DRN-5689794

## The complaint

Miss P complains that Santander UK Plc didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In May 2021, Miss P met someone I'll refer to as "the scammer" who said he was an investment broker and that he worked for a company I'll refer to as "T". She was encouraged to open an account on a trading platform and told she could make good returns by investing in cryptocurrency. Miss P was satisfied that T had a professional looking website and that it had offices overseas, so she decided to go ahead.

The scammer communicated with Miss P via Telegram and told her to download AnyDesk remote access software. He asked her to first purchase cryptocurrency through B and then load it onto an online wallet, and on 5 May 2021, she made a payment for £3,910.87 using her Santander credit card. She also made payments to the scam from Bank H.

Miss P received an initial return of £500, and she could see what she believed were her profits on the trading platform. But she realised she'd been scammed when she was unable to make any further withdrawals.

She complained to Santander, but it refused to refund the money she'd lost and so she complained to this service arguing that it should have intervened before she made the payment. She also complained that Santander was dismissive when she reported the scam.

Responding to the complaint, Santander explained that Miss P had tried to make a payment on 4 May 2021 for £4357.84. The payment was flagged for further review, and she was advised by phone that trading is risky and if she lost her funds, she'd still need to pay back the amount and the interest. It said Santander said there was a further call the following day before the payment for £3910.87, but the call wasn't available.

It also said the Contingent Reimbursement Model ("CRM") Code didn't apply to the payment, and chargeback wasn't applicable because Miss P paid a legitimate cryptocurrency exchange and would have received the service she paid for.

Our investigator didn't think the complaint should be upheld. He didn't think Santander would have uncovered the scam if it had questioned Miss P about the payment because when Bank H intervened before a payment she was making to the same scam, she told it she'd opened the account the day before, she'd done her own research, the funds she'd received into her account had been sent by family who had sold a property in Italy, and she hadn't been contacted and told to move money from the account. She was then given a warning about investment scams.

Our investigator was satisfied that Miss P was asked relevant questions, but her responses prevented Bank H from detecting the scam. He was also satisfied that Miss P had received a clear waring and yet she went ahead with that and further payments to pay the fees she believed were required to make a withdrawal. He further explained that the messages between Miss P and the scammer showed she continued to allow the scammer to use AnyDesk. So, he didn't think Santander would have been able to uncover the scam.

Miss P has asked for her complaint to be reviewed by an Ombudsman. She has further explained that she'd believed she was dealing with a genuine investment company and the scammer had threatened to freeze her trading account and was demanding fees to release her profits. She was also coached on how to answer the banks questions.

**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, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Miss P has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss P says she's fallen victim to, in all but a limited number of circumstances. But she Code doesn't apply to credit card payments.

I'm satisfied Miss P 'authorised' the payment for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Miss P is presumed liable for the loss in the first instance. There's no dispute that this was a scam, but although Miss P didn't intend her money to go to scammers, she did authorise the disputed payment. Santander is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

*Prevention*

I've thought about whether Santander could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payment was made to a genuine cryptocurrency exchange company. However, Santander ought to fairly and reasonably be alert to fraud and scams and this payment were part of a wider scam, so I need to consider whether it ought to have intervened to warn Miss P when she tried to make the payment. If there are unusual or suspicious payments on an account, I'd expect Santander to intervene with a view to protecting Miss P from financial harm due to fraud.

The payment did flag as suspicious on Santander's systems, but Santander hasn't retained the call recording. As it would have known Miss P was sending funds to a cryptocurrency exchange, having contacted her by phone, I would then expect it to have asked her why she was making the payments, whether there was a third party involved and if so how she'd met them, whether she'd downloaded remote access software, whether she'd been promised unrealistic returns, whether she'd made any withdrawals, whether she'd been coached to lie,

whether she'd done any due diligence and whether she'd been advised to make an onwards payment from the cryptocurrency exchange.

I've considered how Miss P would have responded to these questions and I don't think she'd have been honest about the circumstances. Miss P has told us she was coached to lie to her banks and its clear from the call she had with Bank H that she was following that advice. So, I don't think Santander would have uncovered the scam.

I've also considered how Miss P would have reacted to a further warning about cryptocurrency investment scams. Critically, she made payments to the scam having received relevant warnings from Santander and Bank H, and I've no reason to think she'd have done anything different if Santander had given her a similar warning on 5 May 2021. Mrs P has explained that she'd believed the investment was genuine and that she was under pressure to pay fees to release her profits. She was also being coached by the scammer. So, I don't think a further warning from Santander would have made a difference.

I'm sorry to hear Miss P has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Santander is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

*Recovery*

I don't think there was a realistic prospect of a successful recovery because Miss P paid an account in her own name and moved the funds onwards from there.

I've thought about whether Santander could have done more to recover the card when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Santander) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Miss P).

Ms K's own testimony supports that she used a cryptocurrency exchange. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence it had done what was asked. That is, in exchange for Ms P's payment, it converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Santander's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

For similar reasons, a claim under Section 75 of the Consumer Credit Act 1974 would be unlikely to succeed because Miss P paid a legitimate cryptocurrency exchange and received the service she paid for.

*Compensation*

The main cause for the upset was the scammer who persuaded Miss P to part with her funds. I haven't found any errors or delays to Santander's investigation, so I don't think she is entitled to any compensation.

**My final decision**

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss P to accept or reject my decision before 26 January 2026.

Carolyn Bonnell
**Ombudsman**