DRN-5343847

The complaint

Mr W complains that Starling Bank Limited ('Starling') hasn't refunded the money he lost after he fell victim to an authorised push payment ('APP') scam.

What happened

On 1 November 2023, Mr W received a call on his mobile from a third party ('the scammer'). The scammer said they were calling from Starling (who Mr W banks with) and the reason for the call was because Mr W's account had been compromised.

The scammer advised Mr W that to stop his funds being stolen, he would need to transfer them to a different account, specifically created to hold his funds securely, until his Starling account was safe to use again. Mr W followed the scammer's instructions and sent £1,390 at 10:34am to the account details he was given.

Mr W was told that his savings account with another firm ('Z') had been compromised too. Mr W transferred the balance of his savings account from Z to Starling, before making further payments from Starling to the scammer for £500.39 at 10:47am; and £49.40 at 10:50am.

The three scam payments resulted in Mr W losing £1,939.79 in total. All payments went to the same, newly created payee and the final payment reduced Mr W's balance to zero.

After the call ended, Mr W became concerned that the scammer might not have been genuine. So, Mr W called Starling, at which point he realised he'd been the victim of a scam.

Starling attempted to get the funds back from the beneficiary (the firm that received Mr W's money), but it was unsuccessful in recovering any of Mr W's money.

Starling said it wasn't going to refund Mr W because he hadn't followed Starling's fraud prevention warnings or done anything before making the payments to check the scammer was a genuine Starling employee.

Unhappy with Starling's response, Mr W made a complaint. Starling reiterated its decision not to reimburse Mr W and so he escalated his complaint to this service.

Our Investigator upheld the complaint in part. They thought liability for Mr W's total loss ought to be shared equally between Mr W and Starling. The Investigator recommended Starling reimburse 50% of *all* the money Mr W lost, plus 8% simple interest per year from the date of payment until the date of settlement. Mr W didn't respond, but Starling didn't agree.

As an agreement couldn't be reached, the complaint was referred to me to decide. I considered the complaint and issued a provisional decision. Within that, I reached a different outcome to our Investigator.

In summary, I said Starling wasn't responsible for the loss caused by Mr W's first two scam payments. However, I said Starling was equally responsible for the loss caused by Mr W's third scam payment – and I recommended a 50% refund of payment three, along with 8% simple interest per year on the refund, from the date of payment until the date of settlement.

Starling agreed with my provisional decision. Mr W explained that he was disappointed with the outcome but had no further information or evidence for me to consider. As a result, I haven't received any additional evidence or comments which I need to consider.

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, and as neither Mr W nor Starling have provided me with anything further to consider, I see no reason to depart from my provisional findings, which I'll reiterate below.

> "*I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.*
>
> *At the time Mr W fell victim to this scam, Starling was signed up to the Lending Standards Board Contingent Reimbursement Model ('CRM') Code, which required firms to reimburse customers who had been the victims of APP scams like this, in all but a limited number of circumstances. Starling says that one or more of those exceptions applies in this case.*
>
> *In addition to the CRM Code, at the time Mr W made the scam payments, Starling should fairly and reasonably have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst other things). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*
>
> *When the scam took place, Mr W had recently left home for the first time, to attend university. Mr W has argued that this made him vulnerable at the time of the scam. Under the provisions of the CRM Code, where an APP scam victim is deemed vulnerable – they can be reimbursed in full. So, I've considered whether Mr W was vulnerable at the time he fell victim to the APP scam.*
>
> *The CRM Code states at R2(3):*
>
> *"A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim to an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis.*
>
> *In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the Firm had previously identified the Customer as Vulnerable."*

I acknowledge that Mr W was only 19 years of age and naïve to what a bank impersonation scam is, or how one might happen. However, Mr W's explained that when the scammer asked for his personal and bank information, he questioned why the scammer needed this information. This demonstrates he was alert to the dangers of sharing confidential information with unknown third parties and the possibility of receiving scam phone calls.

As a result, I don't think Mr W was unable to protect himself from this type of scam at the time it happened. It follows that I don't consider him to be vulnerable and so he isn't entitled to a full refund of his loss under R2(3) of the CRM Code.

Starling also considers that under the CRM Code there is an exception to reimbursement.

The CRM Code states at R2(1):

"A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place…

(c) 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 with was legitimate…"

I've carefully considered Starling's representations about why it shouldn't have to reimburse Mr W's loss under the CRM Code. I'm really sorry to disappoint Mr W, but I think Starling has fairly established a valid exception to reimbursement applies in this case, specifically that Mr W made the scam payments without a reasonable basis for believing that the person with whom he transacted was legitimate. I say this for the following reasons:

• Mr W was called from a "No Caller ID" number, so the persuasive technique of number spoofing wasn't used to convince him he was speaking to Starling;

• the scammer had made several attempts to contact Mr W by phone and I think it would've been reasonable to expect Starling to have also messaged Mr W via his mobile app if it was genuinely trying to contact him urgently, as had been the case previously when Starling identified fraud on his account – however, Mr W received no genuine notifications from Starling during this time;

• although the scammer knew Mr W banked with Starling, by his own testimony the scammer had to ask Mr W his name, address, sort-code and account number (under the guise these were security questions) – so I can't say the scammer convinced Mr W they were a Starling employee by providing Mr W with his personal information;

• when Mr W reported the scam to Starling, he explained that at the time he thought it was unusual for Starling to be calling him, rather than communicating via his mobile app, describing the call with the scammer to Starling as "dodgy", which suggests he was sceptical about how he was being approached by the scammer;

• the scammer convinced Mr W his savings account with Z had been compromised, but I've been provided with no plausible explanation given to Mr W at the time as to how Starling would've known information about a completely separate business;

• the account Mr W sent his funds to was a personal account, in someone else's name and held with a different bank, but Mr W didn't question this; and

• when making the first scam payment, Mr W was shown warnings, relevant to the scam he fell victim to, which said Starling or any other bank would never ask him to move money to keep it safe. As the warnings addressed the specific circumstances Mr W was experiencing at the time, I think he reasonably ought to have considered these and questioned the scammer about why he was being told to act contrary to the warnings.

Taking the above into consideration, I don't find that Mr W had a reasonable basis for believing that he was making genuine payments at the request of Starling. As a result, I'm satisfied that Starling has demonstrated that it can refuse to reimburse Mr W under the principles of the CRM Code.

Whilst I've established that Mr W didn't have a reasonable basis for belief, I also need to consider whether Starling met its expectations under the CRM Code. Our Investigator argued that the first scam payment was out of character for Mr W and presented a scam risk to Starling, which required it to provide him with a warning which met the CRM Code definition of an "effective warning". Whilst Starling did provide Mr W with warnings when the payment was made, our Investigator wasn't of the opinion that the warnings met the standards set by the CRM Code.

Having reviewed Mr W's statements for the 12-month period prior to the scam occurring, I can see that a majority of the transactions were made online, via Apple Pay or using his debit card. The value of Mr W's typical payments is far less than the £1,390 value of the first scam payment. So, I can understand why our Investigator felt that the first payment demonstrated a scam risk to Starling at the time.

However, I can see that Mr W did also regularly make faster payments and some of those were for similar values to £1,390. Although those larger faster payments went to an existing payee, it makes the value and payment method of the first scam payment appear less unusual. Furthermore, Mr W received a positive confirmation of payee outcome, which will have given Starling reassurance that Mr W was paying an account in the same name of who he intended to pay.

I don't consider the first scam payment was so unusual that it reasonably ought to have given Starling cause for concern that Mr W was falling victim to a scam and so I'm not persuaded it needed to provide Mr W with an effective warning.

I accept that when the first scam payment was made, Starling did ask Mr W some questions to establish why he was making the payment and to provide him with warnings about scams. I haven't seen anything to suggest these questions were asked because Starling had any specific concerns about the payment, rather I think this was required because Mr W was paying a new payee. It's more likely than not that Mr W would've been required to answer these questions regardless of the value of the payment, as required by Starling's internal procedures for new payees.

Starling has provided a copy of the questions it asked, along with Mr W's responses. Unfortunately, Mr W wasn't truthful with his answers. As a result, Starling couldn't provide more specific warnings about bank impersonation scams and I wouldn't reasonably expect it to have brought to life how they work, when Starling wouldn't have reasonably been on notice that Mr W might have been falling for a bank impersonation scam.

In any event, Starling did provide several warnings about bank impersonation scams and the consequences of moving forwards and this information reasonably ought to have resonated with Mr W and affected his decision to go ahead with the payments. So, I don't agree that Starling was required to provide an effective warning when the first scam payment was made and I think the warnings it provided, in the circumstances, were proportionate to the apparent risk.

Whilst the second scam payment was Mr W's second payment to a newly created payee in the space of 13 minutes, I don't think a suspicious pattern of activity, indicative of an APP scam, was present which would reasonably require Starling to have provided an effective warning when scam payment two was made.

I don't think Starling needed to give an effective warning for scam payments one and two. So, I'm not persuaded it has failed to meet its expectations under the CRM Code when those payments were made. It follows that I don't think Starling can fairly and reasonably be held responsible for Mr W's loss caused by scam payments one and two.

Although the final scam payment was for under £50 and significantly less than the earlier two payments, it was Mr W's third payment to a newly created payee within 16 minutes. Not only was Mr W making multiple payments to a new payee in a short space of time (something he hadn't previously done), the third scam payment completely cleared Mr W's available balance – and it was the first time that Mr W had reduced his balance to zero in the previous 12 months. So, there were enough hallmarks of a bank impersonation scam that Starling ought to have done more to satisfy itself Mr W wasn't at risk of financial harm.

I think there was an apparent scam risk that Mr W might be falling victim to a bank impersonation scam when the third scam payment was made – and under the standards of the CRM Code, Starling reasonably ought to have provided an effective warning. However, Starling didn't provide any warnings for this payment and so I don't consider it met its expectations under the CRM Code.

I also think Starling reasonably ought to have gone further than simply providing a written warning. I'm persuaded the circumstances required human intervention from Starling to ask Mr W proportionate questions about his recent payment activity. Had this happened and the common themes of a bank impersonation scam been explained, I think the scam would've come to light and Starling would've been able to prevent Mr W making the final payment. For these reasons, I think Starling can fairly and reasonably be held jointly liable for Mr W's loss caused by the third scam payment.

Once it was aware of the scam, I can see that Starling notified the receiving bank within an hour, in an attempt to recover the funds Mr W had sent to the scammer. Unfortunately, Starling wasn't successful in recovering any of his funds. So, whilst Mr W did report the scam to Starling within a few minutes of the final scam payment taking place, I consider Starling met what was expected of it in terms of attempting recovery and it couldn't reasonably have done anything more to recover Mr W's loss.

Putting things right

As I've explained above, I'm satisfied that Mr W didn't have a reasonable basis for belief when making the scam payments. I'm also not satisfied that Starling failed to meet its expectations under the CRM Code for the first two scam payments. As a result, I'm not recommending Starling needs to reimburse any of Mr W's loss caused by those payments.

However, I don't think Starling met its expectations under the CRM Code when the third scam payment was made, and I also think it reasonably could've prevented the payment being made. So, Starling and Mr W should be held equally responsible for payment three and Starling ought to refund 50% of the payment – i.e., reimbursing Mr W with £24.70.

In addition to refunding £24.70, Starling should also pay 8% simple interest per year on the refund, from the date of payment until the date of settlement."

I have huge sympathy for Mr W and recognise that the loss he suffered, after being the victim of a cruel scam during his first year of university, was significant to him. However, after considering the circumstances of the scam, I think there were enough warning signs apparent to Mr W that I'm not persuaded he had a reasonable basis for believing that the person with whom he transacted with was legitimate.

I'm further satisfied that when Mr W made scam payments one and two that Starling met its expectations under the CRM Code. As a result, Starling can't fairly and reasonably be held responsible for the loss caused by those payments and Starling hasn't unfairly declined to reimburse scam payments one and two under the principles of the CRM Code.

However, it's my opinion that Starling did fail to meet its expectations under the CRM Code when payment three was made. I think Starling should've asked Mr W proportionate questions about his recent account activity and explained the common characteristics of safe account scams. Had it done so, I think the loss from scam payment three, more likely than not, would've been prevented. As a result, I think Starling can fairly and reasonably be held equally responsible for the loss from scam payment three.

Putting things right

To resolve the complaint, Starling should:

- refund Mr W £24.70 (50% of the loss from scam payment three); and
- pay 8% simple interest per year on the refund, from the date of payment until the date of settlement.

My final decision

For the reasons given above, and in my provisional decision, I uphold this complaint in part.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 20 March 2025.

Liam Davies
Ombudsman