glad you said that because we were talking earlier about catastrophic attacks and I think perhaps it was Dr MacWillson who talked about not being less concerned about the individual than the catastrophic attack on the entire system. If I was doing a risk assessment on this and trying to categorise these things I might look at each category of cybercrime and say, “How severe are the consequences? How frequently is that kind of attack going to happen and how difficult is it to execute?” All those three things keep being mixed up. How would each of you categorise cybercrimes, please?

Dr MacWillson: Shall I kick off? Just to reiterate what we have been talking about today: there are two distinctly different but related areas. One is about what the regulators would call financial stability. It is not just DDoS attacks. It is the ability to extract customer data en masse from banks and, more to the point, to look at banks’ sensitive customer transactions about mergers and acquisitions, all sorts of transactions. That is about banking stability and that must be of concern to governments, other banks, the whole financial industry, if you like. Secondly, what we have been discussing, or what we kicked off with, is all about the consumer dimension of cyber. Therefore the main concern is the banks themselves from a reputation perspective and their brand and competitiveness, and, of course, the customer and making sure there is a proper redress if there is a problem.

Some of the mechanisms you would use equally apply across those two different dimensions—mechanisms to protect the customer and to protect the data in the organisation— but they are very different topics and different regulators.

Q161 Steve Baker: Forgive me for interrupting, but I want to just clarify the question. I appreciate and I am glad we have clarified and established they are different topics. If I may be so bold, I think this Committee's job is to figure out what questions to ask. How would you categorise the areas in which we should be asking questions, I hope as simply as possible? Should we be asking a bunch of stuff about authentication and human factors? Should we be asking a bunch of stuff about malware and technical attacks on desktop and mobile devices? Should we be asking a set of questions about sophisticated attacks on the server side? How would you categorise the questions?

Jeff Day: Security is about two primary issues. There are the technical issues with firewalls and everything else and there are the processes and procedures. It is the way you go about doing things and you could take that as a starting point, take it as those two separate issues. You could look at how financial institutions or whatever go about technically addressing these issues, but to some degree technical solutions are kind of easy. You buy a box, you configure it correctly, you put it in the right place and it does its job. What is trickier, I would argue, are the processes and procedures because in there you have the human factor and it is the human factor that is almost always the weakest point.

To come back to the banking scenario, in the banking world I would suggest there are two kinds of people working there. You have the real financiers who know money and how the whole system works and you have a whole bunch of other people who go to work every day, who happen to work in a bank and who do a fine job. But they are not necessarily traditional financiers and they are certainly not security people.

Even if the true financiers know the kinds of risks that go on and may even know some of the ways of mitigating them, the services that the bank then presents down through the average worker behind the till and out to the consumer, the people at that level may not have the same knowledge. For argument's sake, if you have your card hijacked and you phone up the bank and the bank turns round to you and says, "It's your fault", it may be simply because that person you phoned doesn't have the knowledge to understand how it all works.

Q162 Steve Baker: Forgive me, but I will just move on because I am conscious of time. Somewhere in the evidence, I have read that one of the authorities has said there is a rather limited group of good programmers. Certainly, as a software engineer myself I recognise that. Also elsewhere, many of these people will be in Russian-speaking countries. Dr Clayton, I think you have said we should be spending more money on locking people up. How do you think we go about finding the 100 or so brilliant criminal minds, programmers, and locking them up, particularly if they are Russian?

Dr Clayton: Now you are asking me a foreign policy question: how can we get on better with people we have common interests with, which is that we are all against crime?

Q163 Steve Baker: Is that what we need to do?

Dr Clayton: Yes. A number of the places that are often quoted as being places where lots of criminals hang out tend to be places we have bad relationships with because if we were sitting in the US we would expect the FBI to arrest them for us and vice versa. We need better relations. The FBI has been imaginative in the past by persuading people to go across borders where they can be nabbed in order to get hold of these people. But yes, I wouldn't say it was 100. I would say it was closer to 1,000.

Q164 Steve Baker: Only 1,000?

Dr Clayton: Yes, only 1,000. But that is still a large number of people to lock up. If you tend to ask a policeman, you say, "I can list you the 100 worst people to lock up" and they tend to look rather disappointed and you have to move it down to about five or three before they get interested in dealing with it.

Q165 Steve Baker: How hard is it to trace various kinds of cybercrime back to the perpetrators?

Dr Clayton: It varies. Some of it is extremely trivial and some of it is impossible and you give up. It depends how competent the people are, how well-advised they have been and whether or not they thought anybody was going to come after them.

Q166 Steve Baker: How does that level of difficulty of tracing people correspond to the severity of the attack?

Dr Clayton: Not at all. I have seen a \$3 million fraud where if we had better relationships with Nigeria we could go and grab the person who did it. I have seen very small amounts moved around in a competent way where you have no idea where they have gone.

Q167 Steve Baker: Finally, is it conceivably possible, that we could have a catastrophic attack that brings down the financial system and we just have no idea who did it or how to find them?

Dr Clayton: Yes.

Chair: On that rather depressing note, having only superficially touched on so many aspects of this very important subject, I am going to say thank you very much for giving evidence to us. We will no doubt be coming back to you in writing for further information and because we are pressed for time this afternoon we will move straight on to the next session. Thank you very much.

Examination of Witnesses

Witnesses: **Simon Fell**, Acting Head of External Affairs, CIFAS, **Donald Toon**, Director, Economic Crime Command, National Crime Agency, **Andrew Archibald**, Deputy Director, National Cyber Crime Unit, National Crime Agency, gave evidence.

Q168 Chair: Thank you very much for coming to give evidence this afternoon and you will have heard the evidence from the preceding panel. Could I ask each of you in turn whether there is anything of substance that we have heard that you would want to qualify or seriously take issue with? Who would like to go first?

Andrew Archibald: I am Andy Archibald, Deputy Director in the National Cyber Crime Unit in the NCA. There were a number of interesting discussions in that last session, particularly around cyber. I think the last question related to what advice we would give to the general public and to members of the community: it is very much about reinforcing the message through whatever channels we can, and there is a range of different channels to

do that. It is about reinforcing the message about protecting in computers those parts in your life that you value, such as your financials, your photographs, all those aspects that are now online. It is about taking steps, using antivirus and protecting your computer.

Q169 Chair: The key message we have just heard from that session is that fraud is on a much larger scale than it appears from the official statistics and, indeed, they give only a very dim idea of the full scale. Are any of you, from your professional standpoints, taking issue with that?

Simon Fell: I completely agree with that position. Our view is that we see an awful lot of fraud. As an organisation we report it to the National Fraud Intelligence Bureau so that police forces can take action, but it does not appear in the official crime statistics. We are reporting 1,000 cases of fraud a day to the NFIB, and that means people don't have an awareness of the scale of the problem that they face.

Q170 Chair: Nor do we from the information provided by banks on the scale of fraud they are afflicted by—correct?

Simon Fell: Correct.

Chair: Mr Toon, have you anything to add?

Donald Toon: I would generally say that fraud and economic crime in general are probably underreported. We have certainly seen increases in the level of reported fraud but we have no real basis to make an assessment of whether that is a significant increase in the fraud problem or an increase in the proportion that is reported. We have certainly seen—if you link in to the wider financial risk around money laundering—in the last five years a 50% increase in suspicious activity reports coming into the Financial Intelligence Unit. That would indicate there is probably a significantly larger problem in that space. However, frankly, we have a very limited intelligence picture of the scale of the problem around most economic crime.

Chair: That is an extremely concerning but important piece of evidence.

Q171 John Mann: Many banks have been prosecuted for illegalities; do you have proper access into the banks to find out what you need to know about the level of risk as well as about the specifics? I am talking about banks operating in this country.

Donald Toon: That is quite a complex question to answer. There is absolutely a genuine issue for both banks and banking customers, whether they be corporate or individual, about providing access to customer data. There is an absolutely clear issue for us around being able to obtain access through production orders or customer information orders where we need to be able to go in front of a judge and seek authority.

There is a good relationship certainly with all the major banks on providing information that is essentially maybe non-specific, slightly anonymised from individual customers,

looking at trends, looking at types of problem, development of risks, but when we get to the point of customer data that is a hugely sensitive issue. It does require legal governance and that legal governance is in place. We are absolutely working closely with the banks.

The Home Secretary and the Governor of the Bank of England and the Chair of the Financial Conduct Authority brought together a meeting with all the bank chief executives earlier this year. As a result of that there is now a financial sector forum between law enforcement, the Home Office and the banks. That is doing quite a lot of work now on information sharing. We see certainly an improvement in the relationship but it is a sensitive and difficult relationship. The banks are naturally cautious about any risk of providing information inappropriately or inaccurately to law enforcement.

Q172 John Mann: Is there a big variety between the attitude and aptitude of the banks in relation to that?

Donald Toon: We have been working with all the major banks in the UK. All the major banks have been very keen to co-operate as far as the law will allow.

Q173 John Mann: How many cases of cybercrime against financial firms and customers did the NCA investigate last year?

Andrew Archibald: In terms of how many we investigated, there is a differentiation between cybercrime and cyber-enabled crime such as cyber-enabled fraud. We have a number of investigations ongoing at the minute from the National Cyber Crime Unit perspective that are principally against some of those high-end cases—those that develop malware exploit kits and intrude onto those systems in the financial sector, for example. Malware such as Gameover ZeuS and Shylock have had a lot of media attention recently. Our investigations have focused on those particular aspects of cybercrime. For attacks on the financial sector and intrusions into the networks, it is the motivation that changes it into the fraud aspect: cyber-enabled, manipulative access of systems and theft and harvesting of personal data to commit fraud.

Q174 John Mann: How many are we talking about?

Andrew Archibald: In terms of the fraud side, we have around about 40-45 cases against high-end malware and developers and those deploying systems against banks and communities.

Q175 John Mann: Just to follow up on that, what is the timescale for you to thoroughly investigate? Are we talking weeks, months, years?

Andrew Archibald: If you are dealing with cybercrime, it is a global problem and the solution is international, so it is multiple jurisdictions. It is not bilateral investigations. Every investigation we have ongoing involves a number of international partners and the

reason for that is the threat comes from overseas. That is from those who develop the malware, those who sell the malware on criminal-hosted sites in another country. Multiple countries are involved. Some of the investigations or all of the investigations we have involved relationships with a number of countries, 10, 11, 12 countries and that is a real challenge because of different cultures, different values, different judicial systems. All of those are quite challenging. Investigations can last anything from three months to 12 months or beyond. It depends on the scale of the threat, how many countries are impacted by the same threat, the ability to share intelligence and information with those countries and to agree among 10 or 11 countries, 15 or 16 agencies, the best approach to arrest or disrupt or take other intervention steps.

Q176 John Mann: You are doing 45-50 at the moment?

Andrew Archibald: Yes.

Q177 John Mann: What is the capacity you have?

Andrew Archibald: I would say we are at capacity currently.

Q178 John Mann: You are at capacity?

Andrew Archibald: We are at capacity currently, yes.

Q179 John Mann: What happens if more comes in?

Andrew Archibald: We then go into the process of prioritisation. That then gets to what is the report, what is the threat? We speak regularly, and Donald touched on a number of forums, we have regular meetings with the banks through a virtual task force that is an operational group. We meet regularly with the British Bankers Association one-to-one, but if the banks were to come to us, we ask the banks, "What is it you are seeing attacking the banking sector currently? What is your gravest threat?" and we then prioritise that as investigations we would take forward with partners overseas. If the banks came to us and said, "This is now a massive threat because it has just recently emerged" we would have to re-prioritise some of them.

Q180 John Mann: What about consumer fraud?

Donald Toon: If you are talking about fraud in the round then the figures would be relatively similar. Consumer fraud is not a term that I would use generally. Our primary interest as an agency is around serious and organised crime, so serious and organised fraud. The number of cases across economic crime would be very similar to that for Andy

for pure cyber. The length of time would be very similar as well. You are talking months generally for intervention, usually because they are international.

Q181 John Mann: Are you at capacity?

Donald Toon: Yes, we are at capacity. Across economic crime in the round, yes, we are at capacity now.

Q182 John Mann: My final question: A “yes” will do. Is the trend of this kind of crime upwards? Are there more every year?

Andrew Archibald: I think what we are seeing is our situational awareness is improving, so we are seeing more reporting, more information being shared through—I don't know if anyone has mentioned the cyber information-sharing partnership. We are seeing more information intelligence coming to us that perhaps was not previously shared. My sense of things is that this is increasing.

Donald Toon: On the wider economic crime environment, I would say the same, absolutely. Certainly we are seeing our knowledge is improving, our picture of what is going on is improving. As a result of that we are identifying more criminality.

Q183 Jesse Norman: How many prosecutions have you brought on these issues in the last 12 months?

Donald Toon: It is a very hard question to answer in terms of these issues. For economic crime we are talking everything right across from money-laundering, corruption, sanctions evasion as well as fraud. The total number of people prosecuted as a result of those investigations certainly from our side would be round about the three figures, round about 100.

Q184 Jesse Norman: Approximately 100, right?

Donald Toon: About 100 in the last 12 months, yes.

Q185 Jesse Norman: This is related to cyber stuff, not obviously other serious organised crime, with a cyber-angle to it.

Donald Toon: Virtually everything we are talking about would have a cyber-angle to it of some form.

Q186 Jesse Norman: On the other side?

Andrew Archibald: On the other side, having mentioned organisations being in existence 12 months, having described some of the processes, we are involved in prosecutions both in the UK and overseas. There are some other operations, but we have about three or four or five high-level cases that are going through the criminal justice process at this stage. We have also co-ordinated other work with policing and regional resources.

Q187 Jesse Norman: I understand the difficulty of bringing and investigating cases here. You have described it, and also, of course, the difficulty of knowing what the activity is. But nevertheless, we seem to be in a situation where there are hundreds, perhaps many hundreds of serious attacks and a relatively small number investigated at one time, given the resources that you have, and a relatively smaller number being brought to trial. Is that fair?

Andrew Archibald: It is and, given the nature of the criminality we describe, it may not always be possible to arrest.

Q188 Jesse Norman: You mean it may not exist in a way that allows you to bring a prosecution?

Andrew Archibald: If you are measuring success, because of the challenges we have heard described earlier, some of those who are attacking us are in countries where we don't have a particularly good relationship, so part of it is about how we disrupt them, how we work with international colleagues who we may then share our intelligence with so they can perhaps take executive action. It is about a truly global response.

Q189 Jesse Norman: It does not feel to me as though there is a very strong deterrent that comes from law enforcement at the moment, given the number of cases there are and the number you are able to prosecute and investigate.

Andrew Archibald: At the high end.

Q190 Jesse Norman: At the high end. Okay, that is helpful. The next question, if I may, have you guys done any kicking of the tyres on the Bank of England's defences to cyber threat and the strength of the monetary system?

Andrew Archibald: What I can say is I have had several meetings with the Bank of England and I know they are going through a process of recruitment in developing their capability in that area, so I know that they recognise the threat. I think they understand the risk and where the threat comes from in terms of who might target them. They are therefore improving their capability. They have asked for advice and support on how they do that and I am part of an advisory panel that sits to assist them with that, so they are taking it seriously and they are improving their capability.

Q191 Jesse Norman: Thank you, and then the final question: you will be aware that a recent report found that we in Britain have suffered more sophisticated cyber attacks in the first half of this year than any other state in Europe and the Middle East. That is the one by FireEye, and I wonder why that is and whether that means that the UK is more vulnerable or is it that the returns to potential attacks are higher because so much of the financial banking system is in this country?

Andrew Archibald: I think it's the last point you made there. That is why I think we are a target.

Q192 Jesse Norman: The criminal world is getting smarter about focusing on places where they think the loot is and they focus on this country.

Andrew Archibald: Absolutely.

Jesse Norman: Thank you very much.

Q193 Chair: The companion question on the Bank of England's efforts is a similar sort of question that might be asked about the FCA. Mr Fell has written to this Committee on that subject in the past. Are they giving it the right priority? How are they doing? Would you please mark their prep?

Simon Fell: I would probably rather not mark it out of 10, but I think they are doing some good work at the moment. We have found them to be a very good partner in looking at some of the issues that enable fraud and drive fraud.

Q194 Chair: They are getting on top of it?

Simon Fell: They are producing research now, so they have just come out, for instance, with a piece of research that looks at how the over-55s are particularly susceptible to certain cyber attacks. That can then drive work that we do in industry and the banking sector to help drive prevention as well.

Q195 Chair: Would you be inclined to take off the table what you told us three years ago where you said, "The already muddled crime prevention landscape is having another player added to it"?

Simon Fell: I would be very happy to take that off the table.

Chair: I just feel it might be helpful.

Q196 Steve Baker: In the earlier evidence, we heard about the range and scale of cybercrimes and also the potential difficulty of detection. Mr Archibald, how do you categorise and prioritise cybercrimes?

Andrew Archibald: The key to us is, again, to firstly assess what the threat is: what harm is it doing within the UK? Principally, from a cybercrime perspective, it is against the financial sector and it is financially motivated, so we are interested in the scale of that threat, whether losses are attached to that threat, how many individuals, perhaps, are affected by that threat. Where are the actors and which other countries where our international colleagues are also suffering and have investigations into the threat? It is very much malware and the deployment of malware, and then the manipulation of the computer network they have intruded on and the harvesting of personal data that then leads to fraud.

Q197 Steve Baker: That sounds very economically focused, but in the earlier evidence, I asked, “Could we have a catastrophic attack on the financial system and not be able to detect who had carried it out?” I am a bit sensitive about how I ask this question, but to what extent do you work on that problem, the issue of financial stability and the difficulty of detection?

Andrew Archibald: We do. We do work hand in glove with other agencies in the UK who have that as a priority.

Q198 Steve Baker: But your own priority is to concentrate on fraud and individuals.

Andrew Archibald: It is the cybercrime element and there is the other aspect that may be a nation state that is handled by other agencies, but we are linked with them closely and share in an appropriate way.

Q199 Steve Baker: Thank you, that is very helpful. I notice just looking back at your CV, Mr Archibald, you previously led operations for Special Branch nationally, so I feel sure you are familiar with some of the nastiest people we have to deal with. Are those same people involved in cybercrime and to what extent?

Andrew Archibald: It would be difficult to assess that. I think if you are involved in serious and organised criminality then part of your organisation and your criminal infrastructure will involve someone who understands how to hack into and intrude on a computer system. I am pretty confident of that.

Q200 Steve Baker: The range of people we are talking about when we discuss cybercrime will be everything from what is euphemistically called script kiddies, teenagers who have downloaded a kit, through to the most serious criminals internationally.

Andrew Archibald: Yes.

Q201 Steve Baker: What do you think is the origin of the most serious threat we face?

Andrew Archibald: I think Russian-speaking.

Q202 Steve Baker: Russian-speaking organised crime.

Andrew Archibald: Yes.

Q203 Steve Baker: Thank you. What kinds of crimes are occurring in the highest volume?

Andrew Archibald: I think we are seeing the harvesting, through the employment of malware and intruding into what they are discovering, of financial detail. It's then the creation of sites where we then see those credit cards and debit cards then being sold and bought and used across the world to commit fraud.

Q204 Steve Baker: How seriously do you take this idea of spearfishing, the idea that a lot of that stolen data is used to dupe people more effectively?

Andrew Archibald: Yes, absolutely, it is a real threat and it is commonly used and is a tactic that cyber criminals use every day and I would see it as a tactic they would use, yes.

Steve Baker: Mr Toon, do you agree or would you add to what has just been said?

Donald Toon: I would absolutely agree with what Andy says. I do have a concern, perhaps, to an extent that it is possible to see cyber as the only issue here when there are a number of broader issues around cyber-enabled or cyber-linked fraud. But there is criminality that risks undermining the credibility of the UK financial sector that has little or nothing to do with cybercrime. That is when you are into areas around economic crime that are about the provision of the capability to launder money in bulk as a service by the UK financial sector and by related professions. I worry a little that an over-focus on cybercrime may reduce the level of focus on that broader threat, some of which is a traditional threat. Often for banks and other companies, yes, they have a significant concern around cyber and hacking. But, of course, they have a significant concern also about the so-called human factor: the insider threat, the disaffected member of staff who downloads customer data and walks out with it on a stick.

Q205 Steve Baker: Without wishing to put words in your mouth, what I think I am hearing is that we should be concerned about the change in the modus operandi of quite traditional crimes over the hype around some of the more exciting sounding crimes.

Donald Toon: Yes, we should be careful of following the bright, shiny and new. Bear in mind that there are big, older, traditional crimes here, some of which are becoming more

of a problem as the world becomes ever more connected, ever more online. Certainly if you look into the financial transactions world, if you look into things like international corruption, the ability to move money around in seconds in multiple transactions internationally, that is a huge issue. It is not cybercrime.

Q206 Steve Baker: We understand that one of the objectives is to disrupt the supply of so-called hacking software to criminals. As you possibly heard me say earlier, as a software engineer I look at these tools and think, “Well, this is just programming languages and knowing how to use them”. What is your approach to disrupting the supply of hacking software, and how can you possibly do it?

Andrew Archibald: I think the challenge in terms of disrupting the supply and the access to hacking software, which is available to download and to purchase, is that the sale of the malware is not always in an open and transparent way that you would readily find on the internet. It is in encrypted sites, it is in secure sites, and in the same way that criminals have always taken steps to secure their criminal enterprise, cyber criminals do likewise. What they do is they try to sell the products in a secure environment.

Again, it is about us having access to information and intelligence about those, particularly those in the UK we have an interest in who have purchased a download and remote access tools in, for example, Blackshades malware—there was an operation against that where there were members of the public in the UK who downloaded that software. With our colleagues in policing and regional units, we arrested some of those, but we also contacted those who had purchased but had not deployed to give them warnings and dealt with them in that way.

So I think there is a range of things we can do. One is about ensuring that those who are visiting those sites are absolutely clear about the nature of the sites they are visiting, a sense of the criminal activity that they are or could become involved in, and also to try to bring down those sites that function purely for criminal activity and for the sale of criminal goods. To do that, again because the infrastructure is not always in the UK, it becomes a global issue and an international challenge.

Q207 Steve Baker: I am concerned about something when I hear you say that. It sounds good. With something like a Linux distribution, like a Knoppix security tool’s distribution, you download it, you bang it on a CD and it is a very useful tool for legitimate purposes. I used to carry it all the time, at the risk of being arrested on the way out the door. If you are a software engineer, it is useful to have a CD with a range of ordinary software tools, which can have legitimate purposes, including testing security. Are we going to end up licensing software engineers to have relatively ordinary software tools?

Andrew Archibald: It always comes down in terms of the possession. Is the possession with criminal intent? That is the part we are interested in. There are a number of aspects of the cyber infrastructure that we are interested in, but some of that is legitimate. We are only interested in those who are motivated to have an intent to commit criminal activity.

Sometimes it can be difficult to make that assessment but that can become apparent quite quickly as we do further investigations and monitoring.

Q208 Steve Baker: I am trying to understand how you distinguish the two. If a Linux distribution was a boot CD that happened to have a lot of security tools on it but it was freely available to download and quite public, you would not consider that criminal. But if somebody had securely encrypted a site, you had to pay for it and it became apparent that it was intended for malfeasance—

Andrew Archibald: We would be interested in what the motivation was. In terms of the possession, that in itself is not a criminal offence. What we are interested in is the possession and then the activity that then follows.

Q209 Steve Baker: Okay, so given that, how can you meet the objective of disrupting the flow of these tools?

Andrew Archibald: In terms of those particular tools?

Steve Baker: It is about the particular, it is about saying we want to disrupt a tool when it happens to be bundled with obvious malicious intent.

Andrew Archibald: If we return to the case of Blackshades, that is an example of a tool that was downloaded from some of those websites and not everyone went on to commit criminal acts with that. But part of the assessment of the investigation was about who has downloaded that software, what have they done with it, how have they used it and if they have used it, was it a criminal activity. There is a range of other tactics we can use in terms of interventions or establishing whether it is for legitimate use. The point you make about whether we would license software engineers is interesting. It is not an issue we have come up against as a problem yet.

Steve Baker: Just to be clear on the record, I am not suggesting it. I think it would be a disaster, but what I am driving at is the difficulty of distinguishing between legitimate software engineering and criminality. Thank you.

Q210 Alok Sharma: Mr Archibald, you talked about the fact that you deal with or co-operate with 10, 11, 12 other countries. Can you tell us which organisations you are working with and how you work together with them? Also it would be really useful—we have had a lot of general discussions here—if you could give us a case study, obviously on a no names basis, where you have worked together with other agencies and you have achieved success?

Andrew Archibald: In terms of who we work with, I think the UK is in a fortunate position in terms of the international bodies we are involved with. I was in Vancouver last week and chaired the Five Eyes Cybercrime Working Group. I will be in The Hague on Monday chairing the Joint Cyber Action Taskforce in Europol. In that, for example, there are 12 European countries, three US agencies, EFP and RCMP, with staff on the ground in

The Hague. So we work with them in a collaborative way and what we hope to get from that collaboration is the ability to—

Q211 Alok Sharma: Could I just ask you to expand on collaborative? What does that mean? Do you have members of your staff who meet with members of their staff every month, every quarter or whatever it is?

Andrew Archibald: No, they are in the same building, in the same office, in the same room with access to IT and connectivity back to our respective agencies.

The key part is about deconflicting operations. So having an understanding that Shylock malware attacking the financial sector in the UK is also attacking Dutch infrastructure, Spanish infrastructure, US infrastructure and establishing what operational activity we all have in our respective countries and how we pool that together to have the greatest impact against that particular threat. We do that on a routine basis and we have a process for prioritising what the operational activity is we will do through there.

We have had some success already with that. I mentioned Shylock—that would be one of the examples that we could point to. That was very much malware deployed against the financial sector in the UK suffering quite significant losses, also impacting on other countries and infrastructure in different locations around the world, with some of the key actors in different locations around the world. So what we had was a co-ordinated operational activity that resulted in arrests, which resulted in take down of the botnets that were distributing the malware and a successful operation.

The key part, however, is how long does that last. So if we bring down and we are able to disinfect the malware and it reduces the threat in the UK, how long does that last before it re-emerges. That is a key point that we try to establish as well.

We have around 16 operations being progressed through the centre we have in The Hague. I think we want to see that expand to have an engagement with the European financial sector as part of that arrangement as well.

Q212 Alok Sharma: Just so I do not misunderstand, that is 16 cross-border investigations that you are doing out of what, the 40 to 45 you were talking about?

Andrew Archibald: Some of those 40 I mentioned, those are in addition. So we will have—

Q213 Alok Sharma: What percentage of the cases that you have on your books currently have a cross-border dimension as opposed to not?

Andrew Archibald: Every one, but some of those might be with countries that are not necessarily involved in the take down.

Q214 Alok Sharma: Turning to where these cyber attacks are coming from on the UK, I think there was a discussion about Russia being one of the areas that—

Andrew Archibald: Yes, Russian speaking.

Alok Sharma: Russian speaking. Do you have your own internal league table by geography and then also by the type of organisation, whether it is quasi-government, individual or organised crime? Do you have those sorts of figures that you can talk to us about?

Andrew Archibald: We have a priority country matrix.

Alok Sharma: Which are?

Andrew Archibald: Sorry?

Alok Sharma: What are those priority countries?

Andrew Archibald: Some of them are the ones that would immediately jump out at you, Russia, China, Vietnam, Brazil, India. That is in relation to two things. First, it is in relation to some of the actors but the other one is in relation to some of the infrastructure that is supposed to be there. So, for example, the US also features on that as well. In terms of what our engagement was, that is where the critical infrastructure is, that is where the big global corporations are so, again, we see the benefits from the work within Five Eyes.

We are doing a piece of work at the moment, which is across the Five Eyes, identifying sharing on priority countries and looking for duplication.

Q215 Alok Sharma: When you talk about these countries, you are not necessarily talking about government or quasi-government organisations that are doing this?

Andrew Archibald: I am not in the examples that I have given, but there are some countries, of course, where if you are involved in cybercrime and you want to locate your infrastructure, you would choose to locate the infrastructure in a hard to reach place for colleagues and allies or you would put in a place where the framework is less well developed. So there are other countries.

Q216 Alok Sharma: Can I just go back to this point we discussed with the last panel on the number of individuals or organisations that are perpetrating all of this crime. I think there are various statistics about there only being around 100 cyber criminal kingpins. How do you quantify that?

Andrew Archibald: A colleague of mine, Troels Oerting, recently said that it was around 100. I would not put a figure on it. I do not think our intelligence is sufficiently developed to say with real confidence what that number looks like. It was interesting that one of the previous panellists referred to around 1,000. I think that highlights the challenge. I do not think it is a large number, it is a relatively small number. What I am speaking about when I speak about the kingpins are those that write the codes and the programmes, and those

malware developers. Those are the kingpins, I think, but I would not want to say it is 100 or 1,000. I do not think our intelligence is sufficiently developed to be confident about that.

Q217 Alok Sharma: Whether it is 100 or 1,000, would you like to hazard a guess of the percentage of those that are based in China, Indonesia, basically the east and the Far Eastern countries?

Andrew Archibald: I would not like to hazard a guess. What I would say is many of them are in Russian speaking countries. That would be as far as I could go with any degree of confidence. Those skills will continue to develop and that may change, but that would be my pick.

Q218 Chair: Mr Archibald, do you bank online?

Andrew Archibald: I do.

Chair: Do you, Mr Toon?

Donald Toon: I do.

Chair: Mr Fell?

Simon Fell: I do.

Q219 Chair: Would you recommend it to those who are less financially sophisticated as consumers than yourselves?

Andrew Archibald: I would. I would say, however, listen to the advice and take up the opportunities that the banks give you when you do bank online about downloading the security and the protection that they offer. Although I enjoy banking online, I think my wife wishes I had never learned about banking online, it is too easy to access.

Q220 Chair: Mr Toon, Mr Fell, anything to add?

Donald Toon: Very similar position.

Simon Fell: The same from me. The only thing I would add is that from a fraud perspective we are seeing a growth in online fraud. More and more services are moving online and therefore that is where the fraud is going too.

Q221 Chair: That is what is being reported and, as a result, it is putting people off. But the message you are giving today is that it is safer to bank online, that is what it sounds as if you are saying.

Simon Fell: If you use it appropriately, it is certainly safe.

Chair: It is the “used appropriately” that is—

Andrew Archibald: I think that is the message we have to get across and we have to repeat that message as often as possible with some of the government initiatives around: streetwise, get safe online and others. We have to reinforce that if you are going to use those then protect yourself and take advice.

Q222 Chair: Mr Fell, your fraudscape report found that the level of fraud fell by 11% in the previous year but, as you pointed out yourself, the ONS concluded that it had increased 21% over the same period. What really went on? We do not know, do we?

Simon Fell: We are collecting the figures for this year and we are seeing it increase again. Fraud is not going to go away and we only see a small part of the picture.

Q223 Chair: But we do not know the answer, we do not have even halfway reliable stats, do we?

Simon Fell: No, and I think this is—

Q224 Chair: Do you not think we have to do more about that?

Simon Fell: I absolutely do and I think this is a big part of the problem. Going back to your question on online banking, one of the reasons people maybe do take risks when they use services like this online, is that they are not aware of the scale of the threat.

Q225 Chair: What are you as an organisation doing to collect more reliable stats?

Simon Fell: We are fed our information by our member organisations, so we are cross sector, which does include the banks. They are audited, we make sure the figures they give us are accurate but, again, that is only a part of the picture and we are aware that we are, as an organisation, only part of the picture for even just the fraud landscape in the UK. What we would like is to see our figures, and others, collected and put in the official crime statistics. That would allow law enforcement to properly direct resource. It would allow politicians to be able to put the appropriate pressure on organisations to focus on the issues that really affect consumers, and it would allow consumers to be able to look at their own behaviour and think, “Actually, there is a threat here and I need to change the way I am engaging with the online environment”.

Q226 Chair: In the earlier session, Mr Clayton suggested that we should consider finding ways of encouraging banks to compete on minimising fraud, which would presumably require some sort of information in the public domain about the relative performance of each bank. Would you all support that? Would you support that, Mr Fell?

Simon Fell: There are two issues here. As a fraud prevention organisation we work on a non-competitive basis and we have done everything we can to take competition out of the issue of fraud because we know that if you collect more fraud data you can prevent more fraud from occurring. Prevention is better than cure in many cases. But then there is the other issue of keeping your consumers safe. That is providing them with the software and advice in order to keep their home PC or their mobile secure. I think that is an area that is ripe for competition.

Q227 Chair: Did you agree with the evidence that you heard earlier that it may be that not enough is being done in this field by the banks because banks do not have sufficient incentive to put the resources into it?

Simon Fell: They are certainly putting a lot of very good and useful information out there.

Chair: I am talking about the resources into tackling fraud, not the resources into telling the public about it.

Simon Fell: I could not speak for the industry but I think they are putting a lot of resource into it. They are doing their best to—

Q228 Chair: I am not asking you to speak for the industry, on the contrary, we have you before us because we want your view, not the industry's view.

Simon Fell: I think they are doing an awful lot to mitigate the problem. As I mentioned earlier, we are increasingly moving our products and services online. That takes the threat online. If you look at how a fraudster, a cyber criminal, might attack an organisation now, 10 years ago if you were trying to undertake a 419 scam, you would have to buy envelopes and stamps. Now you can send a million spam emails. How many responses do you need back for that to be a profitable enterprise for you? Probably just one. This is a challenge on a scale that we have not seen before and I think banks are doing a pretty good job of managing that.

Q229 Chair: When you buy a motor car you can make up your mind, “Well, I would like to buy a fast car”, which may not be quite as safe as a Volvo or something, or at least the car manufacturers ostensibly—even if cars are nearer having the same level of safety than they might let on—are competing to some degree on safety. In the area of the safety of your bank account, customers are provided with virtually no information by which to make that assessment. Much less at any rate. That is the question that I am asking you.

Simon Fell: I certainly would not have a problem if that was an area they decided to compete on. Consumers might benefit from it.

Q230 Chair: That would not conflict with the objective of the approach you say you have been taking to try to take the competition out of this subject in order to secure co-operation?

Simon Fell: It is taking competition out of sharing information about fraud for the common good. I do not see that those two areas would necessarily conflict.

Q231 Chair: Mr Toon, do you want to add anything to what has been said in those exchanges?

Donald Toon: A couple of small points, perhaps. I would be very cautious about greater competition around security and fraud. One of the previous witnesses made the point that the banks share a huge amount of information because they are very conscious that competition around security could lead to significant problems simply because banks will not share information about risk. They will look for competitive advantage all the time. Ultimately that may be of benefit to consumers but it could certainly be a situation where a lot of consumers will be hurt in the process. It is something I would certainly take as a very cautious step.

Q232 Chair: The end point is that in all cases we are trying to maximise protection for the consumer. Mr Archibald, anything you want to add?

Andrew Archibald: As a consumer I would like to know that. If I was answering that as a consumer looking at which bank I would like to bank with, I think that would be really helpful and it would inform my decision. I would say, just finally if I may, I think the banks are collaborating and sharing a lot more information than perhaps they have in the past, and they are doing it through the cyber information sharing partnership posted within CERT UK, where all the major banks and a number of the other banks share details of attacks or of attempted attacks on their infrastructure, and share code and AMOs and other details that can benefit colleagues in other banks.

Chair: We have had a very interesting second session as well as first this afternoon. Thank you very much for coming to give evidence. We may trouble you with further requests for information in writing. We look forward to those exchanges. Thank you very much indeed.