DRN-4467244

The complaint

Mr H complains that Santander UK Plc ("Santander") won't refund payments totalling £30,900 made from his account that he says he didn't authorise.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Mr H disputed several payments that had been made from his Santander account between 13-24 January 2023. The payments were made to another electronic money wallet held in Mr H's name. Some of the money originated from his savings account, but the vast majority of it had been funded by two loans that had been paid into his account from third party lenders.

The funds were then transferred on from his E-money account to a crypto wallet, where it was then taken by the scammer. Mr H said this happened after his wife used his email address to register her interest for an investment opportunity she found on social media (with what is now known to have been a fraudulent broker

Mr H also said he only made enquiries for the loans and saved them as quotes. He said he never completed the loan applications and thinks a third party was able to gain access to his computer and bank accounts to obtain the loans and pay the money out of his Santander account without his knowledge or consent.

Mr H disputed the payments with Santander, and it was able to recover £2,985.43, which it credited back into Mr H's account on 30 January 2023. But it said it wouldn't refund the remaining balance as it didn't consider the payments to be unauthorised. Unhappy with this, Mr H referred the matter to our service.

Our investigator didn't uphold the complaint. She didn't think there was a plausible explanation for how a third party could have made the payments without Mr H's knowledge or consent. She also didn't think an intervention would have likely prevented the payments from being made, so she didn't think Santander had to refund the disputed payments. Mr H disagreed, so the matter has been escalated to me to determine.

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 conclusions reached by the investigator and have decided not to uphold it. I'll explain why.

Having considered the facts before me as well as the relevant law, it seems to me that the key question I need to determine here is whether it is more likely than not that Mr H authorised the transactions. In other words, I need to decide whether Mr H made the transactions himself or gave someone permission to do so. This is important because a customer will usually be liable for payments they've authorised and, generally speaking, a

bank will be liable for any unauthorised payments.

In this instance, Santander has shown that the payments made to Mr H's E-money account were made via open banking and authorised via a One Time Passcode (OTP). This passcode was sent to Mr H's mobile phone for each transaction, where the payments were then completed on his E-money account.

Mr H said that prior to the disputed payments, his wife used his email address to register her interest for an investment opportunity she found on social media (with what is now known to have been a fraudulent broker). But Mr H said she didn't disclose any of his passwords or banking security credentials to the broker. So, while this may explain how a potential scammer would've known his email address, it doesn't explain how they would have been able to access his email account, computer, or online banking.

After investing, Mr H said he received emails with a link to view his profits. He said that he clicked on this link and wasn't asked to submit any details or security credentials, but that he saw his PC mouse and screen moving as though someone was controlling his computer, following which the payments were made from his account. So, Mr H submits that a scammer had managed to install remote access software onto his computer, which they used to then apply for the loans he had saved quotes for, and then gain access to his E-money account to make the Open Banking payments he has since disputed.

Even if this did explain how a scammer was able to access his computer (of which there's no evidence to substantiate), it still doesn't explain how a scammer would have been able to gain access to his mobile device to obtain the OTPs needed to authorise the payments, which was in Mr H's possession and protected by Face ID. I've seen no persuasive evidence to suggest that Mr H had any remote access software downloaded on his phone. So, there's seemingly no plausible explanation for how his details came to be compromised or the OTPs intercepted and subsequently used to make the payments.

Mr H says he doesn't recall receiving the OTPs, but Santander has confirmed that no new devices were registered to Mr H's online banking at the time, and there's nothing to suggest they were sent to a different device. I can see the number they were sent to also matches the number Mr H uses now. So, again, there's no reasonable explanation for how the payments were authorised using OTPs sent to Mr H's phone if no one else had access to it.

The disputed activity also occurred over a period of 11 days, which wouldn't be consistent with an unauthorised party gaining access to an account or security credentials to make payments. Typically, a scammer would seek to pay out as much money from an account as possible before the victim has time to realise that their account had been compromised. But in this instance, the activity was spread out over almost two weeks, during which time I can see that Mr H's online banking had been logged into. And given the significant amounts being paid into and out of the account, it's hard to see how he wouldn't have noticed these transactions when he logged in, yet they weren't reported at that point.

The money was also going to another account in Mr H's name, which also wouldn't be typical of this sort of fraud, as there would be little reason for a scammer to transfer money to another account before transferring it to themselves. It also seems implausible and far too much of a coincidence to think that the scammer had gained access to Mr H's computer at the very time he had started completing loan applications, for them to then go on and complete them.

Overall, given Mr H didn't share his details with anyone else, and due to there being little evidence of someone applying for loans and gaining access to all of his security credentials through remote access software, the only plausible conclusion is that either Mr H carried all

of this out himself, or gave his details to somebody else, thereby giving his consent and authority for payments to be made on his behalf. I appreciate that Mr H disputes this, but I'm afraid there is no other more plausible explanation for how the payments could have otherwise been made. He has said that it could have been malware on his computer, but as I've set out above, there's little persuasive evidence to corroborate this, and it still wouldn't fully explain how the payments were made in any event.

So, for the purposes of this complaint, I'm satisfied that the payments were likely authorised by Mr H.

Should Santander have intervened and questioned Mr H about the payments?

I've also considered whether Santander should have spoken to Mr H about any of the payments, as there are some situations in which a firm should reasonably have had a closer look at the circumstances surrounding a particular transfer. For example, if it was particularly suspicious or out of character.

And given some of the amounts being paid out of Mr H's account, it's arguable that Santander should have made further enquiries. However, even if it had, I don't think there's enough persuasive evidence to determine that this would have likely stopped any further payments being made from Mr H's account. I'll explain why.

The payment activity from Mr H's account, and the loan applications made in his name, all bear the common hallmarks of someone who has fallen victim to an investment scam. This includes multiple payments being made to another e-money account in the customer's name, with the funds then being sent on to a cryptocurrency account, as well as loans being applied for with multiple lenders in order to finance further investment.

I appreciate Mr H denies that he did this, but he said that his wife used his email address to register her interest for a fraudulent investment opportunity she found on social media, which he eventually invested his money with.

As I've set out above, I think it's more likely than not that Mr H authorised the disputed payments, as there's no other plausible explanation for how they could have otherwise been made. And in the context of him having said he had invested with a fraudulent broker, along with the payment activity being typical of an investment scam, I think it's more likely than not that this is how the payments came to be made by Mr H.

However, Mr H hasn't been forthcoming with any further details about how this scam unfolded. So, it's not possible for me to reasonably determine whether any intervention by Santander would have likely prevented any further loss to the scam. There's also evidence to suggest that Mr H had been questioned by another firm about the payments being made from his E-money account, where he said that he was helping some friends and family out with some money, rather than saying he was investing it. Mr H denies that this came from him, but it was sent from his correct email address, and there's little evidence to suggest that his email account had been compromised.

So, I think it's more likely that this response was sent from Mr H, which demonstrates that he wouldn't have likely been forthcoming with the true nature of the payments he was making, even if Santander had questioned him. As a result, I don't consider Santander can fairly or reasonably be held liable for failing to prevent the scam in these circumstances.

I also don't think there was anything more Santander could've done to recover the money either. It made efforts to recover as much as it could when Mr H disputed the payments, and was able to recover £2,985.43. But given this was all that remained, there's nothing more it

could have done to recover the remaining funds, given it had already been transferred out of the receiving account.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 17 May 2024.

Jack Ferris
Ombudsman