

The complaint

Ms L complains that Santander UK Plc (Santander) won't refund money she lost in an investment scam.

What happened

What Ms L says:

Ms L saw an article online which was apparently promoted by a well-known TV personality. She registered her interest and was then contacted by an 'account manager'. He asked her to open an account with the (fake) investment firm (which I call 'firm A'), and with a crypto exchange firm (which I call 'firm B'). She went through various ID checks and checked the Financial Conduct Authority (FCA) website for the crypto exchange firm B. She communicated with the scammer account manager via online meetings and by emails. She was promised returns of 500%. Ms L had little investment experience and believed what she was told. **(continued)**

Ms L was encouraged to invest more – she could see her investment apparently growing in value. She was also pressurised into investing in a 'bonus' offer. She cashed in various other investments. Over the course of just over a month, she sent £105,000 to the crypto exchange firm B and then to the fake investment firm A:

Date	Payment	Amount
------	---------	--------

7 December 2023	Faster payment to crypto exchange B	£2,000
13 December 2023	Faster payment to crypto exchange B	£10,000
18 December 2023	Faster payment to crypto exchange B	£24,000
19 December 2023	Faster payment to crypto exchange B	£22,000
20 December 2023	Faster payment to crypto exchange B	£17,000
27 December 2023	Faster payment to crypto exchange B	£5,000
1 January 2024	Faster payment to crypto exchange B*	£15,000
10 January 2024	Faster payment to crypto exchange B	£5,000
11 January 2024	Faster payment to crypto exchange B	£5,000
Total		£105,000

*Santander intervened on 28 December 2023

She realised it was a scam when she asked to withdraw money. At that time, she was told her investments were worth £248,000 but she needed to pay a fee of 20% (£50,000) to access the money. All communications with the scammer account manager then stopped.

The scammer investment firm A was the subject of a warning by the FCA on 8 February 2024 – after the scam had taken place.

Ms L says Santander should've prevented the scam. The payments were unusual for her to make. The bank should've intervened before they actually did - on 28 December 2023; as by then, more than £80,000 had been sent. The bank should've asked open and probing questions. If they had, Ms L says the scam would've been uncovered – as it had the hallmarks of a scam – i.e. she'd found the investment through social media; there was a famous celebrity endorsement; she was asked to open an account with a crypto exchange, and she was guided by the scammers.

Ms L says Santander should refund the money she's lost, plus interest at 8% per annum.

What Santander said:

Santander didn't refund any money. The bank said the Contingent Reimbursement Model (CRM) code didn't apply as the funds were sent to an account in Ms L's name.

Our investigation so far:

Ms L brought her complaint to us via a third-party claims firm. Our investigator upheld it in his first view, but after listening to two calls between Santander and Ms L, he issued a second view which didn't uphold Ms L's complaint. He said:

- Santander intervened in the payment for £15,000 on 28 December 2023. On the call, Ms L said no one was helping her to make the payments. She said she got the bank details for the crypto exchange from that firm, and she had had the account for some time.

- Santander had provided a second call which took place on 12 February 2024 – when the scam was discussed with Ms L. On the call, Ms L says she was coached by the scammer as to what to say. This was consistent with the call on 28 December 2023 – where she didn't provide accurate information to Santander.
- So, he didn't think it was reasonable to have expected Santander to have uncovered the scam or broken the spell of the scammer.

Ms L didn't agree and asked that an ombudsman look at her complaint. She said again that an open and probing conversation would have uncovered the scam.

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.

I'm sorry to hear that Ms L has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although she didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, 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 and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Santander should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I need to decide whether Santander acted fairly and reasonably in its dealings with Ms L when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary – and in this case, the payments were made to Ms L's own account with crypto exchange firm B.

If the payments were of a sufficient size and were out of character with how Ms L normally used her account – then we would expect Santander to have intervened and spoken to Ms L about them. I looked at Ms L's account, and it's fair to say that the payments after and

including the one on 18 December 2023 (£24,000) were unusual compared to the way in which she normally used her account.

Up to then, I can see she made occasional faster payments of up to about £5,000 – there had been seven such payments between July 2023 and November 2023. So, I don't think it's reasonable to have expected Santander to have intervened up until 18 December 2023 – for those reasons.

The bank didn't intervene until 28 December 2023 – when Ms L was making a payment for £15,000 (debited on 1 January 2024).

Santander was the expert in such matters and in the call, we would have expected them to ask open questions such as:

- Why are you making the payment?
- Who to?
- For what purpose?
- How did you hear about the investment?
- How were you contacted about it?
- Where did the money come from that you're investing?
- Where is the money going to from your crypto wallet?
- What do you know about crypto investing?
- Have you made crypto investments before?
- How were you given the bank account details where the money was to be paid to?
- Have you given control on your devices to anyone else?

I listened to the call. And it is fair to say that Santander's call handler didn't ask such open questions. I script some of the conversation here:

Santander call handler: Has anyone asked you to mislead the bank. Ms L: 'no'.

Santander call handler: Where is the payment going to? Ms L: crypto exchange B, for stocks and shares.

Santander call handler: Do they (B) manage stocks and shares on your behalf? Ms L: yes, and I've checked that (crypto exchange B) is registered with the FCA.

Santander call handler: How did you get the bank account details for B? Ms L – when I logged into B's website.

Santander call handler: Read out script about safe account scams.

Santander call handler: Are you making this payment because of a message? Ms L: no, a friend told me about firm B.

Santander call handler: Has anyone pressured you? Ms L: no.

I consider this call didn't go far enough – the call handler only asked Ms L about the crypto exchange B - rather than the end investment into the (fake firm) A. This point has been made by Ms L's advisors – and I agree with that.

But equally, I must consider if Santander were able to break the scammer's spell or not – as it's only in that case that we can say that the bank could reasonably have been expected to stop the scam.

I listened to the call between Ms L and Santander which took place on 12 February 2024 – Ms L had reported the scam and the bank asked her some questions about it. On the call, Ms L admitted that she was coached by the scammers. She told the bank she was advised to ‘not say anything about Bitcoin to Santander’. She further said that she was asked a lot of questions by the crypto exchange firm B – and was told what to say by the scammer to firm B.

I further reviewed the emails between Ms L and the scammer. And there are several indications that Ms L was completely under the spell of the scammers. For example:

- On 15 December 2023, 18 December 2023, 19 December 2023, 29 December 2023, and 2 January 2024, she told the scammer details about correspondence between her and firm B – and what questions firm B were asking her.
- On 28 December 2023 and 2 January 2024 – she told the scammer about Santander’s intervention call – and that the £15,000 payment had then been released.
- On 28 December 2023, and 11 January 2024, she shared with the scammer that funds were coming from her other investments.
- On 9 January 2024, she told the scammer she had ‘told lies’ to the provider of an account she was cashing in to send funds to the scammer.

Most of the communications were by online ‘google’ chats which I’ve not seen. But given the evidence I’ve seen; I think it’s more likely than not that Ms L was being coached as to what to say to Santander by the scammer.

So, considering these exchanges and the call with Santander on 12 February 2024, I think it is reasonable for me to say that it’s unlikely that Ms L would’ve been open with the bank - either on the call on 28 December 2023, or if the bank had intervened at another point.

I also noted that Santander sent Ms L several online warnings about the payments. Ms L responded to say the payments were for ‘investment’. The warnings then said (in summary):

- Could this be an investment scam?
- Understand the details of what you’re investing in.
- How did you hear about the investment?
- Where did you find this opportunity?
- Only go ahead if you’re confident it’s not (a scam)
- Legitimate sounding investments can turn out to be a scam.
- Check the FCA website.

In response to the warnings, Ms L said she wanted to go ahead. I haven’t asked Santander which payments the warning was displayed for – as I’m persuaded I don’t need this further information to reach a fair and reasonable decision.

So, taking everything into account and having reviewed the evidence presented by both Santander and Ms L, I don’t consider that Santander could have reasonably prevented the scam from taking place – for the reasons I’ve set out.

Recovery: We expect firms to quickly try to recover funds from recipient banks when a scam takes place. I looked at whether Santander took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

Santander approached firm B’s bank in February 2024 – and were told the funds had been paid away by firm B in its normal course of business. That’s not surprising – as firm B is a recognised crypto exchange business.

And from there, the funds went from the crypto currency merchant (B) and the loss occurred when crypto was then forwarded to the fake investment. In this case, as the funds had already been sent on in the form of cryptocurrency there wasn't likely to be anything to recover.

I'm sorry Ms L has had to contact us in these circumstances. I accept she's been the victim of a cruel scam, but I can't reasonably hold Santander responsible for her losses.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or reject my decision before 6 May 2025.

Martin Lord
Ombudsman