DRN-4718737

The complaint

Ms T complains that Santander UK Plc ("Santander") won't refund money she lost when she fell victim to an employment scam.

What happened

In November 2023, Ms T fell victim to an employment scam. She explains she was looking for remote jobs and came across an advertisement for a company "H". She left her contact details on the web form and a representative reached out to her via an instant messaging service.

Ms T was told she would help H increase its sales by completing a certain number of 'tasks' on its platform. In addition to receiving a commission on completion of a set of tasks (or orders), Ms T could also earn a base salary from working five consecutive days, as well as a month. The representative told Ms T that she would need to create an account with a cryptocurrency platform to withdraw her commission as it was paid in cryptocurrency. It was also explained that to reset orders every day, Ms T would need to 'recharge' her account on H's platform with an amount equalling the negative balance.

According to Ms T's submissions, her initial deposits were made via her account with another bank, "B". But when B blocked one of the transactions, under the representative's advice, she switched to using her Santander account. Ms T made two card transactions – £1,000 and £400 – on 9 November from her Santander account in relation to this job opportunity. She realised she'd been scammed when she was repeatedly required to make further deposits to clear the negative balance.

Santander said it couldn't recover Ms T's funds through a chargeback as she had approved both card transactions through her mobile banking app. It also refused to refund her losses. Unhappy with this outcome, Mr T complained to Santander before referring the matter to our service. Our investigator concluded that the transactions weren't for particularly high amounts and Ms T's account activity showed that she often credited the account before moving the funds away. That made the disputed transactions – which followed a similar pattern – appear less suspicious.

Ms T didn't agree with the investigator's findings and asked for her complaint to be reviewed by an ombudsman. In summary, she accepts she made the payments but did so based on false information. She submits that Santander has therefore failed in its duty to protect her. Ms T says she didn't receive any warning from the bank and has quoted several pieces of legislation to demonstrate why it failed in its duty of care to her. Ms T has also forwarded a copy of the chat correspondence with the scammer.

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'd like to start by saying I'm sorry to hear about Ms T's personal circumstances and how this incident has impacted her further. From what she's told us, I don't doubt that this has been a difficult period for her. I'd like to reassure Ms T and Santander that although I've only summarised the background above, so not everything that's happened or has been argued is detailed, I have read and considered their submissions in their entirety.

It's not in question that Ms T was the victim of a cruel scam. And it's very unfortunate that she's lost a considerable sum of the money. But Santander doesn't automatically become liable to reimburse her loss. Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Ms T made the payments using her security credentials, and so they are authorised.

The Lending Standards Board's Contingent Reimbursement Model (the CRM Code), which requires signatories such as Santander to reimburse customers who are victims of authorised push payment (APP) scams in all but a limited number of circumstances, doesn't apply here for a few reasons. Firstly, the payments Ms T made were card transactions. These are 'pull' payments and not push payments which the CRM Code was designed for. Also, the payments Ms T made weren't sent directly from her bank account to the scammer. They were made via another account in her name with a cryptocurrency exchange which I understand she had control over. Pull payments aside, the CRM Code also doesn't apply to payments between accounts held in the same name.

While I find the CRM Code doesn't apply here, that code is not the full extent of the relevant obligations that could apply in cases such as this. I can see that Ms T has referenced some of those regulations and codes of practice in her submissions. In the interest of brevity, I won't go into the specific regulations. But in broad terms, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert it to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

I've looked at the operation of Ms T's account and I acknowledge what she's said about the previous credits and debits being between her own accounts. Notwithstanding, it isn't uncommon for a customer to make a payment to a third-party every now and then. I don't consider the individual transactions in dispute to be *that* unusual such that I think Santander ought to have had cause for concern. I acknowledge that the transactions were cryptocurrency related. But that in and of itself doesn't mean that they ought to have flagged as suspicious. Buying cryptocurrency is a legitimate exercise.

So, I agree with the investigator's conclusion that the payments didn't look suspicious, and Santander couldn't reasonably have known that Ms T might have been at risk of financial harm.

Even if I were to conclude that Santander ought to have recognised that the first card transaction carried a heightened risk of financial hard from fraud (just to be clear, that isn't my finding here), in the circumstances of this case, I consider a proportionate response to that risk would have been for the bank to have provided a written warning during the payment journey. But I'm not persuaded that a written warning would have positively impacted Ms T's decision making. We know from her submissions that when bank B blocked a transaction, she followed the scammer's instructions and switched to Santander.

Also, I can see from the chat correspondence between Ms T and the scammer that on the day in question she was instructed not to mention cryptocurrency to her bank. Reading the

correspondence, it's also my understanding that Ms T followed the scammer's instructions in opening an account with another firm, "R", from where she also made payments. But as I've already mentioned, I haven't seen any factors at play here such that, in my view, Santander should have been concerned and ought to have intervened before executing her authorised instruction. I recognise that her circumstances at the time made Ms T particularly vulnerable. But from what I've seen, Santander wasn't aware of that until later when she reported the scam.

I've also thought about whether Santander could have done more to recover the funds once it became aware of the situation, as in some circumstances the money can be recovered. These were debit card payments, so the recovery avenue would have been limited to raising a chargeback. But Ms T's payments didn't go to the scammer directly, they went to a cryptocurrency exchange. She wouldn't be able to make a successful chargeback claim in the circumstances because the merchant she paid did provide the service requested (i.e., conversion of fiat money into cryptocurrency). So, I don't think Santander was under any obligation to raise a chargeback dispute for Ms T.

In conclusion, I know that Ms T will be disappointed with this outcome. Despite my natural sympathy for the situation in which she finds herself due to the scammer's actions, for the reasons given, it wouldn't be fair of me to hold Santander responsible for her loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms T to accept or reject my decision before 31 July 2024.

Gagandeep Singh
Ombudsman