

The complaint

Mrs W complains that HSBC UK Bank Plc, trading as First Direct, won't refund her the money she lost after she fell victim to an Authorised Push Payment scam (APP scam).

Mrs W brings her complaint with the assistance of professional representation, but for readability, in what follows I will refer solely to Mrs W.

What happened

In June 2022, Mrs W received a message during the evening, through an instant messaging application, from somebody who referred to her as 'Mum'. The message said that they had broken their phone and had a new number, so Mrs W should delete the old details. Mrs W believed this to be her son, especially as one of the messages said it was her 'eldest'. She's also said the messages matched how her son would normally speak to her. But, unknown to Mrs W at the time, she was communicating with a fraudster.

Mrs W no longer has the messages. But she's explained that she conversed with the fraudster about 'day to day' questions. The following day Mrs W received a further message asking if she'd help pay an outstanding invoice. The message explained that due to the new phone, Mrs W's sons online banking had been suspended. Mrs W has said at the time her son was seconded in a job and she thought it might be something to do with that, she knew this job was important to him and wanted to help. Mrs W added that she's lent money to her son before and he's always paid her back.

Believing everything to be genuine, and with the belief that she was helping her son with an urgent payment, Mrs W called First Direct to make the payment. Relevant extracts from this call are detailed below;

Mrs W – I want to transfer, I want to make a payment please, it's a big payment so I want to do it over the phone, to make sure it goes to the right place.

First Direct – This is coming from your First Account, is that right?

Mrs W – No, can I, I want it, because it's a big sum, it's £2,900. So can I take it out of the ISA please.

First Direct – You want to transfer that into your First account and then make the payment from there?

Mrs W – Yes please, thank you.

First Direct – Ok, so that's £2,900.

Mrs W – Yes

First Direct – Obviously, just to, by transferring from the cash ISA you lose any of the allowance you've already used for the tax year. Just checking you're happy to continue.

Mrs W – Yes, the money is going back in in the next couple of days. It's just a temporary.

First Direct – Yes, just letting you know that by making a withdrawal you lose the allowance, so I was just checking you were happy with that.

Mrs W – Yes, that's fine, thank you.

First Direct – Is it a payment you've made before?

Mrs W – No, that's why I wanted to do it over the phone.

First Direct – Ok, no problem. Ok, so who is it to.

Mrs W – [provides name of payee]

First Direct – Ok, so what's prompted you to make the payment today?

Mrs W – Oh, I'm doing it on behalf of my son, he's got a new phone and so his online banking has been suspended, blocked for 24 hours while, something to do with his new phone. So he needed to do this, so he's asked his mum, like they do.

First Direct – Ok, lovely. And the details you're sending to, are you happy that you've received those face to face, they're the correct details?

Mrs W – Yes, yeah

[Mrs W provides account details, which are repeated back to her]

First Direct – Do you know if that's a personal account?

Mrs W – It's a private account.

[First Direct confirm the payment has debited Mrs W's account]

After this initial payment was made, Mrs W has explained that she received messages requesting for a further two payments to be made. Still believing she was communicating with her son, Mrs W went ahead and made a further two payments, via her online banking. One for £2,400 to a different beneficiary, then a further payment of £1,490 to the first beneficiary. Mrs W said she became suspicious when she was asked for another payment and she mentioned it to a work colleague – who suspected it may be a scam. They suggested Mrs W call her son on the number she originally had for him. Mrs W did this and on speaking to her son, she realised she'd been scammed.

Mrs W raised the matter with First Direct. First Direct is a signatory of the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code). The CRM Code requires firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances.

First Direct issued its final response on 24 November 2023, not upholding the complaint. In summary, it said that during the call (when Mrs W was making the payment for £2,900) its representative had followed its scam warning procedure. It added that Mrs W did not answer honestly the reason she was making these payments, so it didn't agree it had failed in its obligations to check these payments.

In its submissions to this service First Direct added that when Mrs W had called, she said she'd obtained bank details face to face, which was not the case. It said that had she told it of messages being received by the instant messaging service, it was confident a further discussion would have taken place about social media scams, and that it would have asked her to contact her son on a trusted number before proceeding. Alongside this, First Direct said it had provided Mrs W with an effective warning, when making the first of the online payments.

First Direct confirmed that it had reached out to the beneficiary banks (the banks to which the payments were made) and had recovered £13.29.

Unhappy with First Direct's response, Mrs W then brought her complaint to this service. One of our Investigators looked into things and thought the complaint should be upheld. In summary our Investigator;

- Didn't think First Direct did enough when Mrs W first called. It was our Investigator's view that information Mrs W had provided First Direct with during that call included all key features of a scam type that is typically instigated through instant messaging. So our Investigator thought First Direct should have probed further and provided a warning regarding this type of scam. Our Investigator said that had it done this, she thought on balance Mrs W would have realised what was happening and wouldn't have gone ahead and made the payments.
- Didn't consider the warning First Direct presented when Mrs W made the first of the online payments was impactful or effective. She didn't consider it was specific and didn't bring to life how these types of scam may look or feel to a consumer.
- Didn't think First Direct had established that Mrs W didn't have a reasonable basis for believing she was making a legitimate payment to her son.

As well as this, our Investigator also added that the R2(1)(a) exception to the code hadn't been established by First Direct. Overall, our Investigator thought First Direct should refund Mrs W the money she lost, along with interest.

Mrs W accepted our Investigator's view, but First Direct disagreed. In summary, it maintained that Mrs W wasn't truthful when she confirmed she had received details from her son face to face. It said it would only go on what it is actually told and the way the conversation pans out depends on this. Given what it had been told, it also didn't agree it should have opened up a conversation about the particular type of scam Mrs W was falling victim to. It added that it was Mrs W's choice to mislead it, in order to get her payment through, which indicated that she may have believed it would ask more questions and may not make the payment if she was truthful.

As agreement couldn't be reached the complaint has been passed to me for a final decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I have reached the same outcome as our Investigator for largely similar reasons. I am satisfied that:

- Under the terms of the CRM Code, First Direct should have refunded the money Mrs W lost. I am not persuaded any of the permitted exceptions to reimbursement apply in the circumstances of this case.
- First Direct should in any event have intervened further than it did when Mrs W was making the payment, as information Mrs W had provided it with ought to have put it on alert that she was at risk of financial harm. Had it done so, I'm satisfied it's more likely than not the fraud would have come to light and the loss prevented.
- In the circumstances First Direct should fairly and reasonably refund Mrs W the money she lost.
- First Direct should also pay interest on the balance not yet refunded at a rate of 8% simple per year. This interest should apply from the date Mrs W made the payment, to the date of settlement.

As I've said above, the CRM Code requires payment service providers to reimburse customers who have been the victim of authorised push payment (APP) scams, in all but limited circumstances. If First Direct declines to reimburse its customer in full, it is for First Direct to establish that one, or more, of the listed exceptions set out in the CRM Code applies. I don't think it has done that here and I'll explain why.

First Direct says that it is not required to refund Mrs W for the money she lost. This is because Mrs W had misled it when she told it she had received the details for the payment 'face to face'. It said if Mrs W had told the truth then it could have warned her accordingly.

I appreciate the point that First Direct is making here, and if the CRM Code didn't apply to these payments, the argument might have some merit. But as I have explained above, I find that the CRM Code does apply to these payments, and put simply, the CRM Code requires APP scam victims to be reimbursed in full, except where any of a limited number of exceptions apply.

Those exceptions relate to the victim's actions and beliefs about the payment at the time of the scam. Where those don't apply, then the victim is to be reimbursed. That reimbursement isn't contingent upon whether the firm was at fault or could have prevented the scam from occurring.

Indeed, even if it could not have been possible for the firm to have prevented the scam and the resulting financial loss, under the provisions of the CRM Code, the firm will most often still be liable to fully reimburse the scam victim. To quote section R1: *"Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer."*

The relevant exceptions to full reimbursement are set out in the CRM Code at R2. If a firm seeks to rely on R2 as a reason not to reimburse a scam victim, then it needs to establish that one of the listed exceptions applies.

However, the exceptions are limited. Only three of the five possible exceptions listed under R2(1) could be relevant here. I will consider each of those in turn before turning to R2(2).

Firstly, R2(1)(a) requires the firm to establish that:

The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective Warning [...]

When considering the *first* payment Mrs W has made, I don't think First Direct intends to argue that it gave Mrs W an Effective Warning in compliance with SF1(2). Rather, it states it would have given Mrs W an Effective Warning had she answered the agent's question correctly.

However, for this exception to be established, First Direct would need to, as a starting point, demonstrate that it provided an Effective Warning in compliance with the code. If it did not, then regardless of why it did not (whose fault that was) it cannot establish that a hypothetical warning was ignored. It cannot have been ignored, because none was given. It could never have been possible for Mrs W to have failed to take appropriate action in response to a warning she did not receive.

Simply put, First Direct cannot rely on R2(1)(a) here.

I'm mindful that my findings above relate to the *first* payment Mrs W made during a phone call. First Direct have also argued that it provided an effective online warning, when Mrs W made the first of the online payments (the second payment of the three). First Direct has sent us a copy of the warning it says Mrs W was shown when making the payment, but having considered this, I don't think this could be considered effective, when considering the principles of the CRM Code;

- While the warning, in part, refers to paying 'friends and family' and does mention being suspicious about receiving contact from somebody saying they are a family member, it is overall not specific to the type of scam Mrs W was falling victim to. The warning talks about fraudsters misleading the bank about the reason for the payment, contact through dating sites, hacking social media profiles and moving money for safe keeping, none of which were relevant to Mrs W.
- The warning does not mention any of the key hallmarks of this type of scam. Such as parents being contacted, through messaging, out of the blue by their children, explaining that their phones are broken and they have no access to their banking facilities, and asking for a payments/bills to be made on their behalf.
- The warning does not mention the prevalence of the type of scam Mrs W fell victim to. Nor mention that a check the consumer may consider carrying out would be to try and contact their family member on the number they already hold for them and not to proceed with any payments before they have spoken to them.
- I'm also mindful here that, rather than provide and present impactful information in the first instance, the warning requires First Direct's customers to click on links to gather further information about frauds.

I don't underestimate the challenge First Direct faces in providing warnings strong enough to break the spell in scams such as this. But the difficulty of meeting that challenge does not mean the warning given by First Direct was sufficient or contained enough clarity to meet the minimum requirements in the CRM code. Overall, I am not satisfied that the warning met the requisite criteria here. I don't consider the warning given was an effective warning as defined within the CRM code. It follows that First Direct has not established it can fairly apply the exception to reimbursement relating to 'ignoring an effective warning'.

I've gone on to consider whether Mrs W had a reasonable basis for belief when she made the payments. R2(1)(c) may only be applied where a firm can establish:

In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that: (i) the payee was the person the Customer was expecting to pay; (ii) the payment was for genuine goods or services; and/or (iii) the person or business with whom they transacted was legitimate.

While it's not clear that First Direct has argued that Mrs W made the payments she did without such a reasonable basis for belief, I have considered whether this might be a reason that the bank might choose not to reimburse her.

But I am not persuaded First Direct can fairly seek to rely on this exception. I am persuaded by Mrs W's testimony that at the time she made the payments she was convinced she was interacting with her son about payments he needed her to help him with. More importantly, I think it wasn't unreasonable of her to have held that belief in all the circumstances at the time.

Mrs W was contacted on a new number by who she believed was her son. Mrs W has explained that what followed was an exchange of messages talking about day-to-day things, in a manner that her son would usually speak to her in. I think this added legitimacy to what happened the following day, when the fraudsters then asked Mrs W to make payments. This kind of scam is designed to prey on a parent's natural inclination to help and defend their child. And so, it's fair to say, the rationale or circumstances may not be questioned as much as they otherwise might be. The fraudster is playing on an emotional response, that the parent is unlikely to be particularly aware of at the time.

The apparent similarities in how the fraudsters were interacting with Mrs W, compared to how her son usually did, lead me to find it was both plausible and persuasive for Mrs W in the moment. Mrs W believed the messages were coming from her son and that she was concerned he needed her help for his job, which she knew was important to him. In the circumstances, and on balance, I don't think it was unreasonable for her to hold these beliefs.

Therefore, taking all of the circumstances surrounding the payments into account, I am not satisfied First Direct can rely on this exception to reimbursement.

The final exception that could conceivably be relevant to Mrs W's case is R2(1)(e):

The Customer has been grossly negligent. [...]

The CRM Code does not provide a specific definition of gross negligence. In line with the interpretation adopted by the Financial Conduct Authority (FCA) in its guidance document to the Payment Services Regulations I take the view that "gross negligence" is: "a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness."

I do not find this can be fairly applied here. As reasoned above, I have found the scam was plausible and persuasive to Mrs W in the circumstances. I do not find she was very significantly careless in that respect.

I have specifically considered whether Mrs W showed a very significant degree of carelessness in the answers she gave to First Direct's agent when she made the payment using telephone banking – in particular when she stated: 'face to face'. As detailed in extracts earlier, First Direct has provided the relevant call recording and I have carefully reviewed the overall interaction with this in mind.

In the context of the call, I'm not satisfied the importance of the question "*And the details you're sending to, are you happy that you've received those face to face, they're the correct details?*" was made apparent to Mrs W. The question is closed and seems designed to elicit a negative response.

I don't agree with First Direct's assertions that Mrs W has deliberately set out to mislead it with the answers she gave, in an attempt to avoid further questioning from the bank. This is supported by Mrs W telling First Direct that she was making the payment on behalf of her son, whose phone had broken and whose online banking had been suspended. It doesn't seem likely to me that somebody who was trying to circumvent fraud detection systems would give an answer that carried so many hallmarks of the scam they were falling victim to. Rather I'm persuaded Mrs W was telling the truth and had no intent to mislead the bank in any way.

I'm not persuaded the significance of this seemingly innocuous question would have been sufficiently evident to her at that very moment. At the time, I don't think she was aware of why the answer mattered or the consequences of not pausing to think and give the most accurate answer she could.

Given the question was asked with no context around its importance, along with the eagerness she had to make the payments to help her child, I don't find Mrs W was grossly negligent here – nor do I find she was very significantly careless in the answer she gave. On the contrary, I find her answer understandable given the situation she was in at the relevant time, and in response to a closed question.

Neither do I find Mrs W was very significantly careless in any other relevant respects. That means I don't find First Direct is entitled to rely on exception R2(1)(e).

For completeness, under section R2(2) the CRM Code contains a provision applying where:

[...] during the process of assessing whether the Customer should be reimbursed, the Customer has acted dishonestly or obstructively in a material respect.

I don't think Mrs W was acting dishonestly in answering the agent's questions – at most she did so with a slight degree of carelessness, but I don't find this could fairly be classed as "dishonesty". In any event this clause cannot apply here. It refers to dishonest or obstructive acts occurring "*during the process of assessing whether the customer should be reimbursed*". Nothing I've seen suggests this is applicable here.

Could First Direct have done more to prevent the scam?

I am also mindful that when Mrs W made these payment, First Direct should fairly and reasonably have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud or financial harm.

When making the first payment, First Direct questioned Mrs W as to what had prompted her to make this payment. As mentioned above, Mrs W told First Direct that she was helping her son with a payment, as he'd got a new phone and his online banking facilities had been suspended.

The information that Mrs W had given here are classic hallmarks of what are often referred to as 'Hi Mum, Hi Dad' scams. Given the prevalence of this type of scam and in the context of the answers she gave, I think First Direct ought to have been concerned at this point to the potential that Mrs W may have been at risk of financial harm.

Given what it knew, First Direct would have been able to provide Mrs W with information about what to look out for in relation to these types of scam, what they look like and how they typically play out. I've seen no reason why Mrs W would not have listened to First Direct, after all it was the professional in these matters, and I think it more likely than not Mrs W would have recognised all of these hallmarks in what was happening to her and in the payments she was being asked to make. Mrs W isn't an expert in matters relating to fraud. So had First Direct done this, as I think it ought to have done, I think she would have heeded its advice, appreciated what was happening and I don't think she would have gone ahead to make the first, or subsequent payments.

I think this is supported by what happens later, when on the suggestion from a work colleague to try and contact her son, she did so and the scam unfolded. I've no reason to doubt that Mrs W wouldn't have done the same, had this course of action been recommended by her bank. Overall I think First Direct missed an opportunity to prevent the scam when it spoke to Mrs W ahead of her making the initial payment.

The relevance of this finding is that First Direct ought to have prevented the loss, rather than just reimbursed Mrs W under the provisions of the CRM Code. It follows that First Direct should pay Mrs W interest from the date of loss, rather than the date it decided not to refund her under the CRM Code.

Putting things right

For reasons explained above HSBC UK Bank Plc, trading as First Direct, should now:

- Refund Mrs W the money she lost, being £6,790 (less any money it has been able to recover from the beneficiary banks and already return to Mrs W).
- Pay 8% interest on this amount, from the date the payments were made to the date of settlement.

My final decision

My final decision is that I uphold this complaint against HSBC UK Bank Plc trading as first direct bank.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs W to accept or reject my decision before 16 January 2024.

Stephen Wise
Ombudsman