FSR GPS Podcast Series
Episode 8 – Scams Code Framework Briefing

Michael Vrisakis	Hi everyone. I'm Michael Vrisakis, a Partner in the Herbert Smith Freehills Financial Services Team. Welcome to our podcast series called the FSR GPS. This series focuses on topical and emerging issues in financial services regulation which we think are the most strategic and important issues for our clients. Feel free to suggest topics you would like us to cover in the future but for now, we hope you enjoy today's episode.
Charlotte Henry	Hi everyone, I'm Charlotte Henry, a Partner here at HSF in the Financial Services Regulatory team focussing on the non-contentious side of regulation and I'm joined here by my fellow Partner Andrew.
Andrew Eastwood	Hi everyone, I'm Andrew Eastwood, a Partner in the Disputes group here at HSF with a focus on contentious regulatory issues, especially in the financial services sector.
Charlotte Henry	So today on FSR GPS, we'll be discussing the government's consultation on the Scams Code Framework. The audio you're about to hear is from our recent webinar on this topic so apologies if it isn't the best quality. We hope you enjoy this episode. Please do reach out if you have any questions on the draft Scams Code Framework and how best to prepare your organisation. Thank you. So today is a very quick canter through the recent consultation that the government put out in relation to the Scams Code Framework. So let's get started. So just to set the scene, it's obviously, as we know, scams has been one of the biggest issues in the Australian market for well over a year now, longer than that, ever since COVID meant that we all got moved quickly to working, doing banking, communicating digitally. One of the biggest issues from all of that, of course, has been scams. And this has been a whole of government issue. For those of you that attended the various conferences, there have been, you know, scams have been such an important focus of the trade associations, the regulators, the government, and this is the reason. So, in the latest figures that have been published, combined losses have well, increased year on year, exponentially.

The biggest category of losses have been for investment scams, and that's where ASIC has its focus in relation to those types of scams. Worryingly, though, this is obviously just the tip of the iceberg because as you see there, the findings are still that this type of activity is very under-reported. So, there have been a lot of different regulators and try to locations looking at what they could be doing in this space. We also have the private sector that has stepped up and has done some action in relation to what they might do relation to scams. But the government has always said that they would come out with what they think the approach to scams and the Scam Framework should be, and that's what this particular paper that they've put out is meant to do. It's meant to set out the government's approach to how they're going to regulate scams.

I think the first thing that is interesting from the consultation that came out last week is that they are proposing to introduce a definition of scams. We currently don't have anything in the legislation like this. So, it's a dishonest invitation request modification or offer designed to obtain personal information or financial benefit by deceptive means. Quite a broad definition with an express statement that it's not intended to capture and authorise fraud. Obviously, we have the ePayments Code that deals with that. So, investment scams being the highest one that is occurring, the market at the moment, romance scams, phishing employment scams, remote access scams as well.

In terms of the principles that they want to guide the framework and the development of the framework, there are three. So the first one is that it has to be a whole of ecosystem approach. So, bringing in digital platforms, digital communication platforms, not just focusing on the banks or those that are compensating at the end of the scam. So, a whole of ecosystem approach, they want the sort of interconnectivity and interrelation between the different sectors to make sure that things are being approached in a similar way. And this is really interesting when you come to think about the EDR aspect that we'll talk about a little bit later.

It must be flexible and responsive. So, the ability to be able to change as new scams are developed, new players in the market are involved in scams. And then finally they do want it to leverage off of existing regimes and processes that they have at the moment. So, as we know, the ACCC has got their digital platform inquiry, their multiyear inquiry that has been ongoing and they want to leverage off the work that's been done as part of that.

So, what are they proposing? So this is the framework. So there is going to be an overarching framework that will apply in relation to the whole scheme, regulatory, legislative infrastructure and the proposing to put this into the ACL, into the Competition and Consumer Act and the key regulator, they will be the ACCC, obviously the ACCC has already got aspects of scams, right, of activity that it's looking after with the National Anti-Scam Centre, the watchlist line that they have and all the work that they have been doing like doing the digital platform inquiry so that already had government funding in relation to those aspects they're looking after. So, they will take overall coverage and carriage in relation to the overall framework. But then they will be these sort of mandatory, so not voluntary, mandatory sector focused codes that will be developed under that overarching framework and they'll be divided into the bank sector, looked after by ASIC, the telco sector, the digital platform sector and then leaving space for future sectors. So that's the overall framework. And we're just going to touch on a few aspects of this in the session.

So, for the overarching framework, they do want input into primary legislation, so it needs to be enforceable and needs to be the entire ecosystem involved and it will apply identically to both banks, telcos and digital platforms. Well, at least this is what the government's currently thinking at the moment.

In terms of the detail that was set and that will go into the overarching framework. So, there are these four buckets that the government wants to see addressed. So, first to focus on prevention, then detection and disruption, then response and finally reporting. So, I think what's interesting on the first aspect about prevention is that there is, at the moment anyway consulted on, a real focus on wanting to have an anti-scam strategy. And for those that have been involved in responding to ASIC's questionnaires in relation to when they were looking into what banks were doing and what their approach to scams was, there was this focus on what is the strategy. This seems to be different and separate from a broader fraud strategy, but a real focus on strategy. This would need to be a living, breathing document. It will need to have senior approval, senior visibility be shared both with senior managers be shared with the ACCC. This would need to be backed up by anti-scam systems. All reasonable steps be taken to prevent scammers from misusing the services. They also need to build on how customers and consumers are being informed about scam safe practices and an element of training as well.

So, this is what they're expecting, the strategy about prevention scams and in particular organization will involve. So a bit broader than what we have at the moment from, but more focused so that we have at the moment in relation to sort of fraud more generally. I don't know Andrew, if wanted to talk on that.

Andrew Eastwood

Yeah, and I think this requirement for a documented strategy is an important development. The businesses who are going to be subject to this framework are going to need to get their heads across. I think you said one of these things where each strategy is going to be specific to the particular business. It's not going to be something you can sort of just take off the shelf. It's going to be evolving, but also a business's strategy is going to have to be tailored to the particular sector that that business is in, the particular services that it provides and the particular scams that it is seeing and having to deal with.

So that's one point is that I think it's not one size fits all in terms of these strategies. I think another is there could be real questions around what's supposed to be in this strategy or documents that the consultation paper provides a little bit of guidance around that. I think another place to look for some guidance on that is ASIC's report from April 2023, earlier this year when it looked at the big four banks and there's some detail there around what ASIC liked in that particular strategy that it saw that one of the banks had and it talked about how that strategy outlined customer education and awareness campaigns, increasing friction, improving scam detect detection capabilities and the like. But it also had measurable success targets for improving scam prevention and detection and improving the customer experience and how that was going to be measured as well. So, I think if you're looking for guidance as to what this sort of so-called strategy needs to have, that's another place to look.

And that's a really interesting point, Andrew, around the friction piece. So our engagements with ASIC to date, bearing in mind the largest category of scams is investment scams, but they've certainly been wanting firms to be talking about how they're introducing friction into their systems as a way of disrupting the scam and then preventing future scams, which obviously is has a bit of tension to where payments and other types of systems are going on. It's all about making quicker, faster, safer payments. This kind of

---

concept of friction that certainly the language that they've been wanting to hear.

Onto the next bucket then. So, strategy is all about prevention steps that will be taken to prevent scams. Then there's a focus on detection and disruption. And this is all about sort of systems. How is it going to be operationalised? What steps are businesses going to take? And as Andrew mentioned, the strategy is going to be bespoke to the business. So, the steps that will be taken, obviously bespoke to the business as well. So, steps to detect, block, prevent, verify and trace back timely information that's given disclosed to consumers when they might be aware that are scam targets and arm them with tools to verify in real time. And I guess the theme from all of this is that this is going to have a systems impact and potentially require investment in relation to businesses and systems, but also trying to stay interconnected with other sources of information that there will be out there. You know, there is that financial crime task force, an intelligence task force where people are sharing information. So, it's kind of how you're taking all that information, connecting to places where you can get real time information to then be able to share it and act appropriately so we can see that promotion to scams in particular, there might need to be a little bit investment in systems to operationalise the strategy. Did you have anything on that Andrew?

Andrew Eastwood

Only to note that I think the way at least it's been expressed at the moment is that these sorts of obligations are expressed in quite general terms. They're almost sort of principles-based. So, the government, I guess consistent with what Charlotte mentioned earlier in terms of overall objectives, they're not going to be that prescriptive. I think about particular measures that particular businesses need to do that will be more general obligations. But of course then as the market evolves and we see new measures coming into place and being implemented, there's going to be an expectation, I think, that the rest of the market will follow. So just keep on driving the bar higher and higher.

Charlotte Henry

Yeah. Then response. So, taking reasonable steps to prevent further loss and then implementing user friendly and effective scam reporting measures and complaints handling, and that's all about building on existing EDR processes that banks may have internally. I mean, this is quite an interesting topic if we're thinking about this being in the overarching framework and that applying to all sectors. So, we think about the digital

---

communication platform sector at the moment. You know, having an EDR framework is not something that they are required to have. So this will be new for them. And this very much mirrors sort of where the EU has gone in terms of making digital platforms have the ability for customers to complain about an advertisement that might have actually been in an investment scam that was advertised through that platform.

So certainly I'm sure banks already have EDR measures in place, but this would be extending it to all different sectors that are in scope, dealing with them fairly and promptly, we are all familiar with that kind of terminology, and then the ability to take them to an EDR scheme, which obviously currently has for banks and telcos, but would be very much a new world for the digital communication platforms. Andrew?

Andrew Eastwood — Yeah, and I think a really interesting issue here, which is flagged in the paper, but I don't think they have a solution to yet is, how do you achieve coherence between the various EDR schemes? In some sense, because they want this whole of ecosystem approach and they want a consistent approach being taken across sectors and everyone talking to one another so, I think is going to need to be some mechanism for AFCA, or the financial services sector, to be able to in some way communicate with the Telecommunications Industry Ombudsman and whatever else comes in for the digital platforms such that this actually works because I think if we had every EDR mechanism doing their own thing, then that's going to undermine what the government's seeking to achieve here.

Charlotte Henry — And then finally reporting, so reporting to other agency agencies. Yes, reporting to the National Anti-Scam Centre. Yes. But also you can see from the paper that they're sort of expecting this kind of reporting internally as well. So, reporting throughout an organization, truly so separate reporting on scams, not just reporting on it as part of general fraud. Keeping records – I think all the industries are used to record keeping obligations and then responding to the ACCC where there are requests. And this would be overlaid on top of the other regulators that also would be able to request information as well. Andrew, did you have anything on reporting?

Andrew Eastwood — Look, just generally, I mean, insofar as this is capturing internal reporting as well. Then again, another a good place to refer back to in terms of what I think the regulators are going to expect in terms of internal reporting to

---

boards and senior management about scams is if you go back again to that ASIC Report 761, there was quite some useful detail there around at least what our corporate regulator was expecting at that time in terms of the information that such governance bodies should be receiving. And I'd be surprised if the ACCC viewed it differently as to what it would expect in such reporting.

Charlotte Henry

So going back to our framework again, so we've talked high level about what the consultation is proposing in relation to the overarching framework. So then just looking at some of the mandatory sector focused codes. So what I've said is that for banks, they want to have the mandatory code mandated and legislation that's administered by ASIC. So potentially the ASIC Act, ASIC could be the regulator and it's yet to be created. Telcos there already got a particular coverage which will be reviewed and updated, and then digital platforms have yet to be developed as well. They're looking at the regulator specific legislation and then building and mandating where the code or the requirement for the code will be located.

So just to take one sector as an example. So, they have said that they want to have a new banking sector code that applied to everyone that's got a license currently. They said it will be developed by the government with enforcement powers to be given to ASIC and then they've sort of set out what they're proposing that certain items in certain elements would form part of that particular code. So similar, for instance, to the ePayments Code, which looked after it was PayNet but owned by ASIC, you could potentially see a similar type of code being developed here, but obviously it's going to be made mandatory. I know with the ePayments Code, one of the requirements or proposals of that payments reform is to make that mandatory that be made mandatory. So, this is something that the market has been calling for a while about actually checking who the payee is when a transfer is being made, when authorised push payments are being made. And I think the most interesting thing to notice about all of this is obviously the ABA has recently done their accord which does seek to talk to a variety of these aspects that are already being proposed by in this particular consultation by the framework. And, and I think there is generally a sense in the market that banks were wanting to get out ahead of this and all ready to take some of these steps to guide what the code might eventually look like. Andrew?

Andrew Eastwood — Yeah, no, I think that is one of the interesting points from this that there is clearly a degree of overlap between the ABA scam safe accord and what we're seeing in this consultation paper. I don't think that's a coincidence. And as you say, I think that's an example of an industry trying to get ahead of it, get some control over this process. And it'll be interesting to see whether we see that in other sectors as well. I think it's something that I'll be interested to see how it develops in relation to these particular codes is the level of detail to which they end up descending. I mean, the guidance that we're being given in the consultation paper in seeing obligations expressed in quite general terms which would leave a lot of leeway for different businesses as to how they approach it. For instance, implement processes to detect high risk transactions. It's not specifying in any way what those processes would be. It'll be interesting, I think, to say whether we stay at that level or whether we go more specific. And if we go more specific, then obviously the devil's going to be in the details. But yeah, I think that the key thing is for other sectors is do they seem to take the approach that the banks have sought to actually try and get some control over this process?

Charlotte Henry — And also if it gets to stay as an accord because I'm sure that word was chosen deliberately to not have a connotation with the banking code of practice, for instance, which is quite granular. So, we'll see where we get to with that. Okay. Just then, turning now to some liability and how liability might be determined as proposed by the consultation. Andrew?

Andrew Eastwood — Yes, so look, I think liability has obviously been a big issue in Australia and overseas over the last 12 months or so. So scam victims seeking to see whether they can recover from businesses involved in the scams and particularly as against the banks offering involved in the transfer of relevant payments and the like. And what we've seen in other jurisdictions is a variety of different approaches to that. So perhaps at the extreme end is sort of the UK approach where we will see introduced next year, as sort of a mandatory reimbursement approach, where effectively the banks sort of split 50/50 between the sending and receiving bank will be liable to reimburse scam victims unless the banks are able to show essentially gross negligence by the relevant customers. So that's quite an extreme approach. The thinking behind that, presumably from the government is, well, it's putting the real that the emphasis on the banks to be doing everything they can to seek to act to prevent scams that really incentivise the banks on that.

But there are still concerns around the moral hazard created by such a policy.

Singapore recently has issued a consultation paper which is just about phishing scams, but it takes a different approach, really adopts a sort of a waterfall approach where somewhat similar to what we see in this consultation paper, it proposes some specific obligations on banks and some specific obligations on telcos and what it effectively says is, well, if bank doesn't meet its obligations, then it's liable, if it meets its obligations, but the telco doesn't, then the telcos are liable and then if they both meet their obligations, well, it's on the customer. And so that's the approach that they've taken. In Australia to date, we haven't had some kind of systemic approach to it, customers who's been subject to loss – some have sought to pursue claims through the courts. Generally those have been unsuccessful. Many pursue claims through AFCA if they're seeking to claim against their bank. And at least in recent times it's been relatively difficult for customers to succeed in those claims. AFCA has generally taken an approach that it's not the banks responsibility to be maintaining some kind of watching group for scams and unless there were pretty clear red flags for the bank. Then generally speaking, the customer is bearing the loss. And I guess the question is, well, where are we heading? And does this consultation paper give us much guidance on that?

And I think the answer is that the framework that that released still leaves that somewhat up in the air. It's not all that precise around how liability will work, but I think we can say with some competence that we're certainly not in the short to medium term heading down the UK path. What this feels like is something more similar to the Singapore approach whereby if a business doesn't meet its obligations with one of those general obligations under the framework that will be in the Competition and Consumer Act or doesn't meet obligations under one of these specific codes, then in those circumstances it will be liable. And that these sort of ADR mechanisms, such as AFCA and the Telecommunications Industry Ombudsman will be able to sort of enforce those kind of liability mechanisms, but not something like the UK approach whereby essentially banks that was deemed to be liable unless they can show gross negligence. I think that's where we're heading. But maybe we'll get more clarity as this consultation precedes perhaps.

Just briefly, one other thing that the consultation disclosed, is that in addition to potential liability to customers, it will be that the intention is there'll be penalties for noncompliance with those general obligations under the Act and also noncompliance with the specific codes and so there's discussion

around where those penalties should land. And one of the questions as posed by the paper is should we be achieving consistency in terms of penalties across the different across the different sectors? But yeah, I guess key point is there will be some teeth to these obligations once they come into law. Back to you Charlotte.

Charlotte Henry

Thanks, Andrew. So, in terms of next steps, we've got up to the end of January after Australia Day to pop out sponsors on the consultation and the government has said that they want to have the first version taking effect during next year, but they have a very active legislative proposal, proposals next year, including digital assets, including payments. So, it is quite a lot that they're proposing and want to do next year. But in the interim, we do have, as Andrew has mentioned, ASIC Report 761 which was the findings from the initial review of the majors and potentially there could be more there coming with the other thematic reviews that they are doing. So do watch out for that. So if you're looking for guidance about certainly what ASIC will be telling the government in relation to their expectations about what the codes should cover and their expectations about content of things like scam strategy, like what Andrew talked about, then we definitely recommend that you look to that for guidance. Thanks a lot.
