DRN-4874055

Complaint

T complains that Starling Bank Limited didn't pay a refund after it fell victim to a fraud. T is a limited company, and this complaint is brought on its behalf by one of its directors, Mr S. For the sake of readability, I've generally referred to Mr S throughout the text of the decision.

Background

In March 2023, Mr S was called by someone who claimed to be an employee of a bank which I'll refer to as L. The caller told Mr S that malware had compromised the security of his accounts. They speculated that he may have inadvertently downloaded a virus from an email attachment. They told him that the malware could compromise the security of all his accounts (even those held with other banks). He needed to ensure that he transferred his funds to a *"safe"* account. They told Mr S that the fraud team at L were collaborating with Starling to make sure that his funds were kept safe. Unfortunately, the caller wasn't a genuine employee of L, but a fraudster.

The fraudsters knew some details associated with his account at L and that there had been an attempt to make a payment using his card. To demonstrate their legitimacy, they sent a text message to Mr S that appeared in an existing chain of genuine messages he'd received from L. Mr S assumed this meant the message (and therefore the call) must've come from L. He wasn't aware that it was possible for the origin of a text message to be spoofed in the way that happened here.

The fraudsters asked him to download remote access software that allowed them to view his accounts. I also understand that at one point they made the screen on his device go blank. They explained that this was because they were carrying out a search on his system.

At the instruction of the fraudsters, Mr S made several payments to his Starling account from his account at L. He then attempted to move those funds onwards from the Starling account. Only one of those payments was successfully processed – a payment of £12,900.

Mr S says that the fraudsters guided him through the process. Starling asked him several questions about the nature of the payment. There were inaccuracies in his answers, although Mr S explains this by saying that he was answering based on the direction given by the fraudsters. Starling showed him two warnings during that payment process. The first said:

> *"Be wary of anyone guiding you through these questions. Is someone telling you how to send this payment, which buttons to tap, or asking you to read this screen? If so, you're talking to a scammer – cancel this payment and call us. Starling will never ask you to move money to keep it safe. If you send money to a criminal, you could lose it all.*

He then answered several other questions. The following warning was generated:

> *"Take a moment to think. 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. If you transfer money to a fraudster, you might not get it back. If you're not sure the payment is genuine, stop and call us …"

Once Mr S realised that he'd fallen victim to a fraud, he notified Starling. It didn't agree to refund him. It thought that it had provided Mr S with an effective warning about the risk of fraud and that he had gone ahead anyway. It didn't think it should be expected to refund him in those circumstances.

Mr S was unhappy with the response from Starling and so he referred his complaint to this service. An Investigator upheld it. The Investigator didn't think the warnings Starling gave were technically compliant with the Contingent Reimbursement Model (CRM) Code's definition of an *"effective warning."* But in any event, he concluded that Starling needed to do more here than simply provide a warning. The risk was sufficiently clear that it needed a human intervention, such as a telephone call to Mr S, to protect him from the risk of financial harm due to fraud.

Starling didn't agree with the Investigator's view. It pointed out that a warning told Mr S that, if someone was guiding him in how to answer the questions, he was talking to a scammer. It questioned what more it could've done or how the warning could've been more impactful. It also pointed out that the warning told customers that no bank will ask them to move money in this way. It thought this should have prevented the customer from making the payment.

As Starling disagreed with the Investigator's opinion, the complaint has been passed to me to consider and come to a final decision.

Findings

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

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, that isn't the end of the story. Starling has signed up to the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM code"). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one here, in all but a limited number of circumstances.

In addition to that, good industry practice required that Starling be on the lookout for payments that were out of character or unusual to the extent that they might have indicated a fraud risk. That requirement is in addition to the expectations placed on Starling by the CRM Code. On spotting a payment displaying such risk factors, I'd expect it to intervene in a manner proportionate to the risk identified.

The Investigator concluded that Starling needed to do more than simply display a written warning when Mr S authorised the payment. The possibility that the payment related to an APP scam was sufficiently clear that a human intervention, such as a telephone call to the customer, was a proportionate response to the risk.

I'd agree with that conclusion. While there were sizeable payments made from his Starling account in the months prior to the scam, this payment represented almost the entire balance and was being made to a new payee. It also coincided with significant movements of funds into his Starling account from his account with L in a manner that is consistent with a scam of this type. I think that payment should've been paused to allow Starling to make direct contact with Mr S. It could then have told him unambiguously that he'd been talking to a

fraudster and therefore prevented him from making the payment in question.

I've also considered whether it would be fair and reasonable for Mr S to bear some responsibility for his own losses here. In doing so, I've considered what the law says about contributory negligence, but also kept in mind that I must decide this complaint based on what I consider to be fair and reasonable in all the circumstances.

Overall, I'm not persuaded that Mr S was contributorily negligent here. The fraudsters had to take some steps to persuade him that they were calling from the bank – he doesn't appear to have simply accepted their explanations at face value. For example, the fraudsters sent him a text message that appeared as if L had sent it. Since Mr S wasn't aware that it was possible to spoof the origins of a text message in this way, he was reasonably persuaded that he was talking to a genuine employee of L. He's also pointed out that the fraudsters knew some basic information about his account with L, including his card number and that there was an attempted transaction to a fast-food takeaway. He'd assumed this information would only have been available to a genuine employee of the bank.

I've considered the content of the warnings he saw when making the payments. I agree that the text of those warnings is clear. If Mr S had the time to take on board and process their contents, I'd have expected it to have an impact on his decision making. But for that to happen, he needed the time and mental space to process what the warnings said. The evidence submitted by Starling suggests Mr S didn't spend very long looking at the warnings. Mr S has also told us that the scammers talked him through every step of the process. We know from experience that perpetrators of this type of fraud try to prevent consumers from pausing to think by talking continuously and repeatedly stressing the urgency of the situation. The recollections Mr S has given us suggests that was the case here and, as a result, it was inevitably more difficult for the warning to impact upon his decision-making process.

Overall, I'm not persuaded that Mr S was contributorily negligent and so it wouldn't be fair and reasonable for Starling to make deduction from the compensation it pays him.

Final decision

For the reasons I've set out above, I uphold this complaint.

If T accepts my final decision, Starling Bank Limited should refund the money lost to the fraud, less the sum it was able to recover from the receiving account. It should add 8% simple interest per annum to that sum calculated to run from the date the payment was made until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 25 July 2024.

James Kimmitt
Ombudsman