FSR GPS Podcast Series
Episode 6 – Scams – A customer's rights, a bank's obligations

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.
David Curley	Hi, I am David Curley, a senior associate in the banking and regulatory team at HSF with the focus on banking and financial services, non-bank lending, anti-money laundering and digital currency regulation.
Andrew Eastwood	Hi, I'm Andrew Eastwood, a partner in the disputes group at HSF. I specialise in contentious regulatory matters and other litigation in the financial services sector, particularly those involving ASIC, APRA, the ACCC and the police and I've been involved in a number of pieces of litigation recently relating to scams.
Peter Jones	And I'm Peter Jones. I'm a partner in the technology, media and telecommunications team here at Herbert Smith Freehills and like Andrew, I advise financial services entities, although my advice typically is around technology and data projects, including the regulatory implications of technology adoption and adaption.
David Curley	In today's episode, we'll be talking about scams and specifically authorised push payment or APP scams. APP scams stand in contrast to scams that involve a bank account being hacked or compromised in another manner. So what are APP scams? By way of background APP scams occur when a bank's customer instructs their bank to make a payment to a third person. That is, the bank's customer authorises its bank to push money, i.e. a payment to a third party, hence the name an authorised push payment. While the instruction is a valid one, the third party recipient is not who they claim to be, and as a result the Bank's customer falls victim to a scam.

There are many different types of APP scams, with the most common being investment scams, romance scams, force building and online shopping scams.

Unfortunately, in today's society, most people are all too familiar with having received an unwanted call, e-mail or text as part of the first steps in an attempted scam. Famously, last year the ‘Hi Mum’ scam where the scammer posed as a family member or friend did the rounds both here in Australia and abroad with more than 1,150 Australians falling victim to that scam in June and July 2022 alone. This one came very close to home with my own mother almost falling victim to it. So what are the statistics? Well, according to the Australian Competition and Consumer Commission report published in April 2023, Australians lost a record $3.1 billion to scams in 2022. That's up 76% from the same time last year. And this issue is now endemic. Those figures are almost certainly a significant understatement, given a reasonable assumption that many APP scams go unreported.

And what about the law?

While the ePayments code covers scams involving a bank account being compromised, that is where the relevant payment transaction was not authorised by the customer. However, the ePayments code does not extend to APP scams and as a result, banks must consider other legal sources in order to work out what the regulatory duties are and who is liable when an APP scam occurs.

In recent weeks, the Supreme Court in the UK has handed down a major decision on APP scams, which is more clearly defined the boundaries of the so-called “Quincecare Duty of Care” owed by banks to its customers. We'll be discussing this case later in the episode. But first of all, Andrew, when it comes to APP scams, are banks in Australia liable when their customers to their customers when a scam occurs?

Andrew Eastwood Well David, there's no simple answer to that question.

Victims of scams have a number of potential causes of action that they could bring against a bank, including in contract, in negligence, hence alleging a duty of care, knowing assistance in a breach of fiduciary duty, misleading conduct, unconscionable conduct, and, I have to say in recent litigation that I've been involved in assisting a bank. Responding to these types of claims, the plaintiffs have sort of sought to rely upon all of these potential causes of action.

The other issue we need to be aware of is of course, scam victims. Customers can seek to pursue these claims through the courts, though they can also seek to bring complaints in AFCA.

And generally what we're finding in both courts and in AFCA is that scam victims under APP fraud are finding it pretty difficult to recover against a bank, except when the bank is on pretty clear notice of a fraud or the bank has been slow to act, for instance, to seek to recover monies once it does become aware of the fraud. So even AFCA, normally a pretty customer friendly jurisdiction, has been making very clear in a number of its recent determinations that really the key contractual obligation on a bank is to follow its customer's instructions and that generally a bank doesn't have a duty to advise the customer that a particular transaction is not in their best interests or an obligation to monitor transactions on its customer's behalf, or to maintain a watching brief for scams and that really to require a bank to take steps to prevent a fraud, the bank must have special knowledge of what was occurring or been alerted to the real possibility of fraud taking place and sometimes AFCA uses the language of red flags, so is there a red flag that would cause a reasonable bank to suspect that there was a real serious possibility that its customers are being subject to a scam. So I think the summary sort of position David is generally at the moment in Australia pretty hard for APP scam victims to recover against banks in the absence of the bank being on clear notice of the fraud.

David Curley — And in respect of ASIC, what is it said on this liability question?

Andrew Eastwood — There was a really important report issued by ASIC in relation to scams back in April. This is ASIC Report 761 which addresses scam prevention, detection and response by the four major banks and that report actually covers quite a lot of important territory and it's important for people to review that report in its entirety, but on this question of liability when banks are liable or should be compensating scam victims, ASIC says a number of things that they are concerned that the banks are generally taking a narrow approach to liability. Sort of they make the point which you covered earlier, David, that the ePayments code is not the only basis on which a bank could be liable.

ASIC's view is that there's not a consistent response between different teams within banks, for instance, a different response by the scams team as opposed to, say, the complaints team and they say that the stats sort of

---

show that a customer who complains is more likely to receive some form of compensation than if they don't and I think overall ASIC is concerned that it seems like the banks are only compensating around 4% of scam losses and ASIC's view is that that's lower than they would expect or would like.

David Curley

Understood. Now speaking of ASIC Peter, ASIC recently announced that the National Anti-Scam Centre will be coordinating its first time limited task force, or so-called 'fusion cell' on investment scams. This fusion cell is going to be led by the ACCC and ASIC with representatives from the banks, telecom industry and digital platforms. As banks and other market participants lean in on their obligations to protect against technology enabled or technology enhanced scams, what are some of the key related challenges that you see will continue to confront this industry?

Peter Jones

That's a great question. I think actually when you boil it all down, it's two sides of the same coin in some respects. So technology can giveth and technology can also taketh away. What do I mean by that? If we look at the extent to which we have largely a globally interconnected set of economies that has led to a great degree of ability for individuals, organisations, etc to transact cross-border. That's been empowered by technology. Equally however, as a result of international connectivity, there are also some challenges that arise in connection, in this case with scams.

The connectedness is important, and it's also reflected in the nature of the fusion cell that you identified, where we're looking not only at financial services entities but also telecommunications players and digital platforms themselves, and that in itself is essentially, I guess, an indication of the challenge that we are dealing with when it comes to technology-enabled crime – whether that is in relation to scams or some of the issues that we see separately in the cyber area.

But if you play this forward in terms of the area that we now start to see in emerging use of technology in terms of scams, we're talking about a lot of deep synthesis technology, so deep synthesis – otherwise known as deep fake – that could be images, it could be audio, it could be video that is essentially empowered by generative AI. To give an example, there was a case recently in North America involving an individual who his parents were effectively apparently called by a person purporting to be a lawyer who said that their son had been involved in a hit – a sort of a fatal accident involving a person – and they urgently needed funds to post bail. And then they

---

purported to basically engage in a conversation between the son and the son's parents, using essentially a voice generating or a voice generated app commonly available on sort of the internet.

So when you're in essentially in that situation, as it was for those parents who, while they were sort of listening and did, to be fair, have some sort of concerns around the nature of that, the emotional impact of having something that sounds like someone that you know saying, "hey, I need money, can you urgently need to help," is incredibly powerful, and in that case, did lead to a significant amount of funds being transferred. So we sort of have this challenge where we are looking at almost in a sense, the same way that organisations continue to look at personalisation of products and services. The criminal threat actors out there are doing likewise when it comes to these customisation of phishing attacks using a whole range of technology and a whole range of tools, including, as I mentioned, generative AI.

Now, it doesn't also just have to be the sort of the deep audio or the deep video-type arrangements, it can simply be using some of the generative AI tools to effectively mimic the messages that a bank would genuinely send to its customers. So you will end up seeing something in an email that looks exactly like what you would be seeing from your relevant bank. And again, because this is a personalised sort of attack, it will be your bank in terms of it will have information that's relevant to you in terms of your location because in many cases the information relevant to that attack will be available on the dark web and I'll talk a little bit about that later.

The other thing that's really important to note if you go back even probably two or three years, the nature of these kind of deep fake-type technologies was such that you would potentially need a significant amount of base data to generate something like a deep audio or a deep video fake of an individual. With some of the tools in the market you can get a pretty good reflection or mimicking of someone's voice based on literally 20 to 30 seconds of someone. And you might be thinking, well, where are they going to get that from? Well, social media is the prime example. So TikTok, Instagram, Facebook, potentially YouTube, if you're sort of posting videos on YouTube. That in itself provides sufficient data to at least, as I said, develop something that is pretty close to the original voice that you would be hearing if you were speaking to the genuine person.

So we've sort of moved a long way for those that are old enough to remember the days of the first kind of sort of evolution of the scam environment involving Nigerian princes trying to expropriate funds, which

involved spelling errors, grammatical problems, semantic problems. Now, when you sort of see the quality of some of these purported emails that appear genuine, or, as I said, moving into this area of increasing use of deep synthesis technology, the ability for people to critically assess and look at that threat and then manage it appropriately is going to become increasingly challenging. And so for those organisations that are active in this space, and I know that our financial services entities, along with the telcos, along with the digital platforms, this is a very well-known threat issue, they are spending a lot of time and money on identifying better ways of managing against some of these threats. But ultimately in many cases, the convenience that people have gotten used to in terms of financial services ie the ability to essentially say, "I want you to pay X amount of dollars out of my account" and it goes, the sort of the friction that would be imposed on some of those transactions that would be useful if you were looking at how to better protect against scams, is almost contrary to the learned behaviour that many customers have.

So going forward, getting this balance right between convenience versus protection is going to be a key part of the conversation that we need to have, including getting to the point of even education, particularly for some of our more senior and older citizens who may not be technology savvy to the same degree that more digital native individuals are. So I think, David, it's going to be a very challenging environment going forward.

We are also dealing with a broad range of criminal networks, which are obviously looking at opportunities. It is challenging from a jurisdictional basis to essentially prosecute or look at recovery in the event you are subject of one of these scam situations, so, you know, we are sort of in a sense engaging with this threat which is emerging and everybody is trying to obviously ensure that they can better respond.

David Curley

Understood. Andrew, coming back to my comment at the top of the episode, the last month the UK Supreme Court handed down a major decision on APP scams. Can you tell us what they decided?

Andrew Eastwood

Yeah, sure David. That's the case of Philipp v Barclays Bank. That was a scenario in which Mrs Philipp transferred over £700,000 from her account with Barclays to some bank accounts in the UAE, and she actually thought she was doing that to keep her money safe. She thought she was dealing with persons from the Financial Conduct Authority and the National Crime

---

Agency, when in fact she was dealing with the fraudsters. And she brought a claim against the bank, alleging that it owed so what's called a Quincecare Duty of Care to protect her from the consequences of the payment she made. The bank denied that it owed such a duty, and the case eventually made its way to the UK Supreme Court, where largely the bank was successful in saying that there wasn't a duty of this kind on the bank to protect its customer from APP fraud. The UK Supreme Court said that a bank owes a general duty to act with reasonable skill and care when processing customer payments, but this is limited and applies only to interpreting, ascertaining, and acting in accordance with the instructions of the customer, and that the Quincecare Duty referred to in earlier decisions is really just an application of that general duty that arises specifically when an agent of the customer purports to give a payment instruction. And so in that judgement, the UK Supreme Court says, look, the basic duty of a bank under its contract with the customer is to make payments from the account in accordance with the customer's instructions. It says that that duty is strict, and that when the customer was authorised and instructed the bank to make the payment, the bank must carry out the instruction promptly and "it is not for the bank to concern itself with the wisdom or risks of its customers payment decisions".

Now, one aspect in that matter that the court did leave open was an argument as to whether the bank had a duty to act more promptly to seek to recover the payments once it became aware of the fraud on Mrs Philipp, and that's now just going to have to be resolved on the facts. But as a general matter it's a finding that there isn't a duty of care on the bank in relation to APP fraud. And I think when you look at what the court says in that case, David, it actually matches up reasonably closely to what AFCAs been saying over the past year, as I sort of referred to earlier in this podcast.

David Curley

And staying with the UK, we know that they've recently adopted a mandatory reimbursement model which applies to banks. Can you describe how that operates and do you think Australia will follow suit?

Andrew Eastwood

Yeah, good question, David. So UK's had since 2019 a voluntary contingent reimbursement model that a numbers of the banks have sort of signed up to but what the UK is doing within the UKs faster payment system is that they're introducing this sort of mandatory reimbursement model with an implementation date of April next year and broadly speaking, the way this will work David is that where a customer falls victim to APP fraud, but the

---

banks must reimburse subject to exceptions that, that reimbursement is split 50/50 between the sending and the receiving bank and relevantly the only exceptions are where the customer itself has acted fraudulently or the customer's acted with gross negligence, it's pretty clear from everything that's been said, that that bar for gross negligence, is going to be set very, very high. So it's going to be hard for banks to fall within that exception.

Yes, your question around will Australia follow? I mean my best guess is that in the short to medium term, the answer is no. There are a number of consumer groups in Australia pushing hard for us to follow the UK's approach but the indications to date are that the Government is not going to go that far. What Financial Services Minister Stephen Jones has said is that there is going to shortly be a public consultation on a new code of practise and I guess we'll have to see what's in that that consultation draught but my current expectation is the way the model we'll have in Australia will work, is more that there will be a set of obligations imposed on banks, perhaps additional to what they currently face and if the banks don't meet those obligations, then they will be liable but I don't see the Government at this stage moving to the full banks are always on the hook unless you can fall within the exception, but we'll just have to see how the public debate plays out on that and that could be something on which the mood could shift pretty quickly. So I could see that perhaps coming out way down the track.

David Curley

Understood. Coming back to Australia now and leaving aside that question of liability, Andrew, what are the key regulatory changes or risks rather the banks in Australia face right now in this space?

Andrew Eastwood

Yeah, look, I think the biggest one, David, just putting aside liability is just that the fact that the expectations on banks in this area as to what they are doing to detect and prevent and respond to scams is just going to keep getting higher and higher. And I just mentioned this code of conduct that's apparently coming in like to see what's stated in that. You've got the general obligations on banks and other financial licensees under 912(a) of the Corporations Act, including the obligation to be efficient, honest and fair, and I can certainly see ASIC using obligations like that one to seek to sort of ramp up expectations and what banks have to do in their space. We've seen ASIC use that efficient, honest and fair obligation in other areas like cyber security and I think we'll see it here as well, if they are not satisfied with what banks are doing and that's going to be in areas such as what Peter touched on such as technology and artificial intelligence and the like and I think they

---

will be expecting all financial institutions to be closely monitoring what other entities are doing, what initiatives that they're putting in place both here in Australia and overseas and following them and so what we'll continue to see is a lifting of the bar and if people don't follow, then I think ASIC is going to come knocking.

David Curley

Thanks, Andrew and the final question, Peter, Andrew's talked about the UK's mandatory compensation scheme, whether it'll be introduced here, and the potential regulatory liability banks are exposed to arising from scams. What impact do you think these legal risks or indeed the scams themselves will have on the development of technology needed in the future?

Peter Jones

Yeah thanks David I think interesting some point that Andrew raised around sort of not just the legal and regulatory obligation, but the expectation aspects. And I would absolutely agree in this space that it is both a function of legal and regulatory compliance, but more broadly expectation management as well.

Andrew also mentioned cyber and yeah, there are some interesting lessons, I think that any organisation can use when it looks at sort of technology enabled threats, particularly out of the cyberspace and then play them into more of the scam environment.

When we start looking at cyber, essentially you kind of have had historically a sense of the threat and then people have got better at responding to the threat and the threat actor is evolved. So it's a bit like the old analogy, you can build a six foot wall and someone will build a 7 foot, in this case, digital ladder to get over it or some form of tunnel to get under it. So the threat environment will always continue to change as organisations respond, however, while previously in my last answer I might have painted a pretty negative picture of sort of the role of technology. Of course, technology in itself is not necessarily bad, nor necessarily good. It can be used for both of those purposes and we are seeing across the globe a number of banking institutions and financial services institutions using technology, including AI in a way to counter that threat. So that can be things like using AI for complex data, behavioural prediction. They can be looking at things like biometrics down to the way in which individuals might move their mouse or tap their keyboard so that if someone happens to gain access to their particular computer, they can go, this isn't the same person as it normally is because the way in which they type the way in which they use their mouse

---

is different from the usual patterns. You can look at sort of diagnostic tools as well. So there are a range of tools that organisations have already and will continue to evolve as part of a technology enabled response to the threat environment.

The other thing that I mentioned before again will be also the education campaign side of it as well, which is the human firewall for want of a better term and we're certainly seeing that now already with financial institutions endeavouring to ensure that part of the role they play is also educating customers on the threat, the nature of the threat and how potentially they themselves as in the customers can perhaps better protect themselves from those threats from little things like before you click on a hyperlink, hover over it and see what the address is, and if it looks strange, don't click on it. Simple things like that can actually make a big difference in terms of the extent to which these sort of scam threats are spread more broadly. So I'm certainly not here suggesting that we are all doom and gloom, and I do know the extent to which many of the entities out there are spending considerable amounts of money in terms of technology development, which is focused very much on scam and fraud detection and in many cases quite successfully as well that will necessarily need to continue to evolve, whether that's motivated by legal and regulatory change or simply through the views of what organisations should be doing based on the expectation of their customers will probably be seen, as Andrew said, to be driven a little bit through what we will be seeing in the next few months/years, but I do see that there is this potential use of technology in a way that will counter the technology threat itself. So again, very similar to what we see in some respects and Tim to some other cyber elements

---

David Curley — Very good. Well, that's all we have time for today. Thank you, Andrew and Peter for sharing your views and thank you for joining us for this discussion on APP scams.
