DRN-4750366

Complaint

Miss E is unhappy that Santander UK Plc didn't reimburse her after she fell victim to a scam.

Background

In September 2023, Miss E fell victim to an investment scam. A fraudster hacked a social media profile belonging to Miss E's friend. They then posted information online that suggested that friend had earned significant money by investing in cryptocurrency with the assistance of an independent broker. Miss E messaged her friend to ask if this updated was legitimate. She received a reply saying that it was.

She was put in contact with someone who said they would help her with investments in exchange for a 10% fee. They persuaded her to create an account with a third-party cryptocurrency firm and she was given access to a seemingly professional looking trading platform. She then proceeded to transfer funds into that account. Those cash deposits were subsequently converted into cryptocurrency and transferred into the control of the fraudsters. On 22 September 2023, she made two payments of £1,000 using her debit card. The second of these was authorised via Apple Pay. The following days she made two further payments of £1,000 by bank transfer.

Once Miss E realised that she'd fallen victim to a scam, she notified Santander. It didn't agree to refund her losses. Miss E wasn't happy with that response and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. Miss E disagreed with the Investigator's opinion and so the complaint has been passed to me to consider and come to a final decision.

Findings

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

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 2017 and the terms and conditions of the customer's account.

However, that isn't the end of the story. Depending on the circumstances, a range of other considerations come into play. Good industry practice required that Santander be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to make enquiries with the customer to satisfy itself that they weren't at risk of financial harm due to fraud.

Whether it should intervene (and, if it should, the nature and extent of that intervention) should be proportionate to the risk the payment presents and strike a balance between protecting customers on the one hand, but not unduly inconveniencing customers trying to make legitimate payments on the other.

Santander is also a signatory to the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one Miss E fell victim to, in all but a limited number of circumstances.

Under the CRM Code, a firm may choose not to reimburse a customer if it can establish that:

- The customer made the payment without a reasonable basis for believing that … the person or business with whom they transacted was legitimate.

- The customer ignored an effective warning in relation to the payment being made. [1]

In this case, the CRM Code only applies to the last two payments because they were made by bank transfer. It doesn't cover payments made by card.

We now know with the benefit of hindsight that Miss E was falling victim to a scam. The question I must consider is whether Santander ought to have recognised that in view of the information that was available to it at the time.

Unfortunately, I'm not persuaded that it would've had reasonable grounds for intervening in connection with any of these payments. The activity was arguably out of keeping with the way Miss E typically used her account. Nonetheless, the payment value is a relevant indicator of the risk, and I don't think it would be practical to say that Santander ought to question payments of £1,000 (unless there were other factors that indicated a fraud risk) given that this would mean significant disruption for other customers.

Miss E has pointed to another decision issued by this service in which an ombudsman decided that a bank ought to have intervened in connection with payments of a similar size. However, I don't think the two cases are entirely comparable. The main distinction is that in that case, the customer transferred funds to a pre-paid card held in the name of the fraudster. There's more of a fraud risk associated with pre-paid cards and so, in that case, it was a combination of that and other factors regarding the use of the account that led to the ombudsman deciding the bank should've done more. Unfortunately, not all of those considerations are relevant here.

The last two payments

I've also considered whether Santander ought to have reimbursed Miss E under the terms of the CRM Code or whether it can fairly and reasonably rely on one of the exceptions to reimbursement described above. In other words, I have to consider whether Miss E had a reasonable basis for believing that she was participating in a legitimate investment opportunity. I don't doubt that she did sincerely believe that, but I'm afraid I'm not convinced that belief was a reasonable one.

The returns she was promised were extraordinary. I can see in the messages she exchanged with the scammer that she was told that an investment of £4,000 could expect to earn her £25,000 – a return of 625%. I think it ought to have occurred to Miss E that what was being promised must have been too good to be true.

I accept that she attached a great deal of significance to the apparent endorsement of this opportunity by someone she'd known for a long time. Nonetheless, I'm surprised that she was willing to proceed with the investment based entirely on a very brief message exchange on the social media platform. She then appeared to go ahead with the investment very quickly without carrying out any further research or checks to ensure that this was a genuine

[1] There are other exceptions under the Code but they aren't applicable here.

opportunity. I think she ought to have proceeded with greater caution than she did and so I'm satisfied it's fair and reasonable for Santander to rely on that exception.

The CRM Code also says that, where a firm identifies a scam risk, it should provide its customer with an effective warning. The specific criteria for a warning to be "effective" are set out in the Code. However, for the reasons I've already explained, I'm not persuaded that there was a sufficiently clear risk that these payments might be connected with fraud to the extent that Santander would've been required to provide Miss E with a warning.

For completeness, I also considered whether Santander did everything it needed to do once it was notified that a scam had taken place, particularly in terms of recovering Miss E's funds. In respect of the bank transfers, I can see that it did contact the receiving bank and notify them that a scam had taken place. Unfortunately, all of the funds had been moved on from that account which meant recovery wasn't possible.

I don't say any of this to downplay or diminish the fact that Miss E 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.

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 Miss E to accept or reject my decision before 27 September 2024.

James Kimmitt
Ombudsman