DRN-5709207

Complaint

Mr S is unhappy that Starling Bank Limited didn't refund him after he reported falling victim to a scam.

Background

In April 2024, Mr S received a phone call from an individual claiming to be a representative of Starling Bank. He was informed that suspicious activity had been detected on his account. He recalled having recently responded to a phishing text message purporting to be from a delivery company, and the caller suggested that this may have been the point at which his accounts were compromised.

Mr S didn't realise it at the time, but the caller was not a genuine employee of Starling but a fraudster. The individual took steps to appear as though they were securing Mr S's account, before warning him that an account he held with a different bank was also at risk. A little later, Mr S received a second call from someone claiming to be from his other bank. This caller advised him to transfer funds from that account into his Starling account, which they assured him was now secure. Acting on this advice, Mr S transferred £2,806.70 into his Starling account.

Once the funds had arrived, Mr S received a notification via the Starling app asking him to confirm or decline a payment to a third-party company. The amount was slightly higher than the amount he'd just transferred. The fraudster told him that the difference was due to an insurance premium that needed to be paid. Mr S was told the payee was an insurance company. The fraudsters had presumably already entered Mr S's card details with the third-party business. Mr S did not initiate the payment himself. He simply confirmed it within the app. He was reassured that the funds would be returned to his account within five minutes, and on that basis, he agreed to the payment being made.

Mr S realised immediately that he had been scammed and reported the transaction via the Starling app. Starling looked into things but didn't agree to reimburse him. Mr S wasn't happy with that and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. Mr S wasn't happy with the Investigator's opinion and so the complaint has been passed to me.

Findings

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

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 2017 and the terms and conditions of the customer's account. These regulations provide the framework for determining whether a payment has been authorised and, if so, the responsibilities of the payment service provider.

In assessing whether this particular payment was authorised, I have considered the evidence that the transaction was authenticated using Mr S's debit card details. It appears those details were obtained by the fraudsters, who then used them to initiate the payment. A payment can only be considered authorised if the customer consented to it. Importantly, the concept of consent in this context is not equivalent to informed consent. The test is whether the customer took an action that objectively indicated agreement to the payment being made.

In this case, Mr S did approve the transaction within the Starling app. Although he did so under a misapprehension as he believed the funds would be returned shortly and that his account would not suffer any loss. Despite that, he knew that funds would be transferred from his account, and he confirmed that instruction to the bank. I acknowledge that Mr S was misled and acted under pressure. However, the legal test for authorisation is objective and consent isn't invalidated simply because it was obtained through deception by a third party. On that basis, I am satisfied that the transaction was authorised within the meaning of the relevant regulations, and Mr S is therefore presumed liable for the payment in the first instance.

However, that is not the end of the matter. Starling has committed to following the Contingent Reimbursement Model (CRM) Code. Under the Code, victims of authorised push payment (APP) scams are reimbursed, unless an exception applies. However, the Code only covers anything that meets its definition of an APP scam. That means the payment needs to be *"a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer."* This was a debit card payment, and as such, it isn't covered by the CRM Code. Nonetheless, good industry practice requires firms to monitor for account activity or payments that are unusual or out of character and which might indicate a risk of fraud. Where such activity is detected, I would expect the firm to take reasonable steps to protect the customer. This could include providing a clear warning during the payment process or contacting the customer to better understand the circumstances.

The question, then, is whether Starling ought reasonably to have identified this payment as suspicious. While we now know with the benefit of hindsight that Mr S was being targeted by fraudsters, I am not persuaded that Starling had any reasonable grounds at the time to suspect that something was amiss. The value of the payment, while not insignificant, was not so high as to be inherently suspicious. It was somewhat out of character, but not to a degree that would necessarily trigger concern. Mr S has explained that he was under pressure from the fraudsters, and I accept that. However, this was not something the bank was aware of when it processed the transaction.

Overall, I'm not persuaded Starling did anything wrong in failing to intervene. I appreciate that will be a frustrating finding for Mr S. If it had intervened, there was a strong chance that the payment could have been prevented. But I don't think Starling had sufficient grounds to block the transaction or to contact Mr S to explore the wider context and so I don't think it erred in processing the payment without questioning it further.

I have also considered whether Mr S might have had a reasonable prospect of recovering the funds through a chargeback. The payee in this case was a payment remittance company, and the transaction was processed as a card payment. The service provided by the payee was to transfer the funds on to a designated recipient, and it appears that this was carried out. Given that the payment was authorised, and the associated service was performed, there wasn't any realistic chance of a chargeback succeeding.

I do not say any of this to diminish the fact that Mr S was the victim of a cruel and calculated scam. I have considerable sympathy for the position he now finds himself in. I also recognise that aspects of this decision may feel somewhat arbitrary, such as the fact that the CRM

Code doesn't apply simply because of the mechanism used to make the payment. However, I am required to apply the relevant rules as they are written, and I don't have the discretion to extend their scope, even in cases where I feel significant sympathy for the person bringing the complaint, as I do here.

Final decision

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 22 August 2025.

James Kimmitt
Ombudsman