HOUSE OF COMMONS

Treasury Committee

Oral evidence: IT Failures in the Financial Services Sector, HC 1766

Wednesday 17 July 2019

Ordered by the House of Commons to be published on 17 July 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Colin Clark; Mr Simon Clarke; Charlie Elphicke; John Mann; Wes Streeting; Alison Thewliss.

Questions 85-209

Witnesses

I: Graham Bastin, Head of Operational Resilience, Barclays, Anne Boden MBE, Chief Executive Officer, Starling Bank, and Ian Lundberg, Chief Officer, Senior Vice President, Client Services Europe, Visa.

Written evidence from witnesses:

– Barclays, Visa

Examination of witnesses

Witnesses: Graham Bastin, Anne Boden and Ian Lundberg.

Q85 **Chair:** Good morning to our panel. Thank you very much indeed for being here for this evidence session in relation to IT resilience in the financial services sector. I am going to ask you to introduce yourselves. We have a series of questions for you, and we are very grateful to you for taking the time to be here this morning and share your expertise with us. Mr Bastin, perhaps we can start with you—just a brief introduction.

Graham Bastin: Sure. I am Graham Bastin. I am head of group operational resilience for Barclays bank.

Anne Boden: I am Anne Boden. I am CEO and founder of Starling Bank.

Ian Lundberg: I am Ian Lundberg. I am the chief officer for client services for Visa in Europe.

Q86 **Chair:** Thank you all very much for being here. I will ask a general opening question. Perhaps we will start with you, Mr Bastin. It would be very interesting to hear how your institution's attitude to and handling of operational resilience has changed in recent years. I am assuming it has changed; it seems to have shot up the agenda. Did the TSB incident last year concentrate minds in a way that they perhaps had not been concentrated before?

Graham Bastin: The attitude towards resilience has been significant in Barclays for a number of years. We have probably spent upwards of £1 billion over the last three years, and there are probably upwards of 20,000 people in ops and tech who work on this topic, so it has remained a significant agenda item over that period.

I have been running technology resilience for the last three years, and one of the changes that we have seen is the convergence of tech, cyber, third-party, premises, people, and resilience, and the role that I have taken on most recently has converged all of those under one leadership, under me. Looking at TSB, there were certainly lessons to be learned. We actively look at our own disruptions and make sure that we take the lessons learned from those. We also seek out where we have seen issues more broadly, and make sure that we will not succumb to those as well.

Q87 **Chair:** Ms Boden, I know that Starling Bank has not been in existence for that long, so perhaps you could tell us about how important operational resilience is in setting up a bank as well?

Anne Boden: Thank you for inviting me to talk about resilience and reliability, and what Starling Bank is doing about this. I have a long career in technology and banking. Four or five years ago, I decided to start a new bank—Starling Bank—that was built on new technology principles in order to meet the new needs of customers. Technology is what we are all about at Starling. We have a huge number of engineers. I am a computer

scientist. What we have done is build our systems from the ground up so that we can be hugely resilient to a failure in a component part. That is why we are in the market at present giving something that is quite different, and quite resilient and reliable, to customers.

Q88 **Chair:** Mr Lundberg, you obviously come at it from a slightly different perspective as a payment services provider and facilitator, but, again, how important is operational resilience to Visa? Obviously, TSB is slightly different, but we are going to explore when things go wrong; I know you had your own outage at Visa. When things go wrong for other people in the financial services sector, do you look and ask, "What can we learn from that?"?

Ian Lundberg: Security and trust are incredibly important to Visa. They are at the heart of everything that we do. As you reference, in June last year we had our own incident. Certainly, it meant that we fell short of our goal of having the availability of our network 24 hours a day, 365 days a year. Importantly, obviously, consumers and merchants are looking to have it available then as well. We have learned some lessons from that. It is very important, as we work with our partners in the payments ecosystem, that we work together to make sure that the ecosystem as a whole is operationally resilient, not just each individual piece.

Q89 **Chair:** The regulators published a discussion paper on operational resilience. Mr Bastin, what was the Barclays perspective on that paper, broadly? Did it cover the right things?

Graham Bastin: In the main it did. The thing that we really welcomed was the customer lens that they were looking at. At Barclays, we have been looking at the most critical services that we deliver to our customers and making sure that they have the highest level of resilience. I think the discussion paper talks in part about that. We really welcomed that aspect.

The other thing that certainly resonated with me was around the governance. Again, as you can imagine there is strong governance within Barclays. There is a flow of management information, both up and down the organisation, with strong board oversight, which is, again, one of the points that comes out of the discussion paper. The final thing for me was around the culture of the organisation. It is something that we have been trying to embrace, using those governance forums not just to create strong controls but to allow people to express concerns and seek support for the resilience issues that they can identify.

Q90 **Chair:** Ms Boden, obviously we have a very large institution, and perhaps a slightly smaller institution sitting in front of us. It would be interesting to hear your perspective on the discussion paper, but also on proportionality. Where do you feel the regulators are on approaching that?

Anne Boden: We are a bank; we provide essential services to people going about their daily lives. Whether you are paying for your shopping in Tesco or making a payment for your rent, the services have to work. The regulator does not apply proportionality criteria to regulating people like

ourselves. We have to be available. We have 700,000-plus customers now who rely on us.

Q91 **Chair:** And you think it is right that they don't apply—

Anne Boden: Yes, absolutely. We are a retail bank in the UK, and we provide services to SMEs. Those customers need to be able to rely on the service and the technology. Despite the fact that we are smaller than Barclays, our systems are very robust, very resilient, very new and able to cope with the pressures that the customers and the population put on us.

Q92 **Chair:** Thank you. Mr Lundberg, did the discussion paper have as much resonance for Visa as it would for a retail bank? What is your relationship with the regulators like?

Ian Lundberg: Absolutely it resonated with us. I agree with a number of the comments that Ms Boden and Mr Bastin made. The other thing that we welcomed was the idea of looking at the payments ecosystem in total, and the interdependencies between us all. Visa is an important part of that ecosystem, but clearly there are a lot of issues and other players that we need to work with to ensure that, in the event of there being a disruption, the impact on consumers and merchants is minimised. From that perspective, we welcomed the discussion paper.

Our relationship with our regulators is a good, constructive one. It is appropriately challenging and rigorous where it needs to be. We work closely with them to make sure that, as we go forward, we are doing everything we should be doing from a regulatory perspective.

Q93 **Chair:** Mr Bastin, in your written evidence you argue that "technology firms…are increasingly starting to engage in financial services activities, while existing outside of the regulatory perimeter." Can you unpack that statement for us a bit? Which firms' activities were you thinking of?

Graham Bastin: I think it is widely recognised that we are in an interconnected world. Many of the services that we provide to our customers are provided either directly by Barclays, or we use third parties and services. We retain the accountability when some of those things are outsourced, but there are entities that those services traverse that perhaps are not of the same standard or held to the same regulation. The reference in the written submission is a conversation that we have had with the regulators about thinking more broadly about the customer service in its totality, rather than through the individual entities that it goes through.

Q94 **Chair:** Ms Boden, when you applied for a banking licence for Starling, do you feel, given your computer science background, that there were sufficient questions about operational resilience? Was it a big part of the process? There is a concern—we have heard evidence already—that the regulators themselves are struggling to have people with sufficient skill to understand operational resilience, in the same way that they might understand prudential regulation.

Anne Boden: The evaluation process for applying for a licence takes many years. We started the process in the middle of 2014, we received our licence in 2016 and we launched to the public in 2017. During that period, we were constantly challenged to make sure we had gone through all the processes, done the testing and could demonstrate that we understood operational resilience. During that process, we used our own skill, external consultants and various other parties to help those conversations with the regulator.

We are going through a change whereby new technology is being brought into the market. When we started the process in 2014, we weren't operating in the cloud. Since then, cloud technologies have become ubiquitous. People are using them; they are safer. In some respects, the regulator has had to catch up, but it is catching up and it takes these issues very seriously.

Q95 **Chair:** Mr Lundberg, do you think there is over-reporting or under-reporting of incidents generally across the sector? Visa was very open about the issues that it faced. The FCA obviously publish figures about incidents. Do you hear in the sector that people still are not reporting sufficiently?

Ian Lundberg: Obviously we are regulated by the Bank and the PSR, so our reporting requirements are different from those for Ms Boden and Mr Bastin. But from our perspective, I think the reporting that we provide is appropriate here both to the Bank and to the PSR in the event of it having a consumer impact.

Q96 **Chair:** Mr Bastin, you have been in this area a long time. I mentioned skills and a lack of skills in regulating. One of the things we have heard about, again from people giving evidence, is the lack of people with sufficient skills as things develop. Do you struggle to find the right people for Barclays? Do you have to do a lot of training in-house to get the skills you need so that you are satisfied that you are providing the resilience needed?

Graham Bastin: We recognised probably six or seven years ago that the world was becoming much more dependent on technology and the skills required for that would become highly in demand. So one of the decisions we made was to set up a technology campus in the north-west of England, which I run. Back then, there were 2,500 people there; there are now 5,000 people. The way in which we grew that talent—we hired about 600 apprentices and over 40% of those are women. That's not nearly enough, but still it's headed in the right direction.

One of the reasons why we did that, if it's not obvious, is that we saw the need to bring in talent where we could do the knowledge transfer between some of the older technologies and move towards digital and mobile, AI and data analytics, and give those people a career path where they would stay with us for a long period of time. We felt that that would give us an area of strength in terms of people understanding the technology and

being with Barclays for a period of time. That was a significant investment. We are doing something similar in Glasgow as well.

Chair: That is very helpful. We will explore a lot of these issues in more detail.

Q97 **Alison Thewliss:** I am hoping to come and see you in Glasgow soon—your new site is in my constituency. I understand that 65% of incidents reported in 2018 were in retail banking. Do you feel customers are experiencing more IT incidents involving their financial services providers? Is that a growing trend within each of your brands?

Graham Bastin: In Barclays in 2018 to 2019 we have seen the number of technology incidents go down by 40%. In the years prior to that it was a little bit less—in the order of 15%. That is probably as a result of some of the things I referred to earlier, such as the levels of investment, the talent we have tried to hire, the reduction in complexity, addressing some of the legacy that existed perhaps 10 years ago or so, and the movement towards some of the newer technologies that Ms Boden referred to earlier. So I think we are headed in the right direction, but it is not nearly good enough yet.

Anne Boden: We have not had any reportable incidents. That does not mean that our customers have not been impacted. There have been four occasions where we have advised our customers that part of a service was not available.

I think what we are seeing at the moment is that there is more reporting of incidents. I have had a long career in banking and technology, and there is now far more emphasis on really monitoring when something is an issue and not an issue and making sure that report gets in. But I also think there is a situation where organisations are somewhat fearful of making change because of the implications of an outage. It is a balancing act.

At Starling, we have built our systems so that we can constantly update them. A little bit and often means that we can minimise the amount of impact on customers if something does go wrong.

Ian Lundberg: As I referenced before, in June last year we had an incident that was well documented at the time and reported. Since then, we have invested heavily in operational resilience—as we had done before. As you know, we proactively commissioned an independent report to identify what had happened and to come up with some recommendations and findings. We publicly accepted all of those recommendations and findings and have implemented a number of them. We are in the process of embedding them.

To Mr Bastin's point on investments, one of the things we have done is completed the migration from the European authorisation platform we had, which was the cause of the incident last year, to our global Visa authorisation platform, which is a higher level of resilience. Since then, we have not had incidents to report from an authorisations perspective.

Q98 **Alison Thewliss:** The major incidents obviously get a lot of attention in the media, but I think you have all hinted that minor incidents can happen on a smaller scale and perhaps more regularly. Can you tell me how often your customers experience those smaller disruptions, such as to their ability to log on to banking services or make card payments? They may be for only a few minutes, but how commonplace are they, and how are those incidents logged and identified? If they are not of a higher reportable standard, how do you deal with them?

Anne Boden: There are big incidents that hit the press and everybody talks about. Thankfully, we have not had any of those, and we have not had any notifiable incidents, but all banks have small things. We have had four this year. Two impacted the digital wallet—Apple Pay. Another meant that faster payments was intermittent for something like a few minutes. When those things happen, it is very important that the customer understands that there could be an impact. We have several ways of advising customers: in-app messages or broadcast messages. Now we have the technology to communicate with customers, we have to use it. In most cases, new banks are delivering systems that basically are not on or off; certain parts of the system can recover and catch up, so very rarely do people lose the whole system. Therefore, some advice and guidance along the way is a really good idea for customers.

Ian Lundberg: From our perspective, to Ms Boden's point, there are small things that happen, and we log those, track them and do root cause analysis on them to prevent them from happening again. Given the relationship we have with both issuers and acquirers, where we see issues that they may be experiencing, we communicate that to the other party. If an issuer is having a particular problem, we inform the acquirer so they are aware that a particular issuer may be having an issue, and vice versa. We play our role in the ecosystem, as I was referring to before, to make sure that there is that flow of information back and forth, which means both issuers and acquirers can respond accordingly to their consumers and merchants.

Graham Bastin: I am at risk of repeating what Ms Boden said, but just to emphasise it, one of the big learnings we have had over recent years is about the value of communications to customers when there is an incident or an outage—a disruption of any sort. If you send a text or some other kind of alert, even when a feature on the digital mobile app is unavailable, or if you signpost that there is going to be a planned disruption at a weekend, which we have done fairly recently, that is really welcomed. Customers then can conduct their banking services ahead of that or plan around it, or you can point them to a different channel. You can say, "Our mobile banking is going to be unavailable from this period to that period"—usually on a Saturday night into early Sunday morning, when the fewest customers tend to use that platform—"but the ATMs are available," and so on. That is really well received in terms of the communications we share with customers.

Q99 **Alison Thewliss:** Is it your feeling that some of the services you offer are more important or more critical for customers than others? For example,

would you prioritise one part of your service over another?

Graham Bastin: We do. We have a very clear risk taxonomy that describes the most important services to our customers. Just to bring that to life a little, "Get my balance" is probably the most used and the most important service to our customers, along with "Make a payment" and so on, so the level of resilience we put around those services is higher than that for some of the other services, such as "Change of address", which is less time critical. We absolutely think about the criticality of the customer services.

Q100 **Alison Thewliss:** Would that be the same for Starling and Visa?

Anne Boden *indicated assent*.

Ian Lundberg: Yes.

Q101 **Alison Thewliss:** Is there a standard target within the industry for the availability of critical services? You all seem to think that things need to be prioritised that way, but is there a standard across the industry for that? Or is it up to each individual provider?

Ian Lundberg: For Visa and our network, our goal is to be available 24 hours a day, 365 days a year. We are on the global network now. Since the turn of the century, that has been the case for all but 156 seconds over the last 19 years, so we strive for continuous availability.

Q102 **Alison Thewliss:** Mr Bastin, if customers access their data services through different channels, such as open banking, do they receive the same availability of service as if they had accessed those directly?

Graham Bastin: Yes. What we call resilience category zero is the most important service. Getting my balance and making a payment are two examples. Open banking is another one of those, absolutely.

Q103 **Alison Thewliss:** If customers are left out of pocket as a result of an operational incident, would they be compensated by each of you? How do you consider cases of compensation for inconvenience or non-financial loss?

Ian Lundberg: The system in the UK is designed to compensate consumers in the event of an incident like the one we had in June last year. The rules for complaint handling are very clear, and transparency and accountability for it are well documented. From our perspective, the relationship with end consumers lies with banks such as Barclays and Starling. They are in the best position to assess the claims for redress from the consumers. That is something that other consumer advocates such as Which? or MoneyExpert would agree with. Immediately after the incident last year, we said to the banks, "As you stand behind your consumers, we will stand behind you," and we paid all the claims that came through to us from the banks in full upon receipt.

Q104 **Alison Thewliss:** After the TSB incident, some customers struggled to get in touch with the firms. It took time for the firms to process that as well. Say somebody's direct debits, for example, have bounced, and they

go into arrears and all these other things. How quickly would you expect to process that kind of complaint and get full compensation for it?

Graham Bastin: We proactively reach out to customers who have been impacted in much the same way as Mr Lundberg has described. We do not rely on customers contacting us. Some do, but we have exactly the same policy and outlook, in terms of making sure that people are not out of pocket as a result of that disruption, and are compensated appropriately.

Anne Boden: We have never had an incident that resulted in our having to compensate customers, but we would. We are a technology-enabled organisation, so we deploy all our technology forces to make sure that that is done as quickly as possible.

Q105 **Alison Thewliss:** Do you think, Mr Bastin, that different companies do things in different ways? Should there be a standard for what customers should expect from their banks?

Graham Bastin: I think that would help. You will hear me talking about severity 1 incidents, or the way in which we think about customer services, and what we call customer journeys. I am sure other firms think about things similarly, but they probably use slightly different words and taxonomies. I don't think they are materially different, but it probably would help to have consistency, at least in the language that is used.

Q106 **John Mann:** How does one of my constituents find out when there is a major problem?

Chair: Who is that addressed to?

John Mann: All three.

Chair: Mr Bastin, how do Barclays customers find out?

Graham Bastin: We did a major change two weeks ago within Barclays. We had been planning that change for 18 months and discussing it with the regulators and stakeholders. In the week leading up to it, we sent out messages on mobile apps for those that have mobile banking. We informed branch colleagues and contact centre colleagues of the change. When they had the opportunity, they were to discuss it with customers, to let them know that it was happening. Indeed, on all our ATMs throughout the UK, there was a banner that said there would be an outage during this period. We tried to use all those channels for those eventualities.

Anne Boden: If one of your constituents was using Starling and, for example, there was a card problem—they are standing there trying to pay for something, and it does not work—hopefully, we would have got to them first. On the app, we would have sent them a broadcast message, so that they were told there was a problem: "You can't use your card for this, this and this. Go to the post office, or whatever." We have never had that situation, but that is what we would attempt to do.

If there is a problem with the app, it is very unlikely that the whole app would not work; at least certain sections of it would. In that case, yet

again, we would have broadcast messages, because we have the capability to go online and, from our control centre, send out those messages to groups of customers immediately.

Ian Lundberg: From our perspective, one of the things we have introduced in response to the findings and recommendations of the EY report last year, is something called a rapid activation protocol. That means that at the moment we identify that we have a crisis and initiate that internally within Visa, at exactly the same time, we start a communication to all our major stakeholders.

That would involve all our clients, both issuers and acquirers. That is done through both email and SMS to our largest issuers and acquirers. We would also send social media statements, obviously, to our board and regulators. All that stuff happens at the same time that we ourselves are aware of the fact that there is a crisis.

The issuers and acquirers would then share that information with their consumers and merchants alike. One of the other things that we have done is create a community across our largest clients of the relative communication teams, so that we can be constantly in contact with one another and ensure that messages are aligned across the ecosystem.

Q107 **John Mann:** But one of the problems that the sector highlights—I answered some questions from Barclays on this yesterday afternoon—was about crime and people getting fake messages, SMS and emails, from fraudsters pretending to be you. You have all just said, in essence, that that is the methodology you use for communicating. How does one of my constituents know whether it is you or a fraudster? Is there 100% certainty in that? Mr Bastin, it was your bank I was answering yesterday. Why don't you have first go?

Graham Bastin: You are right: scams are growing. When there is any kind of disruption in Barclays, not only can customers not transact with us, but fraudsters cannot as well, so fraud does not occur there.

The challenge, as you described, is that there are criminals who attempt to reach out to customers and pretend to be a bank or another entity, saying, "Could you please give us your credentials, and we can help you in this situation?" They are not always necessarily trying to be Barclays, but they are trying to be helpful groups of people.

One thing that Barclays did, as you will probably be aware, was have quite a significant advertising campaign to make the public—not just Barclays customers—aware of scams, the importance of protecting your password and so on. That is one of the areas, in terms of education and awareness, in which we probably collectively need to do more.

Q108 **John Mann:** But it is about your system. This goes for all of you; I'm not just picking on Barclays, though I will do, because—

Chair: You're here.

John Mann: I completed your survey yesterday. Don't worry, I will come back to the others. There is an inherent contradiction, isn't there? I have been on Barclays training, where you tell people, "Here's how to avoid scams," but as we saw with the TSB fiasco—and with RBS as well—criminals are getting more sophisticated. I don't think they are anything like as sophisticated as they can be, but they are already targeting where there are problems. There is a fundamental flaw in the process, isn't there?

Anne Boden: If I may, I will talk about how it works in Starling. We try to issue notifications and broadcast messages from the app. The app is secure, sits on your phone and is secured by either various biometrics or passwords. You can go into that app, click the information "i" and read the status. Our customers get reassurance from within the app, and not through some spurious SMS messages.

Q109 **John Mann:** What is to stop a sophisticated fraudster creating a parallel app and sending it to you? That has happened in the banking sector, with ramped-up mortgage transactions and people losing the whole of their mortgage transaction—I've had to deal with some. An entirely new parallel bank account is established and sent to people. What is to stop a fraudster creating a mirror app and sending it out? Someone downloads it because they think it is from you, at a time when there is a problem. They have been given advice: "Because there is a problem, here's your new app." What is to stop that?

Anne Boden: We have a lot of processes in place that are part of our cyber-crime programme, and that protect the bank and the bank's customers from that sort of scam. We work very closely with the various authorities and our own technical experts to ensure that it cannot happen. Nobody can say 100% that it can never happen.

John Mann: No, you said "hopefully" previously.

Anne Boden: But the particular problem that you describe is very, very rare. We think—I and other technical experts from banks—that particular problem is unlikely to happen.

Q110 **John Mann:** So far, major problems like the TSB fiasco, which this Committee dealt with at painful length, are rare for my constituents, but they did not really happen at all 15 years ago, so they are not as rare as they were. You are all saying that your institutions and your competitors are moving to increased use of technology, so it is not totally secure, is it? My question is: what are the standards that my constituents can expect, when at some stage, without question, somebody is going to break the system for someone somewhere? What standards are required if my constituents are to feel confident that if they choose you, as opposed to a competitor, as a provider, they are guaranteed? What does "guaranteed" mean for them?

Ian Lundberg: The Visa rules are quite clear. There is zero liability for consumers in the event of there being a fraudulent or unauthorised transaction on their account.

Q111 **John Mann:** Yes, but that is only one definition. Let's take Visa. You left me stranded in Buenos Aires in 2009—you did, Visa—because of your technology being incompetent.

Ian Lundberg: I don't know how to answer the question.

John Mann: You did. It was because your technology was incompetent—your algorithm. I had been in three different continents in five days, as people occasionally have to in this modern, interconnected world. I get to Buenos Aires, and I cannot use the Visa card. I find out retrospectively that it was purely because I was in a third continent. Your algorithm says that my card will not work, and I am left high and dry, with no cash on holiday.

Ian Lundberg: Obviously, I cannot talk about your specific thing.

Q112 **John Mann:** No, but the specifics are true. That is my point. It is a question of what the standards are. Let me broaden the question. Should the standards be stronger and absolutely common among all providers, in terms of what the guarantees are?

Chair: Guarantees of service?

Q113 **John Mann:** Guarantees of service, and guarantees of my money and my position as a consumer, or the position of my constituents.

Ian Lundberg: From a Visa perspective, as I referenced before, we would literally be available 24 hours a day, 365 days a year. Obviously, we are part of the ecosystem. In your particular instance, while I cannot talk about it, the issuer of the card plays a role in that entire transaction, so I don't think it is necessarily fair to lay the blame all on Visa. From our perspective, we strive for availability 24 hours a day, 365 days a year. That is the standard that we work for.

Q114 **John Mann:** But you are not talking about what the standard is there. That is not an acceptable answer. It is only one incident, but it happens to be a real one. I could obviously cite plenty of others from my constituency and all sorts of financial institutions, but let me pick on you, because this is what I am familiar with. I am left high and dry. This is not a complaint about Visa, but about your standards and the industry's standards. I am left high and dry. I am having to make phone calls—luckily I am in a hotel that is prepared to allow me to make phone calls, at great expense—to eventually manage to get someone to sort it out, so that I am able to leave Buenos Aires, having got some cash. There are ways around these problems, but I might have missed a plane because of that. It might have been somewhere rather more remote than a nice hotel in Buenos Aires.

When the service relies on such levels of IT—that is the world we live in—the issue is how you define what those guarantees are. I am not hearing that. Let me broaden the question to you all. What improvements are needed to the industry standards, across the industry, to deal with the kind of problems that will occur to somebody—one of you, or one of your competitors—in a very big way in the future? What improvements are

needed in those industry standards?

Anne Boden: If I could pick that up, I think we, as a technology industry and as a banking industry, have defined things for too long in the way that we would look at things—"It's 99.99% this," or whatever. Technology and banking are so intertwined nowadays that we have to see it from the customer's end. How many times was their card declined? How many times were they left stranded? We all try to put ourselves in the shoes of the customer now.

Your particular incident, when you were left stranded abroad, was probably because of a fraud system triggering because you were travelling. The system was saying, "We want to protect him; let's stop this fraudster spending his money." As we have got more and more technology, artificial intelligence and machine learning, we can make that decision better and better. Yes, we are living in an age where banking is all about technology. The new banks are run by technologists, and we are trying to take more of that intelligence, and to make intelligent decisions about whether to stop your card in Buenos Aires.

That is why the industry as a whole is investing in machine learning, artificial intelligence and better ways of people being able to go into an app and say, "Yes, that's definitely me. That's not a fraudster." That is where we can now apply technology to improve the service. For many years, technology was used to make the customer service agents more efficient. It was something in back office, to make a bank more profitable. Now we need to apply a lot of that intelligence and technology to make the customer experience more acceptable, because a card is so important to your financial life.

Q115 **John Mann:** Mr Bastin, is there an improvement you would like to see in the industry?

Graham Bastin: I know you are looking for standards, but there is a responsibility on multiple fronts. Scams to individuals come from multiple sources, not just from banks, so there is more we can do to educate people to be able to detect when something does not look right. There is further work to be done there, and we should not ignore that. What we do at Barclays—I get your point, because we have a lot of customers who come into branches or call our contact centres because they want reassurance, saying, "I got this email. I am not sure about it."—is, actively through our Digital Eagles network, to try to bring people's education up in that respect.

Q116 **John Mann:** Will you keep more branches open then?

Graham Bastin: We still have the highest number of branches in the UK, as you know.

The third point is that, where we can see customers have taken reasonable steps but have been scammed or defrauded, then, as Mr Lundberg described, policies are in place to make sure that they are properly compensated. That is absolutely the approach at Barclays as well.

Chair: We'll move on. Steve.

Mr Baker: Thank you. I just wish my life was as glamorous, Mr Mann.

John Mann: You're not accompanying me.

Q117 **Mr Baker:** If I may, I will turn to the matter of operational incidents and innovation, but first, may I clarify something? Mr Lundberg, you said it very briskly, but I think you said that you had had 156 seconds of outage in 19 years. Is that what you said?

Ian Lundberg: I did say that, yes, sir.

Q118 **Mr Baker:** That is eight 9s reliability, isn't it?

Ian Lundberg: If that is the maths, yes.

Q119 **Mr Baker:** That's the maths I worked out. Is that not quite an extraordinary standard that you have achieved?

Ian Lundberg: Yes. We invest massively every year to ensure that the security and reliability of our network is what our customers expect—so, 24/7, 365 days a year. The investment is across a whole number of fronts. Here in the UK, for example, we recently invested heavily in a new data centre. We have also invested heavily in creating a cyber fusion hub, which we have here in the UK—we think that is particularly important, given that the UK is leading the way in a lot of the cyber-security activities that take place. We look at investing in our people and, very importantly, in our network, to make sure that the capabilities there are leading-edge, so that we can continue to provide the security and reliability that our customers expect. An example of that is that, twice a year, we release enhancement packages to the networks, and we work very closely with our clients to ensure that they are ready, so that this is a seamless proposition. It also strengthens the network overall.

Q120 **Mr Baker:** You have talked about investing in a cyber-hub and so forth, but what are your top three or five priorities for operational resilience?

Ian Lundberg: Cyber-security is No. 1. We invest heavily in that. It is probably, for all of us, the one that comes top of the list in terms of keeping you up at night. Another thing we are also careful about, as a global digital payments network, is, whenever change is introduced into the system, to do it in a controlled manner. That is incredibly important. As I have just mentioned, that is one of the reasons that we look to package a lot of changes that we make into two releases each year—you might imagine the update that you get to your smartphone iOS, although it is a little more complicated than that. We do that twice a year, working with our clients to make sure that we are strengthening the network that way from a change management perspective. Those are the two major areas that I would look at for operational resilience.

Q121 **Mr Baker:** Thank you. Ms Boden, what would you prioritise when you look at your resilience?

Anne Boden: We are a growing bank. Therefore, our No. 1 priority is to ensure that we retain the trust of our customers. People don't know our name, but are beginning to hear our name, so trust—being reliable, responsive and human—is very important. So resilience, and operational resilience, is a hygiene factor; it has to come before everything else. Unless we are there for customers all the time, they will not trust us, they will not use us, and our business will not grow.

Q122 **Mr Baker:** I might clarify what I am getting at in a moment, but first, Mr Bastin, what are Barclays' top priorities when you consider operational resilience?

Graham Bastin: Whenever we think about operational resilience, as I said before, we think about it through the customer lens. We look at those top, most important things that our customers want to do with us, and ensure that they are designed, engineered and tested to the highest levels of resilience. What that means is not just the technology but, as Mr Lundberg described, cyber, the third parties that we touched on, and maybe the premises—all the components and assets that support those customer services, and ensuring that they are designed and engineered to the highest levels.

Q123 **Mr Baker:** There is a bar chart from the FCA looking at causes. They list, in this order, change management, third-party failure, and software and application issues as the causes of outages, and then cyber-attack, hardware, human error, process/control failure, capacity management, external factors, and "Root cause not found". It was very interesting, Mr Lundberg, that you named cyber first, which is fourth as a cause, overall, of instances, and you talked about change management as your second priority. It feels as if, to achieve your eight 9s reliability, you are pretty good at change management now.

Ian Lundberg: As I look at operational resilience, there are four components to it. One is the investments that you make to prevent there being an incident or an issue in the first place. The second is how you understand the impacts, should there be an incident. Then you look at how you respond, and then the recovery as well. A lot of our investment is in how we prevent there being an issue to start off with. A lot of that investment is around cyber-security because we want to make sure that, as people try to attack the network, we can prevent that from creating an incident itself.

Q124 **Mr Baker:** Ms Boden, you have specifically talked about the ubiquity of cloud services, but nobody has mentioned third-party failure as being one of your resilience concerns. However, according to the FCA, that is the second most common cause of outages. How do you ensure that your third parties do not lead to outages?

Anne Boden: Third parties are very important in the banking structure. We rely upon Mastercard as a third party to provide services to our customers. That list you mentioned, headed up with change management, said that change management is the biggest issue. The technology industry has very much changed its attitude to change management in the

last 10 years. We heard from Mr Lundberg that there is an update every six months. Modern technology is now released and change managed by implementing a little bit of change often. By having a little bit of change—a few programmes changed—and doing it several times a day, you minimise the impact of that change.

We all know that when you do big change—big migrations, big separations of banks, and big migrations of systems—we put customers at risk. Therefore, modern technology techniques are all about a little bit of change and very often. We change our system something like four times a day. We have hundreds of thousands of automated tests that run. We have processes whereby we issue new code into the production environment, and we release it to a small number of users, then to a few more, and then to a few more servers. If anything goes wrong, we can back it out. That is the way modern technology is now delivered. The problem that we have in the financial services technology world in general is that the majority of the systems have been built not to support that method of change management.

Q125 **Mr Baker:** I should say that I was an agile software engineer before I came into politics, so I am delighted that agile has gone so far, but even I am astonished that you are going to live changes four times a day. That really is remarkable. Is that something that Barclays recognises?

Graham Bastin: I agree with a lot of what Ms Boden has just said. We execute 25,000 changes a month. That might sound like a lot, and maybe it is, but it is exactly what Ms Boden described: we decompose those bigger changes into much smaller releases that we know we can test individually. If there were an issue with any of those changes, we can either back that out, or the impact on our customers would be minimal. It would be one of the features on the mobile banking app, for example. With the increase of automation and—you will be familiar with this—with DevOps and agile, we are seeing higher quality execution of those changes, and that is important.

Q126 **Mr Baker:** Really? Twenty-five thousand releases to production a month?

Graham Bastin: Correct.

Q127 **Mr Baker:** That is really astonishing. So your change management procedures are extremely robust, I imagine.

Graham Bastin: They are increasingly getting robust, yes.

Q128 **Mr Baker:** To what extent is your change management automated?

Graham Bastin: Large parts of it are. On the weekend I referred to a couple of weeks ago, which was a big change, some 900 people were working across that weekend to execute those changes. There were 240 applications that were moving into a strategic data centre, and the execution of that plan was all driven by an automated tool, whereas in previous years it would have been manual to step through that all. It is the automation that drives the execution of those changes there.

Q129 **Mr Baker:** That is a remarkable thing. Do you think you have incidents that go undetected for some time? By what mechanism do things get picked up? Is it customers reporting things to you, or do you have automated mechanisms for discovering outages?

Anne Boden: We have probes throughout our systems, which are constantly checking whether something is working. We will know within microseconds whether something has not responded. Depending on what it is, we then have an automated process of escalation. If we have an issue, its severity is assessed. Depending on the severity, it is brought to various levels of awareness in the organisation. The important thing is that, if you were to look at our office, we have big display units where we can see all the various aspects of our systems and how they are performing. That is all automated, because we built it from the ground up with that in mind.

Q130 **Mr Baker:** Thank you. Mr Bastin, do you want to add anything on this point?

Graham Bastin: We have made a significant investment in what we call operational command centres. Some of your colleagues will have been to visit the ones that we have in London. They are 24/7 and are across the globe. The investment that we make in the technology to detect those things early and tell us that there is an issue very early on, and in the people we have to interpret and react to that, is important. Similarly to what Ms Boden said, the agenda has changed significantly. To answer your question directly, we don't wait for our customers to tell us; we try to spot those issues well before that.

Q131 **Mr Baker:** Very good. Finally, does any of you have anything to say about open banking and whether it has any particular implications for your resilience?

Chair: For the banks.

Anne Boden: I think open banking is in its infancy. The concept of open banking is very powerful. For many years, the banks have held data for their own benefit, and not for their customers' benefit. Having an open banking environment, where customers can take their data and own it, is very powerful. There is a long way to go. I think we are five or six years away from having something that is really compelling for customers. It has a huge potential, but we are not there yet.

Mr Baker: Thank you very much for your fascinating evidence. I hope you will forgive me, but I am just going to take care of something else.

Q132 **Chair:** Before I hand over to Wes—I know he is also under tight time pressure—I just want to pick you up on the 156 seconds, Mr Lundberg. Obviously, on 1 June last year, Visa suffered a pretty major outage. I just want to be clear whether you are talking about total or partial outages of 156 seconds. In the letter back to me, Visa said, "our UK processing systems were disrupted such that many UK consumers were unable to complete transactions using their Visa debit and credit cards. The incident

began at 14:35 British Summer Time and ended at 00:45." That is longer that 156 seconds.

Ian Lundberg: Correct. I prefaced the 156 seconds by saying that we are now on the global network. One of the things that we completed on 27 September last year was the migration from the European authorisation platform—the platform with which we had the issue on 1 June last year—on to the global platform, which has a higher level of resilience. It is that to which I referred in relation to the 156 seconds.

Q133 **Wes Streeting:** I'm going to build on the questions that the Chair opened with, and focus on some of the things that came out of our written evidence, particularly around the convening role of regulators and whether regulatory expectations are in the right place. I am assuming that, when an incident affects more than one firm or there is risk of contagion, firms work together to deal with it. Am I correct in that assumption?

Ian Lundberg: From a Visa perspective, the answer is yes. The network is connecting the issuers to the acquirers, so we do work together. Across the board, we need to work collectively.

Q134 **Wes Streeting:** I can see why that would necessarily be the case, given the nature of Visa's service. Would banks naturally work together? If it is not necessarily the case, are there are examples of good practice you are aware of?

Graham Bastin: The highest levels of collaboration that I see are around cyber. The banks and the financial industry generally have determined that there is no competitive advantage from being better than the other guy at cyber. So we work with the intelligence agencies, the cyber-defence agency, GCHQ. We share information and intelligence for the benefit of all. That benefits not just the financial industry; organised crime and other actors play in that space. That is a really great example of where I see collaboration. We could do more along those lines in some of the other areas of resilience.

Q135 **Wes Streeting:** Anne, do you have anything to add?

Anne Boden: I am trying to figure out and give an example of when it would be necessary for the banks to get together to co-operate. I cannot remember a serious incident in the industry where collaborating with another bank to process its work would have worked. For example, when we had a Visa incident, UK Finance gave us advice, and we collaborated in that environment to ensure that all customers had the right information. Starling uses Mastercard, not Visa, but in that circumstance we made sure that our customers understood what was going on, because a lot of misinformation was being circulated.

Q136 **Wes Streeting:** Coming back to Barclays, I think your written evidence suggested that there might be a role for regulators to co-ordinate, were there a significant incident where the impact may be broader than the one firm that is directly impacted. Anne anticipated and began to answer my question. Where do you think that role and convening power might

have been helpful?

Graham Bastin: The discussion paper did stimulate some of that, and conversations have started on things like Safe Harbour, for example. Those conversations are in their infancy. You do see collaboration between, for example, Visa and Barclays, where, if Barclays has an issue with its ATM system, Visa will stand in. Similarly, Barclays has the capability to do that. So there are levels of collaboration, but, honestly, I think there is more that can be done across the different firms.

Q137 **Wes Streeting:** Thinking about incidents that you have experienced, what was your level of interaction with the regulator? Did you find that interaction productive?

Anne Boden: Starling is a new bank, so we talk to the regulator very often. As soon as we feel that something could cause a problem, we tend to pick up the phone and advise. That is far more frequent than is necessary under the processes and procedures.

In the new bank sector, the regulators are very close to us, and therefore we do have people who we can pick up the phone to and say, "We think this could be an issue, and we are working on it. Customers haven't been affected yet, but they could be."

Graham Bastin: Again, I refer to the significant change we made a couple of weekends ago. The level of scrutiny and dialogue we had with the PRA and the FCA leading up to that change, and then during and after the execution, where I was personally updating the regulators, was astonishing. Equally, we have regular reviews where, for not just high-severity incidents but all incidents, we look back and say, "What did we learn? How have we embedded those learnings into the firm?" A great deal of scrutiny goes on before, during and after a change of that kind.

Ian Lundberg: There are couple of things, if I may. The opportunity for us to work across the ecosystem more closely will evidently benefit everyone. The cyber-security example you gave is great, and we are seeing it in other areas as well. UK Finance, which you referenced, has got roundtables on incident management communications. We are involved in them, with a number of other members of UK Finance. There is a cross-market operational working group led by both the Bank and UK Finance, and we participate in that.

Also, the British Standards Institution is in the process of putting together an ISO on operational resilience, and we, together with a number of other people, are providing expertise. I think that is all indicative of how we can work together. Even though the root cause of a cyber-attack is different from what we may see in other forms of incidents, how you assess the impacts and respond and recover offer a lot of learnings that we can leverage across the board. Working together is good.

With regard to the regulator, we have been regulated since 2015, so we are fairly nascent compared with my colleagues to the right. We talk to them almost on a daily basis about a number of topics, of which

operational resilience is one. As you are probably aware, we are under the directives of the PSR and the Bank in respect of implementing the recommendations from the findings of the EY report from last year's incident. While we said publicly that we accepted them and were working through them, that demonstrates the regulators doing their job—the system is working. What they have put in place is a framework that ensures that what we said we would do, we will actually do. It is part of that rigorous and challenging relationship that we have, which shows the system is working.

Q138 **Wes Streeting:** That was very helpful. It sounds like there is broad satisfaction with the interaction during incidents. In terms of proactive interaction with the regulators, have you participated in any regulator-led scenarios or activities to prepare for, anticipate and work through possible scenarios in a proactive way rather than during incidents?

Anne Boden: We regularly take part in internal processes where we rehearse.

Q139 **Wes Streeting:** With regulators? I imagine you all have your own planning.

Anne Boden: Not with regulators, but we have to report to the regulator what happened in those incidents. They will look at our notes from those incidents. There is supervision of what we are doing but not actual involvement, if that makes sense.

Wes Streeting: I guess that must be the same of the rest of you.

Graham Bastin: We are actively working with the PRA for an industry-wide stress test.

Q140 **Wes Streeting:** Okay, so that is something you think ought to happen.

Graham Bastin: No, we are already working with them on that.

Q141 **Chair:** Do you think there should be a stress test? Is there not an industry-wide one at the moment?

Graham Bastin: We are working with them to design and shape that stress test.

Q142 **Chair:** So there is an acceptance that there will be stress test; it is just a question of what it looks like.

Graham Bastin: That has already been shaped out, actually. It is around payments.

Q143 **Wes Streeting:** That is good to know.

Let me turn to the issue of regulatory expectations of operational resilience. We have heard that the volume of regulatory burden on firms to make changes can create operational risk. Is that something you agree with? Our cynicism tends to be that no one likes regulations. I am not sure anyone has ever come in front of us demanding more regulation. I wonder whether that is a characterisation you would agree with. If so, I'd

like you to be specific. We hear too often that the regulatory burden is a risk and creates problems. That can be true, but be specific.

Anne Boden: From Starling's point of view, all change creates risks. You have to put processes in place to manage the release of software in a controlled way. Specifically on regulatory burden, we do not have a significant burden from regulatory changes, because we have new software and new procedures. Like it or not, we work in a highly regulated environment, and we have to do reporting. I think it is part of being prepared to be a bank.

Q144 **Wes Streeting:** Any divergence from that view, or is that a consensus position?

Graham Bastin: I referenced the 25,000 changes earlier. Over half of those are driven by regulation, or are mandatory changes that we need to make to update our resilience or security patches. There is a lot. We have had conversations with the regulators about how we can smooth that out. In the discussion paper, there was been talk about an air traffic control system across the industry, which I think would be welcomed.

Q145 **Wes Streeting:** But you can't think of any examples where regulatory change has driven operational risk either because of the specific regulation or because of unrealistic timelines.

Chair: Or is it just the volume?

Graham Bastin: It's the volume.

Ian Lundberg: There is volume. I think something like secure customer authentication is a massive change that we are having to work through right now, and we are working together with all our clients to see that through. To the point that you made, Ms Boden, there is change associated with making changes of regulations, and that is a particularly large one that we are all working through right now.

Q146 **Wes Streeting:** Should we be worried or concerned that the majority of change is driven by regulators and regulatory requirements, rather than from the industry itself, or is that too simplistic a characterisation of where regulation originates from? Are regulatory demands also being driven as a result of conversations with you guys that leads to regulators working with you to find solutions across industry?

Anne Boden: If I could set the context for how the financial services industry sees regulatory change, large organisations with very complex infrastructures—where I spent most of my career—have a certain appetite for change and a certain amount of change they can do at once on their systems. Because of the level of regulatory change and the complexity of putting that change into legacy systems, there is not much room for new features for customers, or benefit for customers. That is what you hear a lot of. I came to the conclusion in 2014 that it was easier to start from scratch, with a new bank that was easier to maintain. I have a lot of sympathy for the big banks because it is really difficult fixing and

maintaining, and keeping everything up to date. I found it easier to start from scratch.

Q147 **Wes Streeting:** That is interesting. Finally, then, Mr Lundberg, in Visa's written evidence you highlight the importance of consistency in regulatory approaches internationally. Do you have any concerns in this regard in relation to operational resilience, and is there anything you think we can learn internationally from where other countries are doing things particularly well?

Ian Lundberg: A couple of things. One is that I think the UK is leading the way on a number of fronts around things like cyber-security and operational resilience, so I think we are very well placed here in the UK. I think it is important to say that. From our side, it is important that there is no one-size-fits-all to how we think about this globally, but I think to have some minimum standards that we can all adhere to from a resilience perspective would be good, so that we know what the level playing field is.

Wes Streeting: Anything to add on the international front? No? Thank you very much. I am sorry I have to leave. That was interesting.

Q148 **Colin Clark:** You have covered an awful lot of what I was going to ask you about, so I will be as brief as I can. You use outsourcing to provide services to customers, but is it for the bank's advantage, or the customers'?

Anne Boden: We don't use much outsourcing. The banking industry went through a huge amount of outsourcing—offshoring—in the '80s, '90s and 2000s. Technology has dramatically changed, and Starling uses very little outsourcing. The more we can do ourselves, the better. We also believe in hiring software engineers who are employed by Starling and work in Starling, for the benefit of Starling customers. This is much more of a modern way of tackling technology, where we see technology as being so integral to the proposition that we have to do it ourselves.

Q149 **Colin Clark:** Is there a way of measuring it? I come from a constituency where we have got the oil industry, and BP would be able to tell me what percentage of contractors they employ compared to their own. Is there a measurement, if I were to ask you how many are contractors and how many are in-house?

Anne Boden: I have roughly 89 committing engineers, as far as our people are concerned, and I think two or three of them are contractors.

Q150 **Colin Clark:** Which is a very good position. Mr Bastin, in a more established bank is there a percentage for how much is outsourced to third parties?

Graham Bastin: I referenced the technology centre that I run in the north-west, with 5,000 colleagues there. They are 80% permanent Barclays colleagues. That was not the case five years ago. Everything that Ms Boden has just described resonates, certainly with me. That has been a very deliberate strategy that the bank has adopted. Similarly, with outsourced providers we have insourced about 65% of our suppliers. To

answer your question directly, the decision about when we outsource is absolutely driven by the customer. That is the predominant thought.

Q151 **Colin Clark:** That answers the next question, because Megan Butler from the FCA said: "Yet only 66% of large firms, and 59% of smaller firms, tell us that they understand the response and recovery plans of their third parties." They may be speaking about financial services, as opposed to banks. On that, you are actually saying that there has been a reversal from where it was—Ms Boden, you spoke about the 1980s—with banks recognising, and the FCA saying, that third-party ITs are causing an awful lot of incidents, and they are rolling back from that. Is that something we would see across the whole industry?

Anne Boden: Yes, I think so. The '80s and '90s was all about technology being outsourced for cost containment—driving down costs. Technology now enriches our lives and makes financial services better for people. With modern technologies and a different attitude to technology, we are now bringing more things in-house.

Q152 **Colin Clark:** That brings me on to what Committee members will know is one of my pet issues, which I am still trying to get my head around: open banking. You both said you are adopting open banking. Ms Boden, I particularly want to draw you back. You said it is five to six years away. Would you launch it if it wasn't secure?

Anne Boden: I would never launch anything that is not secure.

Q153 **Colin Clark:** That was the answer I definitely hoped you were going to give me. However, isn't open banking an evolution? Isn't it fluid? Will it ever be secure? It is difficult to grasp, because it is five or six years away.

Anne Boden: At the moment, open banking is secure but clunky, and therefore people do not necessarily want to embrace it. Open banking, and delivering safe open banking, is a huge challenge. Starling has been built from the ground up with APIs, open banking and PSD2—the second payment services directive—at its heart. It was relatively easy for us to deliver open banking. It is much harder for the big banks to do that. They have had to spend a huge amount of effort securing their systems and making it easy for their customers to use.

Q154 **Colin Clark:** So it is easier to start from the ground up, as you said earlier?

Anne Boden: Yes, and the fundamentals of what we are trying to do will make things better for customers. However, it is tough. It is easier for Starling. Starling has led the way in all of this, but we started with something very different: we started with a new base. With a new base, you can secure it and make customers much more comfortable with it than other organisations can.

Q155 **Colin Clark:** Mr Bastin, you said something about an industry-wide stress test. Can I draw you towards another idea: pooled audits of common suppliers? I am trying to get at—Ms Boden answered the question very

directly, which was exactly what I wanted to hear—whether you would launch something that wasn't secure. Will there be pressure on the banks because of their competitive nature? Consumers want this open banking—or think they do; it is a bit like faster payments, which we thought was a great idea but has led to more fraud—so will there be pressure on the banks to launch something that is unstable, or fluid?

Graham Bastin: No. We would never consciously launch anything that was unstable. In the case of open banking, we took that very seriously indeed. There was time pressure, going back to the conversations around regulation. There was definitely pressure to hit deadlines on that, but under no circumstances did we cut any corners. In fact, to elaborate further, the easier and quicker way to do account aggregation, for example, would be to do screen scraping, which some firms considered. We never considered that, because it could potentially compromise the integrity and security of the data of our customers. That is a really good example of where the resilience, stability and security of the data—particularly with a service like that—is not compromised.

Q156 **Colin Clark:** Challenger banks are coming in—some of the big tech companies—that do not have banking licences at the moment. They are more familiar with some of this but have had serious issues with the compromising of their IT system. Are you satisfied—you and the regulators right in front of us—that we are not going to come up with something that, because it evolves and is fluid, will be compromised? In terms of competition, you can imagine the situation where the competition comes up with, in the airline industry for example, a jet that goes faster. What will you do to respond to challenger banks coming up with an alternative?

Anne Boden: I think that the industry is constructed in two ways. There are the banks; and, whether they are challengers, or legacy banks or have been around for 300 years, we are all regulated as banks. You then have FinTechs, which do not have banking licences but are regulated within the open banking regime and can consume that data. The banks have responsibility for our customers and we are responsible for compensating our customers if something goes wrong when a customer shares their data with a regulated FinTech. We actually look after our customers.

It has been constructed in a very sensible way. There has been a lot of scaremongering about whether open banking means that customers' data could be compromised, but we have been very careful. That is good for customers; it means that they can get better services, better competition and can take and look after their own data. We must not say that open banking is bad because it is difficult to use at the moment—it will get better.

Q157 **Colin Clark:** Mr Bastin, do you want to add anything?

Graham Bastin: Just on your earlier point about the testing of third parties, whenever we use a third party and that third party might have some of our customer data, we hold them to the same standards. We test them and review their performance, just as with Barclays. That is the way

that we should look at open banking and the standards that apply to any of the third parties that wish to consume some of that important customer data.

Q158 **Colin Clark:** But as you said earlier, you are taking more in-house and are reducing the amount of third parties.

Graham Bastin: The architecture and the technology that Ms Boden described with open APIs is exactly what we are adopting as well. That enables the kind of competition that the industry is looking for.

Colin Clark: Thank you. You have made me feel much happier.

Chair: That is an achievement in itself.

Q159 **Rushanara Ali:** Good morning. I want to talk more about concentration of risk, some of which has been touched on. Earlier on we talked a bit about TSB and the links between TSB's services and other services that people rely on, which, as we touched on, affects other banks. You then have the use of third-party providers and the use of cloud services and so on. My understanding is that there are three major companies that financial services tend to rely on. Can you all talk us through what concentration of risk looks like in the worst-case scenario and what part of it keeps you awake at night?

Graham Bastin: Let me answer the question in different parts. In relation to cloud—I know there is a lot of discussion on concentration risk as it relates to cloud—Barclays are embracing the cloud and our direction of travel is absolutely to leverage that more. When we do that, we need to be thoughtful—we have 24 million customers. We just had the conversation about the importance of data. As we transition from the current architecture to embrace the cloud, we need to do that in a thoughtful and considered way. It is absolutely the direction of travel.

Q160 **Rushanara Ali:** What does that mean exactly?

Graham Bastin: It just means that we have a scale of customers. We have been talking to the regulators about this for many years and we are comfortable and headed in that direction.

Q161 **Rushanara Ali:** You are accountable for your third-party partners—

Graham Bastin: Absolutely.

Q162 **Rushanara Ali:** But do you think that there should be more oversight of what they do? In your doomsday scenario—sorry to be the prophet of doom—you get cyber-attacks and things going wrong internally in a country, with state actors operating in new ways. Do you think we have done enough to mitigate the risks beyond the banking sector, given how reliant now banks are on third-party technology providers, particularly for the cloud, but other services as well?

Graham Bastin: In relation to concentration risk and how that pertains to the cloud, we will go towards the cloud and will use the alternative providers as well. So, there will be alternatives if there is an issue with

that cloud provider. Equally, a large part of our strategy is to ensure that we can bring back those services, if there were some kind of catastrophic failure.

Q163 **Rushanara Ali:** But are they sufficiently regulated? Are they well enough regulated for us to have confidence that it does not have a knock-on effect on your 24 million and others who use the banking system?

Graham Bastin: The way I think about it—others may have a different opinion—is whether the data is held within Barclays or a third party, we are accountable for it. Therefore, we would like to see third parties held to the same standard and regulation.

Q164 **Rushanara Ali:** That is helpful. Ms Boden?

Anne Boden: That is a very interesting question. I think we are talking about the fact that more and more banking and other services are being provided from cloud technologies, which are dominated by AWS, Google and Microsoft. We have three big players providing those services.

Chair: AWS is Amazon.

Anne Boden: Amazon Web Services, yes. That technology is very effective, scalable and resilient and gives organisations the ability to take advantage of the best technologies in the world and grow businesses. So, cloud is very successful. The question is that we have three big technology providers providing services to all of us.

Therefore, what we do in Starling is ensure that, although our principal provider is AWS, we also have fallback services with Google. It is an important point that the vast majority of organisations now are becoming more and more dependent on these big tech companies. For us and our consumers it is very successful, but we need to put the processes in place in all organisations to ensure that we do not have single-company dependence.

Q165 **Rushanara Ali:** Mr Lundberg.

Ian Lundberg: From our perspective, we are not a bank like Starling or Barclays here. From a VisaNet perspective, the processing is all done through our datacentre in the UK. We do not use the cloud for the purpose of that processing. Our only use of the cloud is for some of our internal corporate processes, such as procurement or expenses, things like that. From that perspective, we do not have the same considerations as my colleagues.

Q166 **Rushanara Ali:** Just to come back to it, I did not get an answer to what keeps you awake at night, in relation to any one of those scenarios, particularly an outage—if you suffered an outage linked to cloud service providers, or anything else for that matter. Do you want to come back to it? I hear what you are saying about the opportunities, from which we have all benefited.

These are three big companies. Are they too big to fail, just like the

banking sector was? What are the risks to society if things go wrong, even if there is a small chance of things going wrong, where you have a concentration of risks and so on?

The recent Australian example is not directly related but is about something going wrong in the telecoms sector having a knock-on effect on transactions in shops. The banking sector is an example, even if it is for a day, of very serious consequences for millions of people. Could you talk us through how you are mitigating those sorts of risks and how you are working through that?

Anne Boden: AWS, Amazon Web Services, provides a hugely resilient structure, operating in multiple data centres over multiple regions. In totality, no bank could provide the sort of resilience that AWS provides us. What I think you are referring to is, if something happened, a political issue or some sort of regulatory issue that said that the bank could not rely on AWS or Amazon in some shape or form—

Q167 **Rushanara Ali:** I am not referring to that. I am thinking more of Facebook; it is the other end of the spectrum, but 10 or even five years ago, people were evangelical—we all to some extent probably evangelise technology—and did not necessarily see the downsides, and there have been major data breaches. I recognise that AWS and other have better systems and so on, but you cannot completely disregard a possible scenario where there may be risks to do with data being compromised. That is what I am interested in, not necessarily what the Government might do. There may be other scenarios, but that is particularly what we are thinking about.

Anne Boden: That is why it is important to ensure that you do not have dependence on one company and that your data is safely secured in another environment. We have a process whereby, on a daily basis, we move our data and then constantly update it, so that we can ensure that our data is in an alternative environment and an alternative region at all times.

Q168 **Rushanara Ali:** Mr Bastin?

Graham Bastin: I agree with what Ms Boden says. It is important that we do not have a dependence on any one provider, whether that is a cloud or any third party, and that there is always an alternative. As I tried to explain a moment ago, the heart of our plan B is that we own the data, whether it is with a third party or not; the accountability rests with us and that is really clear. Holding those third parties to the same standard is what we will do anyway, and regulation could help that.

Q169 **Rushanara Ali:** Is there a specific area or source of concentration that you think needs particular attention from regulators?

Graham Bastin: The way that we think about resilience, as I described earlier, is about the most critical customer journeys. We would not think about the cloud or a third party as just some kind of independent thing, "That's where the data is." I would think about it in the context of what it is that our customers are trying to perform and ensuring that that has the

highest level of scrutiny, standards, resilience and controls wrapped around it. On your question of what keeps me awake at night, if there was some kind of issue, it would be knowing that we have an alternative or that we can bring that service back in-house if we needed to, to continue to service our customers.

Q170 **Rushanara Ali:** How realistic would that be, to try to bring something in-house?

Graham Bastin: I said before that we need to be thoughtful and considerate about how we approach the cloud; that is part of the consideration that we would need to give.

Q171 **Rushanara Ali:** My Lundberg, did you want to add anything on that? Otherwise, I have a couple more questions.

Ian Lundberg: No; as I referenced before, we do not use the cloud from a network processing perspective. From a technology capability perspective, that is all done in-house for us and there are no third-party providers.

Q172 **Rushanara Ali:** Is there anything that keeps you awake at night, then—regardless of the cloud?

Ian Lundberg: I think cyber-security is No. 1.

Q173 **Rushanara Ali:** Can you elaborate on that? What part of cyber-security keeps you awake at night?

Ian Lundberg: The fact that you have bad actors, nation states and organised crime out there constantly looking to try to access networks and the data that those networks have.

Q174 **Rushanara Ali:** Would a sector map help in the management of concentration of risks?

Ian Lundberg: A sector map is understanding the ecosystem as a whole and all the various interdependencies within that. To a certain extent, we have that at Visa, understanding the issuers and acquirers that we have, particularly in how we respond to incidents and crises, we have to leverage that and all the information we have to share information with them. To a certain extent, we have something like that in place today.

Rushanara Ali: Does anyone else want to come in on that?

Anne Boden: The question is really about whether there is a piece of infrastructure that we are all using that every single customer transaction would have to go through. What really matters to people is whether they can buy their shopping, make their rent payment or whatever. If both those types of transactions went through the same infrastructure and there was any possibility of its being down at any point in time, we would have to look very carefully at it. That is the sort of thinking that needs to dominate looking at operational resilience. We need to really see what people are trying to use our services for.

Rushanara Ali: Do you have anything to add, Mr Bastin?

Graham Bastin: I don't have anything to add.

Rushanara Ali: I am going to try to put all the questions together, if that's okay. In terms of substitutability, how realistic is it, given the complexity of the bigger institutions in particular—Chair, I'm sorry, I have two questions.

Chair: Just ask the one about substitutability—the ability of providers to step in on behalf of others. Is that what you want to ask about?

Q175 **Rushanara Ali:** Yes, particularly to Ms Boden; you mentioned artificial intelligence. I wondered if any of you had anything to add about the downsides of AI, given that there have been lots of reports about profiling and things going wrong when decisions are made, whether in banking or elsewhere. How much work do you do to look at the differential effects and some of the downsides and risks of AI in getting that wrong?

Anne Boden: I think AI can give us a huge amount of benefit in society, but it can perpetuate prejudice and can, in some cases, perpetuate the situation regarding the financial systems of certain people in one way and that of other people in a very different way. We need to get the models right. They need to be fair and we need to be doing it with our eyes open.

Graham Bastin: On the topic of alternatives, when Mr Baker was here, we talked about testing of third parties and suppliers. We try to go further than that and actually move the production workloads to alternatives, and make sure that the business can still continue to operate with those substitutes. There is more to do and maturity to add, but that is the direction of travel.

Q176 **Rushanara Ali:** Anything on AI to add?

Graham Bastin: I agree with everything Ms Boden said. We use AI in different areas as well. We talked about the role that change plays in driving instability. AI can play an important part in terms of trying to identify where changes may have impacts somewhere in the ecosystem that a human wouldn't perceive. There are some great opportunities, but there are some considerations as well.

Q177 **Rushanara Ali:** I was interested in the safeguards, particularly in relation to gender-based bias, discrimination and race bias. Do you have any safeguards in place?

Graham Bastin: Nothing more to add.

Rushanara Ali: So you don't have any safeguards in place?

Graham Bastin: I don't have anything more to add to what Ms Boden described.

Rushanara Ali: So you don't have any safeguards about using AI to assess whether there is gender-based bias and racial bias in the way AI is being used in banking and in your bank?

Graham Bastin: I don't—

Q178 **Rushanara Ali:** Can you check that and come back to us?

Graham Bastin: Of course.

Rushanara Ali: I would like to know from other banks, Chair, if that is the case, because I think it is important.

Chair: That's outside the terms of this inquiry, but we will write. If that is something Ms Ali wants to proceed with, then obviously we can take that up separately with banks. I don't think it is part of this inquiry, unless there is a particular link to operational resilience. Is there? No. Simon.

Mr Simon Clarke: Last but not least.

Chair: No, we've got one more. Charlie still has to go.

Q179 **Mr Simon Clarke:** Good old Charlie is sitting there. In that case, it's second last but not least.

Charlie Elphicke: Tail-end Charlie.

Q180 **Mr Simon Clarke:** Tail-end Charlie, in so many ways. Moving on—enough of this banter. I was struck, Ms Boden and Mr Bastin, about what you were saying about the fact that, in essence, every day you have a huge number of upgrades that go on seamlessly and in a measured, incremental way, to avoid outages. Before I get started on my questions, I wanted to understand why last year TSB, which obviously had such a disastrous introduction of new technology, experienced what they went through and what their customers were exposed to. Obviously, it would suggest that their procedures were wholly at variance with yours. Is that a fair summary? Were they just doing something very differently?

Anne Boden: I can't speak for TSB. The TSB—

Q181 **Mr Simon Clarke:** It would suggest, though, that the changes can't have been gradual and incremental, and capable of being reversed speedily in the event of problems.

Anne Boden: There are experts on the issues for TSB. What we saw was the impact on their customers. During that period a number of customers came to us, and it takes a while to reassure customers afterwards that everything is safe again. The industry as a whole took a knock as a result of TSB, and it will take a while for the whole industry to recover.

Q182 **Mr Simon Clarke:** Yes. Does that suggest that we may have got an unusual panel? Are Barclays and Starling much more sophisticated in the way in which—what I'm trying to get at is this: with regard to when we issue our report on this issue, are we in essence being misled by outliers, or are TSB the outlier?

Anne Boden: TSB were doing a migration from one set of systems to another. Migrations of systems are very, very difficult to achieve. It's a huge amount of change over a weekend or a couple of weeks, and that is

risky. In Starling, we are not doing a migration. What we are doing is every day making things better for customers, adding on features as we grow our customers—

Q183 **Mr Simon Clarke:** But are you confident that you are a more accurate representative of the sector than TSB in that regard? I am trying to get to the fundamental balance of risk for consumers at the moment. Are you confident that the banking sector as a whole—

Anne Boden: We're a new bank. The reason why I started Starling and got a team of people together to build this sort of organisation was that I felt that new technology, a new banking licence and a new way of going about things would lead to better customer outcomes. I thought that this way of doing things was better. Building technology—taking the best technology from around the world and using our own engineers to build it—was better than buying a banking package and migrating data on to that banking package. This is what Starling has chosen to do, and at the moment it's working out.

Mr Simon Clarke: Indeed, and long may it continue to.

Anne Boden: Thank you.

Q184 **Mr Simon Clarke:** On the point about technological investment, PwC, in written evidence to us, have suggested that one unfortunate legacy of the 2008 financial crisis has been that, at a time of squeezed profit margins, there has been a lack of investment in technological upgrades. Would you describe that, Mr Bastin, as a fair reflection of your experience so far?

Graham Bastin: No. I referenced, in my opening remarks, the fact that we have spent about £1 billion over the last three years on resilience in its various guises. We have talked about cyber and technology and third parties, and it represents all those areas. If I think about the bank that I joined 12 or 13 years ago, there was a need for investment. There was ageing infrastructure, which Ms Boden has talked about. There were elements of legacy. A serious investment was made over a number of years to address that. There are always challenges on budgets, of course, but I have not seen that budget shape change, in terms of resilience, for Barclays.

Q185 **Mr Simon Clarke:** Would you agree, Mr Lundberg, for Visa?

Ian Lundberg: From our perspective, we are a global technology payments company, so we are continually investing significant amounts of money across a number of areas, be it cyber-security, data centres, hardware or the network itself, to ensure that we are as state-of-the-art as we possibly can be to deliver the security and reliability that our customers are looking for.

On the point that Ms Boden made on migrations, we did undergo last year a significant migration. As I referenced earlier, we moved from the European authorisation platform to the global platform, which is pretty much the largest migration, I think, that has ever been undertaken in the

industry. We delivered that over 67 nights. It had no relation to the incident that we had. We took a very thoughtful, methodical approach to the change management associated with that.

Q186 **Mr Simon Clarke:** In terms of the practicalities of doing this, Ms Boden, you obviously bring a background—I was looking at your CV—in computer science. Is there a problem with finding sufficiently trained staff for this, and, in particular, looking at the next generation, is our education system currently providing the stream of future talent that is required, given the increasing centrality of this whole issue?

Anne Boden: Tech is now fashionable. We went through a whole period when tech was not fashionable, or it was seen as a back-office function in many of these institutions. If you are coming out of university, you become an investment banker, and then we had the crisis. Now we have people going in and wanting a career in tech, so it is very fashionable. We are able to hire some great people into interesting roles. We have an advantage in Starling Bank; it is a different sort of environment and is very engineering-focused. It is run by people who love technology and love talking to customers, so we can attract the best, but we need more of them. We need more people doing computer science degrees and more people seeing this as an attractive industry to work in. It has to be far more diverse as well. There are very few women in tech, and we need far more.

Q187 **Mr Simon Clarke:** Indeed. That is a wider challenge. Would both of you gentlemen echo that—that the talent pipeline is still under pressure?

Graham Bastin: Absolutely. The software development and the engineers that we are talking about are highly sought after globally. We work a lot with Manchester, Salford and Liverpool Universities, as well as the schools and colleges, to try and inspire people into this industry. I think Ms Boden is absolutely right. That is the opportunity to address the diversity challenge. At the senior levels, it is a little bit more of a challenge.

Q188 **Mr Simon Clarke:** Presumably that is a generational thing.

Graham Bastin: Absolutely.

Q189 **Mr Simon Clarke:** At the other end of the spectrum, there is a need to make sure that there are the right incentives at the very top of organisations in order to ensure that this really is front and centre. I appreciate that at one level, the risks of failing to act to mitigate problems are obvious. In your organisations, is there any link between remuneration and system reliability? Is that a part of anyone's contract?

Graham Bastin: In Barclays, since the senior management regime came in, it has sharpened the focus. We have the governance structures that I referred to earlier, with a very clear SMF24 kind of structure where it is very clear where the accountability for operational technology resilience lies. The performance is absolutely reflected in my compensation, my team's compensation and up through the lines. It is very clear that it remains a priority for Barclays Bank.

Q190 **Mr Simon Clarke:** That is interesting. Is that common practice, Ms Boden and Mr Lundberg?

Anne Boden: Starling's not a bonus environment. Starling is all about really, really connecting with customers and building our business by making people's financial health better. If we are not available, people will not use our service. We are all highly aware of what our customers feel, so it is not an incentive programme. That's not how Starling works. People who have joined Starling have joined in order to change the financial sector, and providing valuable and highly available services is a part of that.

Mr Simon Clarke: Thank you. Nicky, is Charlie dealing with industry co-ordination or am I?

Chair: You are doing it.

Q191 **Mr Simon Clarke:** I am still doing it. Okay. I didn't want to tread on anyone's toes. Colin talked about the aftermath of incidents, although we all hope that there are not such incidents. In so far as there are lessons that need to be learned on a sectoral basis—obviously, some issues might not be discrete to an individual business; they might well be replicated in others—are there barriers that exist to sharing those lessons? In practice, notwithstanding whether those barriers exist, are there effective mechanisms for ensuring that wider lessons are fed back in, Mr Bastin?

Graham Bastin: I said earlier that I see the highest level of collaboration in cyber. Absolutely there are bodies, intelligence sharing and physical co-location of different entities where that knowledge sharing happens in real time.

Q192 **Mr Simon Clarke:** Real time? Almost as it happens?

Graham Bastin: Absolutely. We second people into some of those agencies—GCHQ, and the Government and so on—as do other entities. They sit in a command centre, and collectively see some of these issues arising and share that intelligence without any boundaries or barriers. I think that there are things that we can learn from that.

Q193 **Mr Simon Clarke:** Absolutely. Mr Lundberg, in Visa's correspondence with the Committee following the 1 June 2018 incident, you explained that you entered into discussion with other organisations in order to improve the wider resilience of the financial sector following that incident. Were there specific findings from those discussions?

Ian Lundberg: There were a couple. We proactively commissioned EY to do an independent third-party review. Five findings and recommendations came through that, and we are implementing—

Q194 **Mr Simon Clarke:** Were they specific to Visa, or were they more wide-ranging?

Ian Lundberg: Five of them were specific to Visa. There was an observation around Visa's part in the ecosystem, and how we could look at our role in that ecosystem and work with other parties. That is something

that we are actively doing. An example is the work with UK Finance that I referenced before, which a number of us participate in. There is the bringing together of communication specialists from each of our largest clients, so that we can continually share information, particularly in the case of there being an incident.

On 12 March this year, we held the first joint crisis simulation with our largest UK issuers and acquirers. All they knew is that they had to be available between the hours of 10 am and 3 pm that day. They were not given any heads up regarding what the simulation was about. Internally, very few people knew what scenario we were using. We ran it really to pressure-test a lot of the processes and procedures that we put in place as a result of implementing the recommendations coming out of the EY review. I led that effort. I think it was very well received. From our perspective, the more that we can do those kinds of joint crisis simulation exercises, the better; it benefits us all. It benefits the ecosystem and, very importantly, it helps to build that muscle memory, so that in the event of an issue, we can all respond and react as quickly as possible.

Q195 **Mr Simon Clarke:** I think most people watching this would find that really encouraging. Your colleague Charlotte Hogg, who is the CEO of Visa Europe, was cited as arguing that the entire payment system can be made more resilient if there is, as Rushanara referred to, substitute ability between different firms in the event of an outage. Is that something where there are any plans in place?

Ian Lundberg: I think—

Q196 **Mr Simon Clarke:** I see that Anne is waiting to leap in.

Ian Lundberg: I think that Mr Bastin referenced something like this. We do have the capability. If there is an issue with one of our issuers, we have the ability to stand in and process transactions on their behalf. That is one very good example of where there is that kind of interoperability; we can perform and process transactions on behalf of an issuer, should they be having an issue.

Q197 **Mr Simon Clarke:** That is great. Ms Boden?

Anne Boden: With many of the things that we are doing in the new banks in the new tech sector, the technologies are used not just in banking but in other industries as well. There are lots of learnings that you can get from those other industries. Other industries tend to be far more open, because it is much more likely to be less subject to fraud or whatever. You get a lot of learnings from attending conferences and talking to people using similar technologies in other organisations. That is quite important.

Mr Simon Clarke: Long may that continue. I am surprised, actually, by the extent to which these things are not considered proprietary, so that is great.

Q198 **Charlie Elphicke:** Good morning. Graham, what is the biggest issue with legacy systems? Is it their existence or the fact that you have to upgrade them?

Graham Bastin: Legacy, as I referenced earlier, was probably an issue that worried me more maybe 10 years ago or so. There was definitely a challenge there—not that those systems added to the fragility of resilience per se, but because of the need to change those. We have gone down that journey. We have made the investments, and we have upgraded. In fact, the direction of travel, as we have been discussing, is one where we have built our own internal cloud and we are now looking towards the public cloud. Really, the thing that worries me more are the topics that we discussed earlier around change management and so on, and less about legacy.

Q199 **Charlie Elphicke:** So when you are deciding on upgrading systems, how much do you take into account the risk that, during the upgrade, the whole thing will just pack up and the bank will not be able to do anything at all?

Graham Bastin: The way we approach the body of work I just described is to look at the most critical customer journeys we have—the most critical customer services—and make the upgrades to those. They are all running on modern technologies. On what you might think of as legacy, some people talk about mainframe as an example of that. We are actually operating with one of the most modern mainframes, in an architecture that gives us what we call active-active, which means if there is a failure in one of those platforms, it can be run from an alternative. When we think about those upgrades, it tends to be the smaller changes we make at the front end of the application rather than larger changes to some of what you might think of as the legacy.

Q200 **Charlie Elphicke:** One thing that UK Finance says to us is that a lot of these problems are caused by vast amounts of change by vast amounts of different organisations. You might have the Information Commissioner, the FCA and some other regulator turn up, but they do not co-ordinate; they do not talk to one another. People think of the Government as a single entity, but in fact it is loads of different entities, all of which want to poke their nose in. My impression is that it is a bit like the utilities companies that come along and dig the street up. The way the regulators all seem to work is that they all dig the street up at the same time, without any organisation whatsoever, and cause chaos in the road. Is that fair?

Graham Bastin: I think the discussion papers stimulated a conversation around something called air traffic control. If we could see greater coalition and co-ordination across the different regulators, not just in the UK but internationally, that would be super-helpful to an organisation like us. That said, we push back on some of those things. When we are executing the volume of change that I referenced earlier and we can see there are collisions or compression on that change schedule, we are very happy to push back on where those changes are coming from and to explain the consequences, or the unintended consequences, of trying to drive that much change through the system.

Q201 **Charlie Elphicke:** Ian, how do you find all these issues?

Ian Lundberg: We are regulated by the Bank of England and the PSR. Obviously, they have different remits: one is around financial stability; the other is around consumers, competition and innovation. What we find is that those two complement each other. We work well with them. We do not find there are particular challenges right now in terms of the volume of stuff that comes through them, but we work closely with them and obviously try to leverage doing things once wherever we can.

Q202 **Charlie Elphicke:** Graham, you are not exactly short of inspectors at the door, are you? Do you think some of the regulatory changes that are demanded by random regulators are just, frankly, a complete waste of time and are done to justify their existence rather than for any real purpose?

Graham Bastin: The regulators are pushing on the same topics. To the question, "What keeps you awake at night?", it is the same three or four things for me. It is cyber, third party and technology change. The regulators come at those three topics from a very similar perspective, and it would not seem too much of a stretch to me to get greater co-ordination around driving their agendas on those topics in a unified way.

Q203 **Charlie Elphicke:** Do you think we ought to aggregate regulators into a super-regulator, or do you think it is just better that they actually try to talk to one another and have some sort of formal system?

Graham Bastin: I think you could solve what we are talking about with greater discussion and talking. I do not know that we necessarily need to restructure. You are probably better positioned to know that than me.

Q204 **Charlie Elphicke:** You had your own little outage in September 2018. That was caused by an issue with technological software changes, which presumably is otherwise known as an upgrade. What happened?

Graham Bastin: It wasn't an upgrade. In that particular case, it was actually a regulatory-driven change.

Q205 **Charlie Elphicke:** There you go—my point exactly.

Graham Bastin: The change itself was conducted overnight and tested, and appeared to work. Only as the day progressed did we start to see some customer impact. That change was subsequently backed out, and we went on from there.

Q206 **Charlie Elphicke:** You wrote to the Committee saying that you followed all your protocols and controls, and there is no problem with it whatsoever. Were the protocols and controls at the time insufficient? What are the key learnings from that experience?

Graham Bastin: Whenever we have any incident—whether major, like the one you described, or smaller ones—there is a process in place, whereby we do a full root cause analysis and the lessons learned are embedded. There were a number of issues with that particular case, but the main one would be what we call live proving. The change itself had been tested thoroughly, but when it went into the live production

environment, we should have tested it for a little bit longer with customers, so that we might have been able to see this issue and back it out. That process had never been embedded within the firm. We now do that increasingly across all platforms.

Q207 **Charlie Elphicke:** Great. Anne, you are sitting pretty. You have no problems with any legacy systems—you have not been going long enough—so that is a great position to be in. Does this provide you with an opportunity to create a more resilient platform for your customers, or are you just lucky, and in 10 years' time you will just catch the same cold as everyone else?

Anne Boden: As organisations get bigger, they might have more acquisitions, mergers and products, so you inevitably get a legacy. However, in Starling, we have architected our systems in a way to make them more resilient to failure.

In modern technology, instead of having one big system, which is either on or off and works or doesn't work, we have 20 or 30 different components looking after a part of the customer experience. These mini-systems communicate with one another. If one of them fails, while it repairs itself, all the other components continue, and when it pops back into action, it catches up.

That means that instead of the app totally disappearing and being unusable, or a service disappearing, just one page or a part of the function might disappear. We design our systems in that way so that they are easier to recover and update. When we roll out more software, we will be able to release something to only 20% of customers. If that is working fine, we can release it to 30% and then 40%.

That is a whole new way of developing and delivering systems, which other industries have used. I have been in this industry a long time. I was a software engineer. I have gone through all the various phases of offshoring and outsourcing and replacing big mainframes. Now we are in a situation where we can bring in the best technology in the world to banking. Yes, it will be legacy one day, but it is part of the constant renewal, which you must do to ensure that technology and banking are fit for purpose.

Charlie Elphicke: Thank you.

Q208 **Chair:** I have one final question, which is directed to Mr Bastin and Ms Boden. Both of you have said that your customers are the important people at the heart of all this. You have also seen operational resilience shooting up the agenda, in the same way as prudential risk and capital risk, as well. In the same way that customers often have a number of different bank accounts, particularly in relation to savings, so that they are caught by the financial services compensation scheme and benefit from those protections, would you recommend that customers should perhaps have accounts with different banking providers, so that if one goes down, they are still able to do much of their banking with somebody

else? Is that something that you have thought about? Ms Boden, you are nodding.

Anne Boden: I think it is a very interesting debate. Lots of customers think that they are only allowed one current account, but that is not the world we live in. We can now offer people lots of different services, and different banks can provide different parts of those services. In the UK, we all use Visa or Mastercard, but are they really very reliable? I do not recommend that people carry a Visa and a Mastercard, but I do recommend that people try to find the right bank account for them and try us out. Try a bank account—if it works for you, then you can switch. It is worth trying.

Q209 **Chair:** Mr Bastin, what is the Barclays view?

Graham Bastin: The same, really. Everything we have done is around what the customer is trying to get out of life. Increasingly, it has become less about the financial transaction itself and more about the broader experience. When you buy a house or a car or get married, there is something important going on in your life, and we want to be central to that as we go forward.

Chair: And to be ultra-reliable, presumably.

Graham Bastin: And to be ultra-reliable.

Chair: Lovely. Thank you very much indeed; I know that preparing for a Select Committee session takes time. We are all very grateful for your evidence this morning.