DRN-5480923

The complaint

Mr G complains that Starling Bank Limited ('Starling') hasn't reimbursed him in full after he fell victim to a scam.

What happened

I'll briefly summarise the facts of the case. Mr G says that on 26 July 2024 he received a call from an unknown number from someone who purported to be from Starling. He didn't know at the time, but the caller was a scammer. The scammer advised Mr G to look him up on a social messaging platform and sent Mr G a text from Starling's usual number. He told Mr G that fraud was suspected on his account and that it was compromised as a result, and that the funds in an external account were also at risk. Mr G transferred funds from his external account to Starling. Then, on the instructions of the scammer, Mr G made transfers of £4,001.99 and £1,301.99 to a safe account.

The scammer told Mr G that he would call back later that day. Mr G didn't receive a call and became concerned. He contacted Starling to report what had happened.

Starling said it could have done more to protect Mr G and Mr G also could have done more. It reimbursed all of the second payment (£1,301.99).

Mr G was unhappy with Starling's response and brought a complaint to this service.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. She said the Contingent Reimbursement Model Code ('CRM Code') doesn't apply to the scam transactions as they were made by card and no valid chargeback rights exist. The investigator thought that Starling acted reasonably in processing the first transaction, which is the only one now in dispute.

Mr G didn't agree with the investigator's findings and asked for a final decision. He said:

- He believes he completed all reasonable checks and explained why.
- He doesn't understand how the payments were made by card if they were made in the Starling app.
- He thinks the transactions are covered by the CRM Code and notes that the code doesn't exclude card payments.
- The first transaction was out of character, and he questions why the investigator said that the second payment was suspicious and the first wasn't.
- Starling should be held accountable because a scammer was able to hack or duplicate its messaging system.
- He questioned how the scammer got hold of his card details to request the payments.

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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice and, where appropriate, what I consider to have been good industry practice at the time.

I will first address the type of payments that were made from Mr G's account during the scam. Mr G believes that as the payments were made in the app, they can't be card payments, but this is incorrect. I have seen evidence which shows that I am considering card payments made within the app and that a 3DS challenge was applied on each occasion.

The investigator was right in saying that the CRM Code doesn't apply to card payments. The code sets out the payments that are covered by it, so does not need to specifically exclude card payments. It defines an APP scam as, "a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer…". This means that card payments aren't covered.

I've gone on to consider Starling's wider obligations. In broad terms, the starting position at law is that a bank such as Starling is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

I consider it fair and reasonable in July 2024 that Starling should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- 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 (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving and the different risks these can present to consumers, when deciding whether to intervene.

In this case, I appreciate that the first transaction was of a higher value than previous transactions on Mr G's account. But customers do from time to time make one off larger payments. There were also no other concerning factors at the time that might have alerted Starling to a heightened risk of fraud. A balance needs to be struck between Starling identifying potentially concerning payments, and responding appropriately to any concerns, and minimising disruption to legitimate payments. If all transactions like those made by Mr G were flagged by a bank for additional checks, many legitimate payments would be affected. So, I don't think Starling acted unreasonably in processing the £4,001.99 payment without taking any additional steps.

When Mr G made the second payment, I agree that Starling ought reasonably to have done more to protect him. It was the second payment to a new payee in a short space of time and the overall value of the transactions was more concerning. Starling has refunded this transaction in full, so I don't need to consider this point further.

Because I'm not persuaded Starling should have taken additional steps before processing the first payment, I don't need to consider Mr G's actions and whether he took reasonable steps to check the scammer was who they said they were.

Mr G has suggested that Starling should be liable because a fraudster was able to send him a text message from the number used by Starling. This doesn't mean that Starling's system was hacked though. It just means that a fraudster was able to use sophisticated techniques to persuade him to part with his funds. I can't fairly say that Starling should be responsible on this basis.

I don't know how the scammer got hold of Mr G's card details and this isn't something I need to decide.

For completeness, I've considered chargeback, which is a process that allows debit and credit card holders to reverse a transaction when there's a problem with the goods or services they have purchased. It is organised and run through the overarching card scheme but customers wishing to use the service must go through their card issuer (Starling in this case). The chargeback scheme is voluntary, and banks are not under any formal obligation to submit a chargeback claim. But this service's view is that it is good practice for a bank like Starling to make a chargeback claim where the right exists, timescales are met and there is a reasonable prospect of success.

In this case though, I consider that Starling acted reasonably in not raising a chargeback as there was no applicable chargeback reason, so no prospect of success. Mr G made a payment via an international money transfer service which provided the service expected – the money was transferred to the intended recipient. It wasn't the money transfer service which 'scammed' Mr G out of the funds, but any chargeback would need to be raised against it.

Overall, whilst I'm sorry to hear about this cruel scam and the impact it has had on Mr G, I can't fairly require Starling to do anything more.

My final decision

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 15 October 2025.

Jay Hadfield
Ombudsman