DRN-4673933

The complaint

Mr N complains that Santander UK Plc (Santander) won't refund all of the money he lost when he fell victim to a safe account scam.

What happened

In August 2022 Mr N received a text which appeared to be from Santander, asking whether he had authorised a card payment to a well-known retail company. He replied to confirm he hadn't. Later that day, he received a follow-up call from who he believed was Santander – but who was actually a scammer impersonating the bank.

Mr N says the caller followed a verification process that seemed identical to Santander, and were also aware of a previous scam he fell victim to. So he believed it was Santander calling him back about the fraud attempt. They told him they would need to set up a new account and card number to protect his funds. Following which they instructed him to send his funds to a new account which they claimed to have set up for him.

After making a few payments, Mr N said something felt off. He then saw another call coming in, and so he ended the call with the scammer to answer it. The new call was genuinely from Santander, who had identified some of the account activity as suspicious. Through speaking to Santander, the scam was uncovered.

As well as the transfers Mr N made – which Santander has refunded under the Lending Standards Board's Contingent Reimbursement Model (CRM) code, which covers some transfers but not card payments – he says he also found out several card payments had been sent to a cryptocurrency merchant (C), which he wasn't aware of. Santander didn't agree to refund the card payments and instead suggested that Mr N contact the merchant.

Unhappy with Santander's response to his complaint about the payments, Mr N referred the matter to our service. Our investigator didn't uphold it. She thought the payments should be deemed authorised, as she couldn't establish how someone would have been able to get hold of his card details, as well as completing 3DS security – which required access to Mr N's mobile banking – without his knowledge or consent. She also considered if Santander ought to have identified the payments as suspicious at an earlier point, but ultimately thought it had been reasonable to allow the card payments to go through without further checking.

Mr N has appealed the investigator's outcome. He says a new device was registered on his account without him being aware, and he didn't make or agree to the payments, so he shouldn't be held liable for them.

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've reached the same overall conclusions to those of our investigator. I'll explain why.

Is it reasonable for Santander to treat the payments as authorised?

I've started by considering whether the payments should be considered authorised as under the relevant regulations – the Payment Services Regulations 2017 (PSRs) – Mr N would generally be liable for payments he authorises, whereas Santander would generally be liable for unauthorised payments.

If someone disputes making a payment, it's down to Santander to show that it was properly authenticated. In practical terms, that means it must show the correct payment procedure was followed. I'm satisfied Santander has done that. The records it has provided show the payments were made using Mr N's card details – but also by completing a "3D secure" check, requiring the payment to be confirmed via his online banking.

However, that in itself doesn't mean the payments were authorised. That comes down to whether Mr N consented to them. As the PSRs explain, consent must be given in the form, and in accordance with the procedure, agreed between Mr N and Santander. In practice, this means Mr N consents to a payment if he completes the agreed payment steps – such as entering his card details and completing the 3DS check.

Mr N can also consent for someone else (an agent) to complete payments on his behalf. And if he has permitted a third party to appear as if they have his authority to make payment transactions, those payments would generally be considered authorised – even if he didn't instruct the party to make any payments, and/or know that they were doing so.

It's this scenario – of whether an apparent agency relationship has been created – that I'm mainly considering here. Santander's information does suggest that Mr N's card details were used to initiate the payments from a different location. And that a new device was used to complete the 3DS checks. The key question is how the third party was able to gain the information and access needed to complete these steps.

The investigator asked Mr N about what happened during the call, to establish if he might have been tricked into giving away or displaying security information unknowingly. Mr N maintains he didn't share his card details. He also says he didn't download any applications etc. on his phone. Nor did he receive or share any texts or emails containing links.

In order to set up a new device on Mr N's account, a third party would have needed a code sent to Mr N's phone or in the app – in the latter case the account's login PIN would also have been required. As things stand, I can't see how someone would have been able to set up the device and make these payments without Mr N's involvement.

It's also important to consider the wider context of the scam Mr N fell victim to. It's clear Mr N knew/agreed that he would be moving funds from his account – it's just that he says he was only aware of/made the transfers, not the card payments. I do appreciate Mr N has been consistent in his testimony, and I'm satisfied he has provided full and honest recollections. But in the context of the scam, I don't think it's *more likely than not* that Mr N didn't do anything which gave the third party the appearance of authorisation. In those circumstances, I think it's fair to deem the payments to be authorised.

Are there any other reasons why Santander holds liability for Mr N's loss from the payments?

As mentioned above, Mr N would normally be held liable for authorised payments. But there are situations when it might be appropriate for Santander to have identified that a payment presented a fraud risk – and to therefore have taken additional steps before processing it. If Santander failed to do so when it should have, and those additional steps would have prevented the fraudulent loss, then it might be fair to hold it liable.

The type of scenario when Santander might have cause to complete further checks could be when a payment is significant unusual or uncharacteristic compared to the normal use of the account. I've considered whether that applies here.

Santander actually did identify the account activity as concerning at a point, as it rang Mr N – and that is what uncovered the scam. But the records I've seen show it triggered this response after the card payments had been made (although I appreciate the dates pull through differently on Mr N's statements). So, I've considered whether it should have taken this action sooner.

I do appreciate that the payments were going to a merchant Mr N hadn't paid before. And they were made in quick succession. On the other hand, they were being sent to a legitimate merchant. And the 3DS check gave some reassurance Mr N was *likely* making the payments.

Santander's primary duty under the PSRs is to process authorised payment instructions without undue delay. Thinking about the value and volume of payments banks like Santander process, there is a balance to be struck between reacting to indicators of fraud, and ensuring minimal disruption to legitimate payments.

Overall, while I appreciate the payments were arguably unusual for Mr N, I'm not persuaded they were so significantly risky, thinking about the overall amount sent at that point, that it was unreasonable for Santander to intervene after the sixth card payment – but not before. I therefore don't think it's fair to hold Santander at fault for not preventing the payments.

I agree with the investigator that Santander likely couldn't have recovered the funds either. As they were made by card, they fall under the scope of the voluntary chargeback scheme. But there are limited grounds to raise a successful claim, and I don't think they apply here. The payments were 3DS authenticated. And the dispute ultimately wasn't against the merchant paid directly – which is what a chargeback would consider – but the scammer.

I appreciate this will be disappointing for Mr N, who has clearly lost out to a cruel and sophisticated scam. My role is to look at Santander's liability for what happened, bearing in mind it wasn't the bank who perpetrated the scam. Having carefully considered what's happened here, I'm not persuaded it would be fair to direct Santander to reimburse Mr N for his outstanding fraudulent loss.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 16 April 2024.

Rachel Loughlin
Ombudsman