DRN-5158044

Complaint

Ms L is unhappy that Santander UK Plc didn't refund her after she fell victim to a scam.

Background

In 2020, someone Ms L knew through a social media platform contacted her. They recommended that she make extra money by investing in cryptocurrency. They put her in touch with an investment professional who they said could help her with this. This wasn't a genuine investment opportunity, but a scam.

Over several months, Ms L made multiple payments using her Santander card to a third-party cryptocurrency platform. Those payments funded deposits into an e-wallet with that platform that was in Ms L's own name. Those deposits were then converted into cryptocurrency. She was persuaded to transfer the cryptocurrency to an e-wallet controlled by the fraudster on the basis that they would manage her investment on her behalf.

She made the following payments in connection with the scam:

	Date	Type	Value
1	01-Jun-20	Card payment	£ 100
2	30-Jun-20	Card payment	£ 307
3	09-Jul-20	Card payment	£ 600
4	10-Jul-20	Card payment	£ 125
5	14-Jul-20	Card payment	£ 1,665
6	27-Jul-20	Card payment	£ 4,300
7	29-Sep-20	Card payment	£ 3,500
8	05-Oct-20	Card payment	£ 2,310
9	05-Oct-20	Card payment	£ 100
10	05-Oct-20	Card payment	£ 50
11	23-Oct-20	Card payment	£ 1,700
12	13-Nov-20	Card payment	£ 800
13	20-Nov-20	Card payment	£ 720
14	20-Nov-20	Card payment	£ 180
15	09-Dec-20	Card payment	£ 1,100
16	02-Feb-21	Card payment	£ 1,500
17	02-Mar-21	Card payment	£ 550
18	02-Mar-21	Card payment	£ 250
19	06-Apr-21	Card payment	£ 800
20	03-Sep-22	Faster payment	£ 1,000
21	03-Sep-22	Faster payment	£ 1,000
22	06-Sep-22	Faster payment	£ 500

Her last card payment in connection with the scam was made on 6 April 2021. She also made three payments by bank transfer in September 2022. These were apparently to cover fees and charges that she was told she needed to pay to withdraw money from her investment.

Once she realised that she'd fallen victim to a scam, she told Santander. It looked into things but it didn't agree to refund her. It said that, as she'd authorised these payments, it hadn't done anything wrong in processing them. It also said that it had done everything it could to attempt to recover the money from the receiving bank, but this hadn't been successful.

Ms L wasn't happy with that response and so she referred the complaint to this service. It was looked at by an Investigator who upheld it in part. The Investigator said that Santander was expected to be on the lookout for payments that were unusual or out of character to the extent that they might have indicated a fraud risk. She was persuaded that it should've been concerned at payment 6 in the table above. If it had intervened at that point, the Investigator was persuaded that it would've prevented Ms L from suffering further losses to the scam. However, the Investigator also concluded that it was fair and reasonable for Ms L to bear some responsibility for her own losses by way of contributory negligence.

Ms L accepted the Investigator's opinion, but Santander didn't. It said:

- Ms L had made payments to the cryptocurrency intermediary. This was a legitimate business in its own right and Ms L should direct her complaint to it.
- It's speculative to say that an intervention call from the bank would've made a difference here, particularly given that Ms L would've confirmed that she was paying her own account at the cryptocurrency intermediary.
- Its position is consistent with the approach set out in the Supreme Court's judgement in the case of Phillipp v Barclays Bank.

As Santander disagreed with the Investigator's view, the complaint has been passed to me to consider.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I issued a provisional decision on this complaint on 1 November 2024. I wrote:

> *In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account.*
>
> *However, that isn't the end of the story. Good industry practice required that Santander be on the lookout for payments that were out of character or unusual to the extent that they might have indicated a fraud risk. On spotting such a payment, I'd expect it to intervene in a manner proportionate to the risk identified.*
>
> *Santander is also a signatory to the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. In certain circumstances, that Code requires firms to reimburse customers who have fallen victim to scams. However, it doesn't apply to all payments. The first 19 transactions here aren't covered by the CRM Code because they were debit card payments. However, it does apply to the final three*

payments, as they were processed as bank transfers. I'll consider the provisions of the Code in connection with those payments later in this decision.

Payments 1-19

We now know that Ms L was falling victim to a scam. However, the question I have to consider is whether that ought to have been apparent to Santander at the time given the information that was available to it. The Investigator concluded that Santander ought to have been concerned about the fraud risk at the point Ms L asked it to make payment 6. She said it shouldn't have processed that payment without first making contact with Ms L to satisfy itself that she wasn't at risk of financial harm due to fraud. I've thought about this carefully, and I'm not convinced that Santander had reasonable grounds for stepping in at that point.

The value of payment 6 wasn't so high that it would've automatically been regarded as cause for concern, setting aside other potential risk factors. I accept that these payments were being made to a cryptocurrency exchange and that Santander would've been aware of that. However, that exchange only accepts deposits from accounts in the same name as the e-wallet receiving the funds. Although Santander wouldn't have known that Ms L was paying her own account, it wouldn't have been unreasonable for it to have assumed she was and to have taken some reassurance from that.

In addition, there were significant gaps between these payments. Santander was expected to look at individual payment instructions and make a judgement as to whether they were out of character. But by the time Ms L asked it to make payment 6, she'd already made several card payments to that payee over a period of nearly two months. In light of that, I don't think payment 6 would've seemed out of the ordinary.

I realise that this will be hugely disappointing to Ms L. If Santander had intervened at payment 6, there was a good chance it could've prevented her from making further payments in connection with the scam. However, for the reasons I've explained, I don't think it did anything wrong in processing that payment without asking further questions. For similar reasons, I'm not persuaded it needed to intervene in connection with any of the later payments either.

Payments 20 - 22

The final three payments were processed as Faster Payments, which are covered by the CRM Code. According to the Code, Santander should reimburse customers for losses unless one of the Code's exceptions applies. One exception is where the customer didn't have a reasonable basis for believing that the transaction or the person they were paying were legitimate.

I accept that Ms L did sincerely believe that she was making those payments in order to get access to her investment. But I'm afraid I don't think that belief was a reasonable one.

The returns that had apparently been earned on her behalf by the investment manager were so extraordinary that they were clearly too good to be true. I think she ought to have questioned whether a legitimate investment could earn such vast returns. Furthermore, the investment opportunity was introduced informally through a social media contact, and there was no formal contract or documentation alongside it. The lack of formalities should have prompted Ms L to be more cautious.

Santander is also expected under the CRM Code to provide customers with effective warnings where it spots a fraud risk in connection with an individual payment. However, I'm not persuaded that any of the last three payments were sufficiently high in value or suspicious that I'd have expected it to display a warning.

Other issues

For the sake of completeness, I've also looked into whether Santander did everything I'd have expected in terms of recovering Ms L's funds. I can see that it did contact the receiving bank in an attempt to do so. Unfortunately, she notified Santander over a month after making the final payment. Fraudsters tend to move fraudulent funds on very quickly from the receiving account and so the prospect of there being any of her funds left in that account over a month later was always remote.

I don't say any of this to downplay or diminish the fact that Ms L has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for her and the position she's found herself in. However, my role is limited to looking at the actions and inactions of the bank and I'm satisfied it didn't do anything wrong here.

Santander didn't respond to my provisional decision. Ms L responded to say she didn't have any new information to provide. In the absence of any new evidence or arguments to consider, I don't see any reason to change the conclusion I arrived at in my provisional decision. I can only imagine how disheartening this outcome must be for Ms L. However, for the reasons I've explained I'm not convinced that Santander is at fault and so I can't uphold the complaint.

Final decision

For the reasons I've explained above, I don't 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 18 December 2024.

James Kimmitt
Ombudsman