

The complaint

Mr R and Mrs H complain Santander UK Plc (Santander) won't refund the money they lost when Mrs H fell victim to a scam.

What happened

Mrs H was looking for work when she was contacted via a messaging app about a job opportunity. This involved completing tasks on a website/online platform. Mrs H thought she had to simulate sales to boost the algorithm for those products. And she was directed to send cryptocurrency to the platform in order to simulate the sales and "unlock" tasks. Unfortunately, this was actually a scam.

Between April 2023 and early May 2023, Mrs H sent over £60,000 to the scam from two other accounts. She then sent the following payments, totalling almost £39,000, from the Santander account she holds with Mr R:

- Payment one: £6,825 to "Individual One" on 4 May 2023
- Payment two: £5,950 to "Individual One" on 4 May 2023
- Payment three: £25,000 to "Company One" on 4 May 2023
- Payment four: £1,120 to "Individual Two" on 5 May 2023

Mrs H has explained these payments were to purchase cryptocurrency. She paid the sellers, who then loaded the cryptocurrency to her (genuine) cryptocurrency wallets. From there, she sent the funds on to the scammers.

When the scammers kept instructing her to pay further amounts in order to withdraw her earnings from the platform, Mrs H realised she had been scammed. In June 2023, Mrs H complained (via a professional representative) to Santander. She said it should have realised the payments were potentially fraudulent. And if it had intervened appropriately, it would have realised she was being scammed.

Santander didn't agree to refund Mrs H, so she referred the matter to our service. Santander then told us it had managed to recover over £7,000 from one of the recipients, which it had credited back to Mrs H. But it wouldn't refund the remainder of her loss. It said it had spoken to her about the payments to Individual One and she had misled it about what she was doing – claiming she was paying a friend to build a website for her, and had received an invoice for the work.

Our investigator didn't uphold the complaint. He thought the Lending Standards Board's Contingent Reimbursement Model (CRM) code applied. This is a voluntary code that generally requires firms who are signed up, including Santander, to refund victims of Authorised Push Payment (APP) scams – unless certain exceptions apply.

One such exception is where the consumer doesn't have a reasonable basis for believing they are transacting with a legitimate business/for legitimate purposes. The investigator thought that applied here – and also thought Santander met its standards under the code. He also agreed with Santander that Mrs H hadn't been honest about what she was doing, hampering its ability to uncover the scam.

Mrs H appealed the investigator's outcome, so her case was passed to me to decide. She said she didn't have an explanation for paying a "foreign entity" (Company One) if Santander had asked her about this – which it should have done, because the payment was very unusual for her. She also said the scammer told her a merchant page would be developed for her, which is why she said the payments to Individual One were for a website.

I contacted Mrs H for some further information. She provided records of her written contact with the scammers, along with records showing the payments being credited to, and sent on from, her cryptocurrency accounts.

Mrs H also explained that one of the other accounts she used questioned her about the scam payments – and the scammers advised her to say some were for graphics and some were payments to friends. She said the scammers also told her they would be sending her an invoice for her own website.

I then issued my provisional decision in May 2024, explaining why I wasn't minded to uphold the complaint:

Banks have a contractual duty to make payments in compliance with customers' instructions. So, as Mrs H authorised these payments – albeit she was tricked into doing so by the scammers – the starting position is that she is liable.

The investigator considered if Mrs H was due a refund under the terms of the CRM code. However, I'm not doing so as I've found the code doesn't apply here. The CRM Code only applies to certain types of payments made, in pounds sterling, between accounts based in the UK. It doesn't apply to payments made to another account the consumer holds, or payments to fund genuine purchases.

Here, I understand the payments were used to make genuine cryptocurrency purchases, which were then loaded to Mrs H's own cryptocurrency wallets. And the payments to the scammer were made in cryptocurrency. The CRM code therefore doesn't apply here.

I've thought about whether there are any other reasons why Santander ought to be held liable for Mrs H's loss. Although Santander has a duty to execute authorised payment instructions without undue delay, I would also expect it to be on the look-out for the possibility of fraud or scams and have taken additional steps, or made additional checks, before processing payments in some circumstances – as in practice all banks, including Santander, do.

If Santander failed to identify and/or respond appropriately to an apparent fraud risk, I'd need to consider whether appropriate action would have prevented (some of) the fraudulent loss. If it likely would have done, it might be fair to expect Santander to refund Mrs H and Mr R.

It's apparent Santander did have concerns by the time of the second payment to Individual One, as it blocked the payment in order to speak to Mrs H about what she was doing. I've listened to this call to consider whether Santander did enough.

Santander questioned Mrs H about what she was doing, and she said she was paying a friend to build a website for her. Santander told Mrs H during the call that if anyone had asked her to lie or mislead the bank – including about the payment purpose – that would be a scam. She told it that wasn't what had happened.

Mrs H has since said she thought the scammers would be building a web page for her, seemingly to explain what she told Santander. But having considered her explanation, I'm still not persuaded she was being honest during the call.

Mrs H specifically told Santander she had received an invoice for the work. She has now confirmed she didn't receive one, but was expecting to. The circumstances of the scam also don't appear to fit with her telling Santander the recipient was a friend, or that she knew others who had used their services. I also haven't found any reference to Mrs H chasing up the invoice, or asking about the website page, in her written contact with the scammer.

Regardless of whether Mrs H thought she was being truthful about what she was doing, I don't think it would have been obvious to Santander that she was falling victim to a scam. Based on what it was told, Santander understood Mrs H was paying a known person for work which she had received an invoice for. There was no mention of her sending the funds to cryptocurrency, or that it was linked to work she was doing which involved completing tasks.

Despite not being given much information relevant to the scam Mrs H was falling victim to, Santander still issued relevant warnings – such as about the scam risk if she was being told to lie about what she was doing. Yet Mrs H made it clear she wanted to proceed. In those circumstances, I don't think Santander can be held at fault for not uncovering the scam at this point.

I've considered what Mrs H has said about why she thinks Santander should have questioned her about the next payment. I do agree that, given the size of the payment, it probably should have prompted further questioning from Santander. It looked uncharacteristic compared to how Mrs H – and Mr R – normally used the account.

As this payment went to an account linked to a company based abroad, Mrs H says she wouldn't have had an explanation for why she was paying them. But she has also told us she followed the scammer's directions on other occasions about what reason to give for payments to the scam. In addition to what she told Santander about the website payment, she has also confirmed the scammers told her to tell another account provider that scam payments were to pay friends, and/or for "graphics".

In those circumstances, it seems likely to me Mrs H would have been similarly guided by the scammers if Santander had asked her to call to discuss this payment. I can't see why the account name means the scammers wouldn't have been able to provide a cover story. I also don't think the recipient account name would have made the scam obvious. Based on what Mrs H has told us, the recipient paid was legitimate – as they sold her cryptocurrency, which she then sent on to the scam.

While Mrs H says I can't presume how this call would have gone – she's asked me to make a finding on whether Santander is liable for her loss. That involves making a judgment on whether it's likely any mistakes by Santander contributed to her loss. Deciding to uphold the complaint would therefore require me to presume that a call would have uncovered the scam. So, in order to decide this case, I can't avoid making a judgment on how I think that call would have gone.

Overall, for the reasons I've set out, I'm not persuaded further intervention by Santander would have uncovered the scam. I've also seen records that Santander acted promptly to recover the funds once it got Mrs H's permission to contact the recipient banks – and was able to recover over £7,000. Given what we now know about the recipients, it also seems unlikely they were complicit in the scam – as it appears they provided Mrs H with legitimate services (cryptocurrency purchases). So if Santander hadn't taken recovery steps, I'd likely consider that reasonable.

I appreciate this will be disappointing for Mrs H and Mr R, who I appreciate have lost a lot of money to this scam. But having carefully considered all the circumstances, I'm not persuaded the loss they are claiming for was caused by Santander's errors. I therefore don't think it would be fair to expect it to refund them.

I invited both parties to provide any further comments before I made my final decision. Santander hasn't provided anything further, and the deadline I set has now passed. Mrs H responded to raise the following arguments:

- Santander should have picked up that the £25,000 was going to a “foreign entity”, and if so that would have rung alarm bells with her. Her professional representative (who stopped acting for her following the investigator's view) told her other banks have flagged payments to this entity as fraudulent.
- She did chase the scammers for the website invoice, that is just not shown in her written correspondence.
- If Santander had called Mr R as the joint account holder, he would have realised something was wrong. She says we can't assume how a call with him would have gone, and he didn't hear from the bank once.

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 decided not to uphold it. That is largely for the reasons given in my provisional decision, as set out above and which also form part of my final decision. So, I'll focus here on responding to the points raised by Mrs H following receipt of my provisional findings.

I've considered Mrs H's points around why she thinks the scam would have been uncovered if Santander had flagged the £25,000 payment. I appreciate she says she would have been concerned about the payment being sent to a “foreign entity”. But from what I've seen, the payment was sent in pounds sterling. And the recipient account provider who Santander attempted to recover the funds from is also regulated in the UK. So, I don't think the payment destination made it obvious there was a “foreign” connection.

From having looked up the recipient name used, and knowing that Mrs H was purchasing cryptocurrency, I do think there is a likely connection with a (genuine) company based abroad. But as Mrs H was the one to make the payment by transfer, it was her who would have entered all the recipient details. As the recipient name was already known to her, I don't think it would have been cause for alarm if mentioned during an intervention call.

From what I've seen, I'm also satisfied the recipient paid was legitimate. As mentioned, it appears the payment was used to purchase cryptocurrency via a genuine merchant. Mrs H has confirmed she received cryptocurrency from this transaction which she sent on to the scam. So again, if Santander had spoken to Mrs H, I'm not persuaded the recipient alone would have made it obvious she was falling victim to a scam.

It may also be helpful to explain that a bank isn't expected to play amateur detective and carry out extensive research into a recipient its customer chooses to pay. But if a payment looks particularly unusual – as I think the £25,000 did – I would expect a bank to contact its customer to find out more about the circumstances in which they were making the payment. I would expect them to be guided by the responses given to better assess if there was a likely fraud risk – and to warn the customer if so.

Based on how Mrs H responded to the earlier intervention call, and what she has told us about her contact with other banks, I'm not persuaded she would have responded to contact about the £25,000 transfer in a way that made the scam risk clear to Santander. While she says she didn't have an explanation for this payment, I consider it likely the scammers would have prompted her on what to say if it had been flagged. And this explanation would have been designed to minimise the apparent scam risk.

This is because Mrs H has already told us the scammers guided her on what to tell the provider of another account which she used to send money to the scam – such as saying she was paying friends or paying for graphics. That suggests Mrs H was seeking input from the scammers on what to say about the payments.

While Mrs H maintains she *did* think the scammers were building her a website, it's still clear she was untruthful during Santander's intervention call – in a way that made the risk less obvious. Such as claiming she had an invoice for the work, when she didn't.

As previously explained, I also find it hard to reconcile this explanation with the nature of the scam and the lack of records to support that she was expecting this website. I appreciate it's possible this could have all happened over calls and not have been mentioned in any of the written communication. But what I'm deciding is what is more likely. It does seem unlikely to me that, if Mrs H was chasing up for something she hadn't received, there would be no written record of this. By contrast, I can see her chasing up payment of her balance.

Mrs H has also questioned why Santander didn't speak to Mr R about these payments as the joint account holder. But Mrs H is authorised on the account to make payments directly; payments don't require sign-off from both account holders. So I can't see why Santander would have had cause to speak to Mr R directly. And if it had flagged the £25,000 payment for further checks, it seems more likely Mrs H would have been the one to respond – as happened when Santander flagged the earlier payment.

I appreciate this will be disappointing for Mr R and Mrs H. But having carefully considered all the circumstances, I'm not persuaded it's likely Santander would have uncovered the scam if it had intervened further. I therefore don't consider it fair to direct Santander to reimburse them for the money they lost to this scam.

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 R and Mrs H to accept or reject my decision before 26 July 2024.

Rachel Loughlin
Ombudsman