

The complaint

Ms B complains that Santander UK Plc ('Santander') won't refund the money she lost as the result of a scam.

What happened

In 2022, Ms B was contacted by someone who said they worked for Santander. They said Ms B's account had been compromised and three high value transactions had been attempted on her account. The scammer told Ms B to safeguard her money she needed to move it to another account.

Unfortunately, this was a safe account scam, and the caller didn't work for Santander.

Ms B made the following payments on the instructions of the scammer.

Date	Details of transaction	Amount
21.7.2022	Transfer to a cryptocurrency wallet in Ms B's name	£9,000.00
21.7.2022	Transfer to M – an individual	£4,110.01
21.7.2022	Transfer to K – an individual	£3,980.01

During the last call with the scammer, Ms B asked how she would access the funds she had transferred, and the call was ended.

Through a professional representative, Ms B raised a fraud claim with Santander in April 2025. Santander refunded 100% of the last two payments Ms B made, under the Contingent Reimbursement Model Code, but declined to refund the first payment. Santander say as the first payment went to an account in Ms B's own name, they're not liable.

Ms B wasn't happy with Santander's response and brought a complaint to our service.

An investigator looked into Ms B's complaint and upheld it. The investigator felt Santander should've been concerned and intervened on the first payment. If they had, the investigator felt the loss would've been prevented. So, they felt Santander should be liable for 50% of all the payments Ms B made – meaning they had to refund an additional £2,509.99.

Santander disagreed with the investigator's view and raised the following points:

- They don't understand why we're only recommending a refund of 50% on the last two payments.
- They don't agree they are liable for the first payment as it was made to an account in Ms B's name using an existing payee, which reassured them. Also, as the funds were moved on to the scammer from the cryptocurrency wallet, the loss occurred on that platform and Santander aren't liable
- They disagree that a warning would've prevented Ms B's loss on the first payment, as she selected the payment purpose "paying for a service". So, the warning provided wouldn't have been relevant to a safe account scam.

As the case couldn't be resolved informally, it was passed to me to review.

Having reviewed the case, I reached the same overall outcome as the investigator but with a different redress recommendation. So, I issued a provisional decision explaining why and giving both parties a chance to respond before a final decision was issued.

My provisional decision

In my provisional decision "What I've provisionally decided – and why" section, I said:

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account. It's not in dispute that Ms B authorised these payments, although she did so not realising she was the victim of a scam.

The last two payments Ms B made to M and K

Santander are a signatory to the CRM Code which requires firms to reimburse customers who have been the victims of APP scams like this, in all but a limited number of circumstances.

The starting position under the CRM Code is that the customer is entitled to a full refund unless the bank can establish that an exception to reimbursement applies.

Santander haven't said that an exception to reimbursement applies, so Ms B is entitled to a full refund of the last two payments – which Santander have already provided.

As Ms B has already been refunded in full under the CRM Code, I don't need to consider the point she has raised regarding her vulnerability – as she's already received the maximum refund for these two payments.

The first payment Ms B made

The CRM Code only applies where the customer has transferred to an account not held in their own name. As the first payment was transferred to a cryptocurrency wallet held in Ms B's name, I can't apply the CRM Code to that payment.

But, taking into account relevant law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that Santander should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud. This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by

maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment; · have been mindful of – among other things – common scam scenarios, how fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

While I appreciate that the first payment was made to an existing payee, the payment was significantly out of character compared to Ms B's usual account activity and it was identifiably going to cryptocurrency.

In the prior eight months, Ms B had only made one payment higher in value than this payment. That was a transfer to another account held in her name for £80,000. However, this was a one-off payment and usually the payments out of Ms B's account were for £3,000 or less. Also, Ms B didn't regularly purchase cryptocurrency, and cryptocurrency is commonly associated with scams. So, this payment of £9,000 was sufficiently unusual that I'm satisfied Santander should've identified a potential risk of financial harm from fraud and intervened.

I think the appropriate response would've been for Santander to have called Ms B to discuss the payment, before allowing it to go through. If Santander had called it's more likely than not the scam would've been uncovered, as Ms B believed she was already on the phone with Santander. Also, while Ms B received numerous calls from the scammer, she said they were reasonably short calls over an extended period of time. So, I think it's more likely than not Santander would've been able to get in touch with Ms B to discuss the payment.

I have taken into account that Ms B remained in control of her money after making the payment from Santander. It wasn't lost until Ms B took further steps. But Santander should still have recognised that Ms B was at risk of financial harm from fraud, made further enquiries about the first payment and ultimately prevented Ms B's loss from that point. So, I think Santander can fairly be held responsible for Ms B's loss in such circumstances.

But I also have to consider whether Ms B could've mitigated her loss and should share responsibility for the loss of her first payment.

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

Having done so, I think it's fair for Ms B to share responsibility for her loss on the first payment and reduce the refund by 50%. I say this because:

- Ms B says the scammer asked if she had a Bitcoin account and asked her to transfer funds to that account to safeguard her money. Ms B should've been concerned that she was being asked to purchase cryptocurrency and was then asked to move the money on to another individual. I can't see there was any reasonable explanation as to why she had to purchase cryptocurrency or why that cryptocurrency had to be sent to a third party.
- The scammer's ID on Ms B's phone said Santander, and Ms B says they knew her name and address. But it doesn't appear that the caller completed any of the usual security checks that would be done when a bank calls its customer.

I appreciate that safe account scams are successful predominantly because they play on a customer's fear that their money is at risk and the sense of urgency that is created by the scammer. However, Ms B says she received calls over a 14 hour period and that there were numerous short calls made during this time. So, she had the chance to stop and think about what she was being asked to do. And, based on the concerns that I've highlighted above, I would've expected Ms B to have asked more questions before making these transfers.

On that basis, I'm satisfied that it's fair for Santander and Ms B share liability for the loss on the first payment and ask Santander to refund 50%.

As Ms B has been without the use of these funds, it's fair for Santander to pay 8% simple interest per year on the refund of the first payment. This interest should be calculated from the date the payment was made until the date of settlement.

My provisional decision was that I intended to ask Santander UK Plc to refund 50% of the first payment Ms B made, being £4,500, and pay 8% simple interest on the refund.

Responses to my provisional decision

Ms B responded to say she accepted my provisional decision.

Santander disagreed with my provisional decision and raised the following points:

- The first payment was being made to an account in Ms B's name using an existing payee – which would've reassured them that it was genuine. There wasn't any information available to Santander to suggest they should've been concerned in relation to the first payment.
- The loss didn't occur when the funds were moved from Ms B's Santander account, the loss occurred when the funds were moved out of the cryptocurrency wallet – so Santander aren't liable for the loss.
- We can't predict how a conversation with Ms B would've gone if Santander had intervened.

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.

Where there is a dispute about what happened, and the evidence is incomplete or contradictory, I've reached my decision on the balance of probabilities. In other words, on what I consider is more likely than not to have happened in light of the available evidence.

Having carefully considered the points Santander have raised, I've reached the same outcome as in my provisional decision – I'll explain why.

While the first payment was made to an existing payee, I can see that Ms B had only made two other payments to this payee in the prior 12 months. These were payments made in December 2021 for £500 and £1,000. This wasn't a payee that Ms B used regularly, and the other payments were for significantly less than the payment made in July for £9,000.

Santander say that because the funds were going to an account in Ms B's name they were reassured. However, Santander should've been aware of multi-stage scams, whereby customers transfer funds between accounts in their own names, before moving the funds on to an account controlled by the scammer. So, the fact that Ms B was making the payment to

an account in her own name, doesn't mean Santander shouldn't identify a potential risk of financial harm from fraud.

Based on the size of the payment and that it was identifiably related to cryptocurrency, I'm still satisfied that Santander should've identified a potential risk of financial harm and intervened when the payment was made.

As Ms B believed she was already in contact with Santander as part of the scam, I'm satisfied that it's more likely than not contact from the real Santander would've uncovered the scam and Ms B would've realised that Santander wasn't asking her to transfer the funds. So, I'm satisfied that intervention by Santander would more likely than not have prevented Ms B from making the first payment.

Santander say as the loss occurred from Ms B's cryptocurrency account, they aren't liable. I have taken into account that Ms B remained in control of her money after making the payments from Santander. It wasn't lost until she took further steps. But Santander should still have recognised that she was at risk of financial harm from fraud, made further enquiries about the first payment and ultimately prevented her loss from that point. So, I'm satisfied that Santander can fairly be held responsible for Ms B's loss in such circumstances.

As I haven't been provided with any new evidence or arguments, I'm still persuaded that it's fair for Ms B to share responsibility for her loss on the first payment – for the reasons given in my provisional decision. So, Santander should refund 50% of the first payment.

Putting things right

To put things right I require Santander UK Plc to:

- Refund 50% of the first payment that Ms B made, being £4,500
- Pay 8% simple interest on the refund, calculated from the date Ms B made the first payment until the date of settlement.

My final decision

My final decision is that I uphold this complaint against Santander UK Plc and require them to reimburse Ms B as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 13 January 2026.

Lisa Lowe
Ombudsman