DRN-5176794

The complaint

Miss S has complained that Santander UK Plc ("Santander") failed to protect her from falling victim to a cryptocurrency-related scam, and hasn't refunded the money she lost.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Miss S has used a professional representative to refer her complaint to this service. For the purposes of my decision, I'll refer directly to Miss S, but I'd like to reassure Miss S and her representative that I've considered everything both parties have said.

Miss has explained that around December 2023 she contacted unexpectedly via social media by someone ("the scammer") claiming to be a cryptocurrency investment mentor. The scammer, mutual followers with Miss S, making her seem credible. Miss S says the scammer's profile was filled with investment-related content and apparent success stories from other clients. Miss S says that as she had no prior investment experience, she believed this was an opportunity to improve her financial situation and help her family. She's explained how the scammer shared personal information about her life and family, to build Miss S's trust and enable the scam.

The scammer told Miss S she would guide her through the investment process and help her make a good profit. She directed Miss S to what she's described as a professional-looking investment platform, which had features like live trading graphs, different dashboard tabs, and a customer service team. Miss S was told that to participate, she needed to set up accounts with two cryptocurrency exchanges, which the scammer helped her do. Miss S was then encouraged to invest as much as possible to maximise her returns.

Miss S says that as she believed the scammer was an expert, she followed her instructions and started investing on 2 January 2024. Miss S has explained that she could see her funds being deposited into what appeared to be her investment account, which reassured her that the process was genuine. She then made three further payments on the same day, totalling £4,500.

The transactions relevant to the scam were all made or attempted using Miss S's debit card and are as follows:

	Date	Amount	Merchant
1	2 January 2024	£600	Debit card to crypto platform
2	2 January 2024	£1,500	Debit card to crypto platform
-	*2 January 2024*	*£1,500*	*Declined as suspected fraud*
3	2 January 2024	£1,500	Debit card to crypto platform
-	*2 January 2024*	*£1,500*	*Declined as suspected fraud*
4	2 January 2024	£1,500	Debit card to crypto platform

Total	**£5,100**

Miss S says although Santander blocked some transactions initially, she was able to proceed after answering some security questions. She's now complained that Santander's interventions weren't thorough enough to make her reconsider her actions, and she wasn't given an effective scam warning.

Shortly after making the payments, Miss S attempted to withdraw funds but found she was unable to do so. She contacted the scammer's supposed customer support team, but after several unsuccessful attempts to recover her money, she realised she had been scammed. The scammer then cut all contact with Miss.

Miss S made a complaint to Santander on the basis that it failed to recognise that the transactions were significantly different to her usual account activity. She saus in the three months leading up to the scam her largest payments were to herself, never exceeding £1,500, and her transactions mainly consisted of routine, low-value payments to established payees. She alleges that the sudden and significant payments to a new payee, linked to cryptocurrency should have been a red flag for Santander. She says if Santander had done more to intervene it would've uncovered the scam and prevented her losses.

Santander didn't uphold Miss S's complaint as it said the transactions weren't covered by the Contingent Reimbursement Model ("CRM") Code. It said that because the payments were made using Miss S's debit card, so it didn't agree it should be held responsible for her loss.

Miss S remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that Miss S discussed two of the payments with Santander and Miss S didn't give Santander accurate answers when it questioned her about the payments. She also said that Santander gave her appropriate warnings but Miss S confirmed she wanted to go ahead with the payments.

As Miss S didn't accept the investigator's opinion, the case has been passed to me to make a decision.

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 disappoint Miss S but having considered everything I'm afraid I'm not upholding her complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Miss S authorised these payments from leaving her account. It's accepted by all parties that Miss S gave the instructions to Santander and Santander made the payments in line with those instructions, and in line with the terms and conditions of Miss S's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I've started by considering whether Santander ought to have been aware that Miss S might've been at risk of financial harm. That's to say, whether any of the characteristics of the payments ought to have made it aware that Miss S was, or may've been, falling victim to a scam.

Having thought about this I think it would've been reasonable for Santander to intervene before Miss S made the third payment. I say this because the first three transactions were made in fairly rapid succession – within three hours – and were being made to an identifiable cryptocurrency platform. Given that Santander would've known cryptocurrency-related payment carry an elevated risk of being fraudulent, as well as the pattern of payments being unusual, I think an automated warning before payment three would've been proportionate.

How did Santander intervene?

The evidence I've seen suggests Santander declined payment three as it was flagged as potentially fraudulent, and Miss S was required to speak to Santander by phone before the it was processed. Santander also initially declined payment four for the same reason, and again Miss S was required to speak to it before she was able to make the payment successfully.

I've listened to the first call between Miss S and. Santander starts by telling Miss S it needs to eliminate its concerns about fraud and scams.

The agent firstly asks how Miss S found out about the investment, to which Miss S gives the name of the app she's been using. The agent again asks how Miss S found out about it, and Miss S explains she's been using it for a while using a different bank.

The Santander agent then asks if Miss S has checked that the company is registered with the Financial Conduct Authority. The agent then checks and finds that the company is in fact registered.

The Santander agent goes on to explain that there are a lot of criminals in the cryptocurrency space, who appear very helpful, but they tend to ask individuals to set up a cryptocurrency wallet which they'll have access to. They then take control of the account once it's been funded. The agent asks if anyone else was involved in the setup of the account, which Miss S confirms they weren't, and she tells the agent she did some in-person training with a third party company which made her aware of the investment opportunity. Santander again checks that a third party isn't involved in the payments or the investment, and Miss S confirms that to be the case. There's then a discussion about security on Miss S's Santander account and the agent agrees to call her back in around five minutes.

When the call resumes Santander starts by explaining "you should not make this payment if you've been asked to setup an online investment account, or a wallet, whilst someone else is connected to your device." It then asks if this applies to Miss S's situation, which she confirms it doesn't. Santander then tell Miss S "You shouldn't go ahead with this payment if you've found the investment through a social media advert, and you've not directly called the company you're investing in to confirm the legitimacy of the company. So you've said you didn't find this opportunity on social media, right? And Miss S replies "No, no".

Miss S then goes on to explain she's been investing for around eight months following some training. Santander follows this by explaining that some companies may offer a high rate of return but these companies are often not authorised or regulated, and that she may lose any money she sends to them. Miss S confirms she understand this. The agent then checks whether Miss S is happy to continue, which she confirms she is, and Santander advises her

she can reattempt the payment whilst on the line to ensure it goes through. Miss S does this successfully and the call ends.

I've also listened to the second call, which followed the other declined transaction.

Miss S starts by explaining that the payment is being made to a cryptocurrency platform and that it's for an investment, and Santander asks where Miss S saw the investment advertised. Miss S explains it's all done on an app that is covered by the FCA. Santander then asks if Miss S invests on her own or if someone helps her, to which she confirms she does the transactions on her own and she's "done all the training".

After a brief hold the agent returns and explains he can see two transactions for £1,500, which Miss S confirms is correct, and that one of those two needs to be unblocked. Miss S is directed to do the payment whilst on the call to ensure it's processed, and she doesn't have to call Santander again. Miss S enters the payment details and confirms the payment has been made successfully, and the call is ended.

Did Santander do enough to protect Miss S from harm?

Having carefully considered the events that took place during the scam, I'm satisfied that Santander took proportionate steps to understand the reasons behind Miss S's payment, and to warn her about the risk associated with it, during her calls with the first agent. The agent asked direct questions, to which Miss S gave some untruthful answers, and the agent also probed those answers and Miss S continued to give inaccurate information. The agent did however give several warnings about the risks involved with cryptocurrency, and although the specific situation Miss S was in was pointed out to her (seeing an advert about an investment on social media) Miss S chose to continue regardless.

So I'm satisfied that the first intervention was sufficient, and whilst Santander had a duty to protect Miss S from harm, it was also entitled to rely on the information she gave it when it did so. As the information she gave was inaccurate, I don't hold Santander responsible for the intervention being unsuccessful.

Turning to the second call, I'm not satisfied that this represented an effective intervention. Whilst the agent asked some broad questions about the payment, he didn't probe Miss S when she gave somewhat evasive answers, nor did he give any warnings before unblocking Miss S's account and allowing the payment to be made.

However, it's also necessary for me to consider whether this made a difference to the outcome for Miss S, and having thought carefully about that, I don't think it did.

I say that because during the first call Miss S gave evasive answers when asked about how she was introduced to the cryptocurrency investment, presumably to avoid rousing Santander's suspicious further. She also wasn't honest when she was asked whether anyone else was involved, or whether she found the investment via social media. These key questions would've allowed Santander to understand the elevated risks associated with the payment that it otherwise wouldn't have known about.

Although the second agent didn't ask Miss S as many questions, the answers she gave in relation to the questions that were asked followed a similar narrative to what Miss S said during the first call. So I'm satisfied that even if Santander had asked more probing questions, Miss S would most likely have given similar answers so as not to raise Santander's suspicions, to ensure the payment was released.

With the above in mind, I don't hold Santander responsible for the losses Miss S made as a result of its interventions being unsuccessful.

Recovery of the funds

As the payments were made using Miss S's debit card, the chargeback process is relevant here. But raising a chargeback is at the discretion of the bank and I'd only expect it to do so where there was a reasonable prospect of the chargeback succeeding.

As the payments were made to a legitimate cryptocurrency exchange, to an account in Miss S's own name, and she was able to access the cryptocurrency, the service Miss S paid for was provided by the merchant. Santander wouldn't have any grounds to raise chargebacks for the transactions in question, so I don't think that was a route it ought to have pursued.

I'm very sorry that Miss S has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Santander responsible for that.

My final decision

I don't uphold Miss S's complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 28 April 2025.

Sam Wade
Ombudsman