DRN-3789659

The complaint

Mr F complains that Starling Bank Limited ("Starling") didn't do enough to protect him when he fell victim to a scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat them again here. Instead, I'll summarise what happened and focus on giving the reasons for my decision.

- In March 2022, Mr F was tricked into transferring funds to a scammer and into making card payments to a cryptocurrency exchange provider.

- Mr F was led to believe he was speaking to another bank before being passed over to Starling. He made these payments with the intention of protecting his funds and those of his girlfriend, after being misled into thinking his accounts had been compromised via his WiFi.

- After realising he'd been the victim of a scam, Mr F contacted Starling. While it contacted the beneficiary bank to try to recover the funds, it was unsuccessful. Starling believes it acted appropriately overall so hasn't agreed to refund the lost funds. Unhappy with this, Mr F complained to our Service.

- The investigator explained the Contingent Reimbursement Model ("CRM") code which Starling has signed up to – and that this would have applied to three of the payments made – as they were faster payments made to a third party. But she felt Starling had fairly applied an exception to reimbursement – namely that Mr F didn't have a reasonable basis for belief when making the payments. The remaining two payments didn't fall under CRM as they were card payments to a cryptocurrency exchange provider.

- Ultimately, the investigator didn't think Starling ought to have done more than it did as she didn't consider the overall activity significantly large or unusual. So, she didn't recommend that Starling refund the money. And she concluded it had done enough in terms of attempts to recover the funds.

- Unhappy with this, Mr F asked for a decision. Following this, he also made us aware of circumstances and health-related matters which he says left him vulnerable to the scam. So the complaint was passed to me to decide.

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 agree with the outcome reached by the investigator – I'll explain why.

It's not in dispute that Mr F has been the victim of a scam. But it's also not in dispute that he authorised these payments, albeit unaware that he was making payments to a scam. So I've first considered whether the three applicable payments should be refunded under the CRM code.

The CRM code says, in summary, that a customer who was vulnerable when they made an Authorised Push Payment ("APP") scam payment should receive a full refund of that payment, regardless of whether the firm knew about the customer's vulnerability before the scam took place. Vulnerability has a specific definition under the code, which isn't the same as other definitions (such as that of the financial regulator). The code says a customer is vulnerable if:

"*it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered."*

I've carefully considered the evidence I've been provided, as well as the point at which our Service was given the details of the vulnerability. And I'm not persuaded that Mr F couldn't reasonably be expected to have protected himself from the scam because of the vulnerabilities. The fact these circumstances were raised so late makes me think Mr F can't have seen these as key to his actions at the time. Nor do I think the circumstances he's raised rendered him unable to take steps to consider the scam risk. Having said that, there are further considerations under CRM besides vulnerability, which I'll move on to.

Under the provisions of the CRM code, both the bank and its customer have obligations. If it can be shown that the customer has met their requisite level of care, they will be fully reimbursed. If the customer has not done this, it's for the firm to show that it's met its obligations under the Code. The most relevant obligation for the firm is to provide an 'effective warning'. If a firm hasn't met its obligations, subject to any liability of the bank which received the money, it will be liable for 50% of the customer's loss.

In terms of whether Starling met its requirement to provide an effective warning, I don't consider that it did. But, having identified a potential risk, Starling asked Mr F a series of questions before processing the payments in relation to the purposes and recipients of the payments. Seemingly, Mr F was coached into providing incorrect responses to indicate that he was paying family or friends, that payments were for rent, bills and gifts – all of which were incorrect. But this means that Starling was *prevented* from giving an effective warning as it wasn't provided with answers to accurately reflect the situation. So, for this reason, I'm not persuaded Starling has failed to meet the standards set under the CRM Code in not providing an effective warning.

In terms of Mr F's obligations, Starling has argued that he made payments without a reasonable basis for belief that the person he was transacting with was legitimate. In thinking about this, I've noted the following:

- the caller purported to be from one bank before handing over to 'Starling';
- the caller talked about how the accounts had been compromised due to the WiFi;
- in attempting the keep the account safe, Mr F transferred funds to named people he didn't know;
- he was directed to enter in payment references such as "happy birthday" and "refurbishment" and to select that payments were being made to family members or friends;
- the confirmation of payees didn't match or couldn't be checked;
- Mr F was asked to transfer his girlfriend's funds too; and
- Mr F was provided with a warning stating that fraudsters tell customers how to

answer questions and that a genuine organisation would never ask a customer to move money to a new, 'safe' bank account.

Overall, I don't think I can fairly conclude that Mr F had a reasonable basis for belief on this occasion. While, individually, some of the points above would be reasonably believable, I'm not persuaded that the scenario as a whole was, when these are all considered in combination. Of particular relevance here would be the belief that Starling would ask Mr F to select incorrect payment purposes despite this linking through to its own systems, and direct him to make payments to payees with names besides his own – which then couldn't be verified. Also of relevance would be the belief that Starling would suggest that another individual give Mr F access to their funds. And that a warning reflecting the situation Mr F was in was presented to him but that he continued anyway. So, given all of this, I agree with Starling that the exception to reimbursement applies.

While I don't think the payments should be reimbursed under CRM, I've thought about the usual APP considerations for these payments. So, the starting position is that a bank is expected to process payments and withdrawals that a customer authorises it to make. But there are times where a bank might be expected to question a transaction, even though it might have been properly authorised. Broadly speaking, firms like Starling have certain obligations to protect customers from fraud.

Starling has said that it did consider the payments to have been unusual and that this prompted an additional review process before any payments were released. And, as a result, before each of the faster payments, Mr F was presented with the following warning:

"*Are you being told to make this payment? Anyone telling you what buttons to click, or asking you to read the text on this screen out loud is a criminal. You must not make the payment if you are being told how to answer the questions or explain the payment. Read each question carefully and answer truthfully, otherwise you could lose all the money sent."*

The evidence provided shows Mr F responded with "*I understand".*

Despite entering incorrect information, he was then provided with the following warning:

"*Fraudsters will tell you how to answer these questions to scam you. A genuine organisation will never do this. A bank or any other organisation will never tell you to move money to a new, 'safe' bank account. Fraudsters can make phone calls appear to come from a different number. Are you speaking with who you think you are? If in doubt you can call us…"*

Again, Mr F responded with "*I understand".*

I'm satisfied that Starling's intervention was proportionate and I don't think reasonable further or different attempts to intervene would likely have resulted in a different outcome – I think Mr F was under the spell of the scammer and would have proceeded regardless. The warnings, which largely matched the situation he was in, weren't enough to deter him from making the payments. And we already know that he provided false information under the instruction of the scammer.

Moving on to the card payments, I can see that two payments were made to a legitimate cryptocurrency exchange provider, so I wouldn't have expected the merchant to have been of concern to Starling. And neither payment was particularly large so I wouldn't have expected these to have alerted Starling to a potential fraud risk. But, crucially, given that Mr F had provided incorrect information when questioned on the earlier payments, I'm not satisfied that an intervention by Starling with these payments would have resulted in stopping Mr F from making these card payments.

For completeness, I would note that, for both payments, Mr F would have been presented with a message stating:

"*Starling will never contact you and ask you to use this screen. If someone is telling you to approve this transaction, please tap 'Reject Payment' and contact customer service."*

So, based on all the evidence I've been provided with, I don't think it would be fair to hold Starling responsible for any of these payments. I wouldn't expect it to have taken any further action in terms of intervening prior to processing the payments.

With regards to recovery, Starling contacted the beneficiary bank but was unable to recover any funds. And, in relation to the card payments, a chargeback would have been unsuccessful due to the scheme rules and the payments being made to a legitimate merchant. So, I'm satisfied that Starling did enough to attempt to recover the funds.

While I appreciate how disappointing this will be for Mr F, and I'm sorry he's been the victim of a cruel scam, I don't think it would be fair or reasonable to uphold this complaint. So, I won't be asking Starling to take any further action.

My final decision

For the reasons given above, I don't uphold this complaint against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 14 September 2023.

Melanie Roberts
Ombudsman