HOUSE OF LORDS

Financial Services Regulation Committee

Corrected oral evidence: The FCA and PRA's secondary competitiveness and growth objective

Wednesday 6 November 2024

11.35 am

Watch the meeting

Members present: Lord Forsyth of Drumlean (The Chair); Baroness Bowles of Berkhamsted; Baroness Donaghy; Lord Eatwell; Lord Grabiner; Lord Hill of Oareford; Lord Kestenbaum; Lord Lilley; Baroness Noakes; Lord Sharkey; Lord Vaux of Harrowden.

Evidence Session No. 15 Heard in Public Questions 208 - 213

Witnesses

I: Soups Ranjan, Co-Founder and Chief Executive Officer, Sardine; Simon Taylor, Head of Strategy and Content, Sardine.

USE OF THE TRANSCRIPT

1. This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witnesses

Soups Ranjan and Simon Taylor.

Q208 **The Chair:** Mr Ranjan and Mr Taylor, you very kindly were here for the earlier session. You realise why we have gone on a little longer than we intended. You heard what I had to say about the transcript and everything else, so we will go ahead with the session now. Did either of you want to make any kind of opening statement?

Soups Ranjan: Yes, sure.

The Chair: Go on, then.

Soups Ranjan: I am very grateful for the opportunity to present in front of this committee, and I look forward to the discussion. I am the co-founder and CEO of Sardine. We are a venture-backed start-up based out of the US. I am personally based out of San Francisco, California. Today we work with about 250-plus financial institutions globally, including banks, payment processors and fintech start-ups. I am here to represent my views as well as the views I have heard from our customers, who span the globe. I am really grateful for this opportunity.

Simon Taylor: I echo Soups' comments. The only thing I would add is that I was head of crypto R&D at Barclays. I also spent some time helping set up its start-up outreach programme Barclays Rise and Techstars. I have worked in a large financial institution. I was also founder of a company called 11:FS that worked very early on in the fintech ecosystem in the United Kingdom. I have been involved on the media side on that as well. I possibly offer a more UK-centric perspective and one that is potentially closer to how some of the start-ups think and feel here on the ground. I am based in London.

Q209 **The Chair:** Perhaps I could get on with the first question. Some fintech firms have been criticised recently for failing to protect consumers, and in particular victims of authorised push payment fraud, which relies on social manipulation. We understand that one of the services is to offer software that monitors transactions, identifies instances of fraud and intercepts these. What costs are associated with prevention in addition to compensation? Can you share any data on which types of firms are hardest hit by APP fraud?

Soups Ranjan: Sure. APP scams affect everyone pretty much across the board, including large banks as well as fintech start-ups. One of the differences, though, between the large banks and the fintech new banks is that consumers use the large banks as their primary bank account, whereas the fintech new banks are normally the secondary bank account. That means that fintechs, to begin with, have access to a much smaller amount of data in order to detect potential scams and fraud attacks. With a larger bank, if you get your pay cheque in and you know that a consumer has certain types of counterparties that they interact with, you can presumably make a more educated decision when somebody is paying a counterparty as to whether that is fraudulent or not, just on the

basis of past association and history, whereas fintechs are missing that data.

That brings me to the main point, which is that in order to detect fraud we need to enable information sharing across large banks as well as fintechs, because at the end of the day fraud detection should not be thought of as a competitive mode; it should be thought of as a utility that essentially helps consumers and smaller start-ups to become more competitive in detecting APP scams or fraud.

I would also like to point out that, in the current reimbursement regime proposed by the PSR, certain issues have not yet been addressed that also make APP scams harder to detect because the regulation has taken a stance towards reimbursement instead of prevention of scams. That means that a few things have not yet been taken into account that are going to affect both banks and fintechs.

Today, the liability is shared 50:50 between the sending bank and the receiving bank. It could be argued that, if the sending bank has done its share of the prevention work, it should not be held liable. In the current regime of sharing 50:50, the receiving bank may not pay as much attention to the prevention. Secondly, because liability is being shared 50:50, once the money has left the sending bank, the receiving bank, because it is also being held liable, will hold on to the funds for far longer. It will hold on to the funds for up to three days, which has been prescribed, which means that faster payment systems could come to a halt or slow down immensely.

The second point is that the reimbursement model also defines gross negligence in a confusing way right now, because it is unclear whether a payment service provider may ever win a gross negligence case. If a consumer has been given enough warnings that they are being scammed and they still go on with that payment, I would argue on behalf of the industry that the sending bank in this case should not be held liable because they have done enough.

The third point is that the liability period is 13 months right now, which means that the sending banks as well as the receiving banks have to hold in their capital reserves all the Atoa, or faster payment, or CHAPS transfers for up to a 30-minute period because all of that could be clawed back. In contrast to the rest of the world, that period is very long. If you contrast it with the US system for ACH, the liability window is 60 days for retail and three days for commercial transactions.

The Chair: ACH?

Soups Ranjan: ACH, yes.

Simon Taylor: It would be like BACS.

Soups Ranjan: Secondly, for card payments, the liability window is six months. Therefore, I would argue that 13 months makes it less competitive.

The Chair: Lord Vaux, this is your specialist subject.

Q210 **Lord Vaux of Harrowden:** The reason for the reimbursement regime is to try to create an incentive for the banks to prevent fraud. That is why it is there. It is not an either/or. It is designed to try to encourage the banks to take the steps to make sure the fraud does not happen in the first place. The reason it is targeted at the banks is that all fraud ultimately has to go through the banking system one way or the other, so that is the touchpoint that every fraud has.

That said, I absolutely agree with your point. I have always felt that the receiving bank should perhaps be more the target than the sending bank if the sending bank has taken appropriate steps to identify. I get that point.

But the fraud environment is much wider than that and there is a whole chain from where the fraud begins to where the money finally ends up and gets cashed out. Do you think we have the incentives right for the rest of the fraud chain? If not, how could you do it to make sure they do their bit to prevent the fraud arising in the first place?

Soups Ranjan: To your point, the reimbursement scheme is great because it protects consumers. However, one of the biggest things that is missing right now is co-ordination between the financial services sector and other sectors, referred to as the polluting sector, which are social media companies and telcos. The vast majority of those scams, based on our conversations with our customers and other parties, originate from either social media forums or a phishing attack that started from a text message or a voice call.

Singapore has created an ecosystem where banks, telcos and social media companies can share information together. First, before you initiate an SMS message in Singapore, you have to be registered with a caller ID. Secondly, only registered aggregators are allowed to originate SMS messages. Thirdly, telcos have to take measures to call out scams that are being perpetrated via their networks. Those things are still missing in the UK.

Simon Taylor: There is a bit of a gap, if I may add, between the UK Government's fraud campaign, the Online Safety Act and some of the work that came out of the Online Safety Act and DSIT, and the work of Ofcom and of course the PSR liability scheme. All these things cut across fraud and scams in some way, but it is particularly disjointed, and there is an opportunity there to think about how that impacts larger and smaller firms. That is point No. 1.

Point No. 2 is that data sharing, as Soups raised, is very much a devil-is-in-the-detail issue. Lots of initiatives to share data are available. Open banking has an optional standard called TRI, the transaction risk indicator, that could, if used, send any risk related to a payment through an existing regulated channel. However, it is optional, so most of the banks choose not to use it because it might be additional work and additional expense. So there is that channel.

There is an initiative by Pay.UK for enhanced fraud data. But we see that there is a need for real momentum. A lot of that data-sharing conversation is driven by those who can afford to put people in the room to have the conversation—the larger institutions—and is poorly represented by smaller organisations, despite the good work of some trade bodies in attempting to level that out.

On data sharing, there are pieces we can deal with in financial services, but a lot of what is coming out of the online platforms is, "You give us your data and we'll tell you if we think it's a scam", rather than "We will share data on a more equitable basis". The opportunity for good co-ordination there is vast.

Lord Vaux of Harrowden: The data thing is interesting. The excuse that is usually used is, "We can't provide this sort of data because of GDPR". Do you have any views on that?

Soups Ranjan: Absolutely. There is definitely existing technology to allow for data sharing in a privacy-preserving way. That is my first point.

Secondly, we at Sardine have built the entire company on the model of data sharing. We have a consortium machine learning model that right now comprises 2 billion devices and 160 million customer identities tied to those devices, and that benefits everyone. We strongly think that in this case, if we were to bring the big tech companies such as Google and Meta into a data-sharing agreement, there are several things that can be done where even PII data does not need to be gathered.

I would like to share a common tactic that fraudsters use today. Oftentimes, before a scam starts, a scammer will chat with hundreds of victims. I am sure all of you probably get text messages that are not really meant for you. Do you think the scammers are typing those messages themselves? They are not. More often than not, they have jerry-rigged a device farm. I have videos where the devices are lying flat on the table, and they use software to make the chat conversation on Instagram or other forums.

Let us say I receive a text message. If only I could know that that text message came from a bot that was not typing directly—it was typing but the phone was face down—which in itself is not a PII signal, and that alone could provide everyone in the ecosystem enough evidence saying, "Hey, Soups, you're chatting with a potential scammer and, therefore, please be forewarned that any other subsequent activity you undertake that could be financial in nature is a scam".

Lord Vaux of Harrowden: Is there anything the ICO should be doing to clarify the data rules?

Simon Taylor: It would be helpful, I suspect. I have no specific immediate examples that I could give. My experience of the culture of financial services, having worked with and consulted to them, is that everything is hard if it involves data because it is, but that does not mean

we should not do it. Of course, we have lots of precedent for sharing data when it comes to anti-money laundering and dealing with fraud: CIFAS, National SIRA, and the National Hunter database. Many such examples are live and in production and shared with law enforcement on a regular basis. This is absolutely achievable. It has been helpful, in my experience, to not only create that clarity at the regulatory level but to engage in participatory round tables and discussions where that clarity is built on in conversation with the industry. That would be particularly helpful. Whether that is a "Dear CEO" letter or whatever else it needs to be is for smarter people than me to decide.

Q211 **Lord Grabiner:** I have one question, if I may. You are both experienced in digital assets. Is that right? The point I am interested in is the volatility in particular of the bitcoin market. Overnight, with the American election results, the price has gone to $75,000 or something. I just had a quick look on the phone and that is what it said. That volatility is potentially extremely damaging to consumers, most of whom or a very large number of whom are attracted by the prospect of an immediate profit, but based on complete ignorance. At the moment, as I understand it, none of this is regulated. What do you think about that?

Soups Ranjan: I am happy to take a first shot at it. I agree with you that the volatility could hurt customers as well. One method of regulating crypto could be to think of it as any asset that has a lot of volatility. You could think of regulating it like gambling.

Lord Grabiner: That is exactly what it is.

Soups Ranjan: Yes, that is right. When I speak with my friends who are interested in crypto, the advice I give them is, "Only invest the money that you're not afraid to lose completely". In that regard, it is very much like gambling. Right now, the fact that it has not been—

Lord Grabiner: Your friends have access to you, but what about somebody who does not know you and is very attracted by the headline in the morning newspaper?

Soups Ranjan: Yes, that is an issue.

Lord Grabiner: Should they not be protected by regulators or by regulatory structure?

Soups Ranjan: I agree with you 100%: they should be protected by regulation.

Lord Grabiner: Why are they not? Do you know?

Soups Ranjan: In different countries, regulation often lags behind technology. That is what has happened. Regulators are still not able to comprehend in lots of jurisdictions outside the US whether crypto is a security or a utility or something else.

Simon Taylor: If I may, Soups, the FCA has done a commendable job clarifying the nature of what a crypto asset is for the benefit of the UK population. There has been good work clarifying the online promotions section of the FCA handbook. There is now a register of crypto asset firms held at the FCA. It is rather unfortunate that the crypto industry is also very correlated with the scamming industry. It has a very negative reputation.

As somebody who has worked in financial services and payments change for a very long time, I remain a massive fan of the technology. Digital assets, when properly regulated, packaged and disclosed, and not sold as a speculative asset but, rather, used for payments and used by regulated institutions, could be transformative. I recognise the good work of the blockchain APPG in producing a lot of good insight into a lot of that work.

Volatility is something, to the previous conversation, that probably comes back to some level of disclosures, and we need to make sure that that continues to be focused on. My understanding is that the online promotions regime—forgive me, I am not familiar with the exact Act—has been clarified quite clearly. There is also a direct licensing regime from the Financial Conduct Authority for any firm offering these types of products—crypto assets—to UK consumers. They must be licensed by the FCA. To some extent, despite their risk, they are in fact regulated. That should be an ongoing conversation. We should continue to evolve that conversation, and where there are consumer harms we should be directly addressing that.

Q212 **Lord Lilley:** You have given concrete and detailed answers so far, which is very refreshing. If I were in your position, I would have come before a committee considering financial regulation with two or three changes I wanted in financial regulation—a specific rules change or a change in the way the regulator operates. I suspect you are the sort of people who would have come with those two or three ideas. What are they?

Simon Taylor: That is a great question. I would simplify it as: No. 1, the co-ordination of the financial services regulators with non-financial services regulators; No. 2, the encouragement of data sharing between larger and smaller firms and non-financial firms, in whatever way the committee deems appropriate—I do not have a direct policy answer to what that should be; No. 3, the encouragement of standards for that data sharing. I am rather concerned about the lack of technical knowledge that goes into standards development from the policy side. I would point you to the Open Banking Implementation Entity and the difficulties that the industry had getting to open banking standards. It took many years. The larger institutions had the largest voice, and the smaller organisations complain of lack of access.

Where data sharing is promoted, it must be done via a tech-led approach—a tech-savvy regulator and a tech-savvy policy voice in the room. That would make a meaningful difference to the issue of APP fraud, mule activity and other activities.

There are other questions in here. I can pause there and take direct thoughts towards how we make the UK more competitive on the global stage and what metrics we should look at. I can dive into those if that is helpful, but I thought I would give you the higher view.

Lord Lilley: You will get those questions specifically from my colleagues.

Simon Taylor: Was that helpful?

Lord Lilley: Very helpful.

Soups Ranjan: To add to what Simon just said, I would like to make two points. Regulators should embrace new technologies. Even before AI existed, financial services companies used to get questions about machine learning, and now that AI is here regulators are probably thinking about how banks should adopt AI technologies. In that regard, I do not think there is full clarity as to what you are allowed and not allowed to do with AI.

With machine learning, the regulatory question that we often get is, "Are your machine learning models explainable, or are they a black box?" For those types of questions, technology can explain machine learning models pretty adequately.

Moving on to AI, it would be helpful if regulators could explain that it is okay for the bank to have AI models that do things like populate a SAR narrative, which is a piece of technology that we have developed at Sardine, but what is not clear, if I am submitting that SAR, is whether I could submit it directly with—

Lord Lilley: What is SAR?

Soups Ranjan: Suspicious activity reports. Could I submit the suspicious activity reports directly to the FIU, or does it have to be reviewed by a human? What we have seen is that once you start using technology such as AI you can improve the efficiency of compliance professionals by five orders of magnitude or even more. In that regard, it directly correlates with reducing the cost of doing business for banks. Therefore, I would argue that regulators should help banks to adopt newer technologies.

The second point, which is particular to APP scams and elaborates on what Simon said, is that regulators could also embrace public/private sector partnerships much more—for example, with the efforts that Simon mentioned on data sharing, which have been proposed by the public bodies in the UK. Our conversations with fintechs have revealed that not many of them have adopted those data-sharing technologies because they are not at par with what the industry is looking for. Therefore, instead of the regulator playing the active technologist role, I would argue that they should essentially invite industry to come and run those data-sharing systems in partnership with the public sector, because that would be a net win-win for the entire industry.

Lord Hill of Oareford: This is a small follow-up to Lord Lilley's question.

You are not regulated by the financial services regulators, but what you do is very affected by regulation. Has the FCA ever come to talk to you and asked for your advice and experience on how its regulation is affecting our ability to deal with APP fraud? Does it ever talk to you?

Soups Ranjan: No, not yet.

Lord Hill of Oareford: Okay, thank you.

Soups Ranjan: We have had conversations with the regulators in the US such as the OCC, the FDIC and others, but not yet in the UK.

Simon Taylor: In a prior life, when I worked at a large bank and I was head of crypto asset R&D and digital asset R&D, I found myself spending a lot of time with the regulators.

Lord Hill of Oareford: Not as a small guy.

Simon Taylor: Not as a smaller firm. However, if I was a smaller regulated firm, it is fundamentally different; but, as a technology supplier, very little. I should mention, though, that in a private capacity I have had some less formal interactions, but not through the company.

Q213 **Lord Sharkey:** May I ask about the responsibility of the customer in all this, and especially in what turn out to be fraudulent transactions? The technology you have been talking about to combat fraud already exists to some extent. When it is deployed, at what point might it be reasonable to recognise that consumers have been suitably informed and therefore they are at least partly responsible for the transaction?

Simon Taylor: I will give you a worked example of what best practice tends to look like in informing consumers. One of the downsides of being a younger technology company that is a secondary account is that you do not have as much data. You have to find other ways to prevent fraud, so you see some exceptional best practices in prevention. One example I would point you to is Monzo. It has an "active call-in session" flag in its mobile app. If somebody calls you and says, "Hello, I'm from your bank. I'm here to take all your money", you can go into your mobile app and check if you really are on the phone with this bank and it has secured that link. That is a positive development that technology could also make, and I would like to see that throughout the industry.

Another best practice from a consumer responsibility standpoint, if they still wish to make a payment, would be to play a small educational video and then make them wait for three hours. It is not just a single, simple warning; it is taking them through wait periods. It is doing everything you can using the technology itself to try to break the spell of the scammer. Once you have done that, after three hours, after you have had time to think about it and time to cool down, if you still want to break the glass and move the money, at that point you have to be really sure that you want to move the money. It is very much the case that people will still be legitimately and genuinely defrauded, and there will still be legitimate and genuine scams against the vulnerable populations.

Lord Sharkey: What is a legitimate scam?

Simon Taylor: There is a broader issue, which is first-party fraud. A lot of people will say, "Sorry, I've been scammed". First-party fraud makes up the vast majority of fraud; it is chancers—people buying a product and saying, "Oh, the goods were never received". That is an illegitimate reporting of fraud because it is first-party fraud.

Lord Sharkey: It is still fraud, surely.

Simon Taylor: Yes, it is, but the customer is saying, "I was defrauded", when actually they were the fraudster.

Soups Ranjan: It is a friendly fraud.

Lord Sharkey: That is interesting. The point of my question was: is there a point at which the consumer, the customer, has to take some responsibility for the subsequent fraud?

Simon Taylor: Yes. I apologise, I took us down a rabbit hole and used an incorrect definition, which one should never do in the House of Lords. I would argue that given sufficient warning—and sufficient warning should be best practices, and those best practices should be reviewed on a regular basis—yes, that is a point. The exception I would make is for vulnerable populations where perhaps that threshold should be higher.

Soups Ranjan: May I add to that?

The Chair: Before you do, we have had evidence from banks that they have told people and they have still sent the money. Just picking up on Lord Sharkey's question, surely, it is ridiculous that they should be reimbursed in those circumstances.

Soups Ranjan: I agree with you.

Simon Taylor: I would agree.

Soups Ranjan: Oftentimes, the nature of the scam is such that you are completely in a spell, and even if you try to break the spell they often go ahead and make the transaction. In cases like that, right now the reimbursement regime does not go further as to establishing liability back to the consumer. What I would argue that we should do next is establish some sort of a challenge mechanism where the sending bank can challenge back to the ombudsman, potentially, saying, "Hey, I did all these things. I have evidence here. I have shown them a video. I have given them sufficient warnings. I have even delayed the funds being sent, and they still went ahead and did it". In that case, the consumer should be held liable. Right now, that challenge mechanism does not exist. It does exist for card networks.

What I would also argue will happen as the reimbursement regime plays out is that fake scams will skyrocket. One big experience that we have had running Sardine is that fraudsters take advantage of every law that

has been created. Right now, the law is very much in favour of the consumer. What prevents me sending money to Simon, for example, from a brand-new device? Let us take Revolut as an example. Maybe I install Revolut on a brand-new device and I claim that my account got taken over and somebody else installed it. Then I sent money to Simon, we split the proceeds and we also get reimbursed. Those types of fake scams will skyrocket unless we implement a challenge mechanism.

Lord Sharkey: There are two things. A challenge mechanism would clearly be a good idea, but if you notify people, they will lose their money and there will be no refund—

Simon Taylor: A consequence.

Lord Sharkey: —if they proceed.

Soups Ranjan: I agree.

The Chair: Unless there are any other questions, on that note of consensus, we thank you very much for coming today, for being so patient at the start of the session and for giving us so much information both in the background and so on. We may come back to you with some further questions that we have not had a chance to cover today. We wish you every success in your endeavours to get at the fraudsters. Thank you very much. That concludes this session.

Simon Taylor: Thank you.

Soups Ranjan: Thank you for having us.