DRN-5222405

The complaint

Mr S complains about Santander UK Plc (Santander) refusing to refund the amount he lost as the result of a scam. Mr S is represented in this complaint, but I'll refer to him as it's his complaint.

What happened

There is limited information on what happened here.

Mr S says he transferred the following funds from his bank account with Santander to an account he held with Company A (a legitimate cryptocurrency exchange):

- £10 on 13 January 2022
- £3,660 on 14 January 2022

He then moved the funds from Company A, in cryptocurrency, to a cryptocurrency scheme that turned out to be a '*massive scam'* and he lost his funds.

In 2024, Mr S complained to Santander alleging that '*any warnings that may have been given*', in relation to the above payments, were not effective, sufficiently clear nor impactful. He also said he was '*clearly vulnerable'*.

Mr S claimed a refund of £3,670 under the Contingent Reimbursement Model (CRM) together with 8% interest and £1,000 compensation for poor service.

Santander didn't uphold Mr S's complaint. They said Mr S decided to proceed despite them giving him scam warnings and the payments were not covered under the CRM Code.

Mr S referred his complaint to our service: however, our investigator didn't think Santander could've done more to prevent his loss.

As Mr S remains dissatisfied his complaint has been referred to me to look at.

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, whilst I'm very sorry to hear that Mr S has been the victim of a cruel scam and lost a significant amount of money here, I'm not upholding this complaint, and I'll explain why.
I'd first like to say:

- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on balance of probabilities.
- As the following requested information hasn't been made available by Mr S, I checked the file to ensure Mr S had been given a fair opportunity and sufficient time

to provide it:

- *'Transcript of Messenger chat with the scammer from the first to last points of contact*
- *Emails with the scammer – from the first to last points of contact*
- *Screenshots of the scammer's platform showing the consumer logged in and any funds available*
- *All evidence of the scam, including any documentation that was sent as part of the scam*
- *Evidence of financial loss, including demonstrating what has been forwarded on crypto assets from any wallet*
- *Explanation of the source of funds, including bank statements covering any sending/funding transactions. Also ensuring that the sort code and account number of any funding account is provided please.*
- *Have any funds lost to the scam been recovered from any other sources?'*

I found that the above information was requested by our investigator on 12 September 2024 and, after Mr S requested more time, this was extended to 3 October 2024. Upon request it was subsequently further extended until 20 January 2025 and on 21 January 2025 Mr S said he:

> *'Does not have any further information / evidence to provide. Please can you provide a final response without the evidence.'*

So, before making a decision, I was satisfied that Mr S had been given a fair opportunity to make submissions.

Although Mr S hasn't provided any evidence that a scam occurred, I considered whether Santander had acted fairly and reasonably here. I took into account relevant law and regulations, regulatory rules, guidance and standards, codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

Why the CRM Code isn't applicable

Santander is a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code). This requires firms to reimburse customers who have been the victim of a scam in most circumstances.

Customers are only covered by the CRM Code where they have been the victim of an authorised push payment (APP) scam – as defined within the CRM Code. Also, the payment would need to be made to '*another person'*.

In this case, the payments went to Mr S's own account, which he had control of, with a legitimate business (Company A) and they then acted upon Mr S's instruction to send the funds to the scammer. So, I'm satisfied the payment didn't go to '*another person'* and the CRM code doesn't apply here.

The relevant law and regulations in place at the time

In broad terms, the starting position in law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (2017) and the terms and conditions of the customer's account. However, where the customer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though they authorised the payment.

It isn't in dispute here that Mr S authorised Santander to make the two payments totalling £3,670 from his account with them. So, although he didn't intend the money to go to a

scammer, the starting position in law is that Santander was obliged to follow his payment instruction and Mr S isn't automatically entitled to a refund.

Firms though have a duty to exercise reasonable skill and care, pay due regard to the interests of its customers and to follow good industry practice to keep customer's accounts safe. This includes identifying vulnerable consumers who may be particularly susceptible to scams and looking out for payments which might indicate the consumer is at risk of financial harm.

However, they do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider Santander should at that time fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look 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

Mr S mentions a vulnerability, but Santander don't have any record of this and, from the limited information provided, Mr S appears to be referring to inexperience in cryptocurrency and / or investments. So, there isn't evidence of a vulnerability that Santander ought to have been aware of or responded to differently.

Santander's records show interventions took place on the two transactions as Company A wasn't on their automated confirmation of payee list. So, the following interventions occurred as part of their scam prevention processes:

- Mr S received a warning message for the £10 payment to Company A on 13 January 2022. The warning said:
    - *'If youve been cold called or contacted out of the blue about an investment opportunity, this is highly likely to be a scam. Please check the company details thoroughly, including on the financial conduct authoritys website (fca.org.uk) before transferring any money. If youre at all nervous, cancel this payment and call us immediately.'*
- Mr S received a warning message for the £3,660 payment on 14 January 2022, which said:
    - *'Could this be a scam? If youve been contacted and asked to make an urgent payment, this could be a scam. Please take a minute to check the payment details and the reason for the payment is genuine. This could save your money from being stolen. If youre at all suspicious, or someones pressuring you to act quickly, dont continue.'*

Whilst I don't have any information on either the actual scam and Mr S's interaction with the scammer, if Mr S was inexperienced in cryptocurrency and / or investments, I think these Santander warnings would've highlighted risks and signposted him to make checks and seek assistance from them or the FCA. And at the time of the transactions there was an FCA alert about the crypto investment scheme that Mr S was planning to pay from his account with Company A.

There is evidence on the file, of a further intervention, before Mr S could proceed with the £3,660 on 14 January 2022. This was a human *'scam conversation'* with a Santander agent.

Due to the passage of time there isn't a recording for this intervention call. However, from reviewing Santander's historic records, I'm satisfied it took place.

Although it isn't possible to know what was said about Mr S's investment plans, bearing in mind Santander's record keeping, scam warning process and the FCA alert, I think it more likely than not that:

- The Santander agent would've:
    - Probed Mr S about his intentions
    - Asked Mr S the following type of questions:
        - How he came across this investment
        - The checks he had completed
        - The expected rates of return
    - Highlighted the risks and mitigations of crypto investments

Whilst evidence from both parties is limited, I'm satisfied Santander's response would've been proportionate in the circumstances.

I've taken into account that these payments were made to cryptocurrency providers and I'm aware that scams involving cryptocurrency are becoming increasingly prevalent and well known to banks.

But, at the time these payments were made, I think it was reasonable for Santander to take into account a range of factors when deciding whether to make further enquiries of its customer about a particular payment.

In this case, the pattern of payments wasn't consistent with fraud. And based on the available information, I think it more likely than not that Santander gave Mr S proportionate advice and / or warning and Mr S made a decision to proceed with the transfer.

Finally, regarding any attempts to recover the funds, even if Santander had details of the scam, due to the time gap and the funds being sent to a crypto exchange and then onto the scammer, there wouldn't have been any funds left for Santander to recover from the crypto account.

So, having considered all the available information, whilst I'm very sorry to hear that Mr S has been scammed, I'm not upholding this complaint against Santander UK Plc.

My final decision

My final decision is that I'm not upholding this complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 5 June 2025.

Paul Douglas
Ombudsman