

The complaint

Mr C and Ms S complain that Santander UK plc did not do enough to protect them from the financial harm caused by an investment scam company, or to help them recover the money once they'd reported the scam.

What happened

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

Mr C and Ms S were victims of an investment scam. Mr C had been investing in cryptocurrency with the help of a broker I'll refer to as "C". In August 2021, he received an email from C explaining his cryptocurrency wallet was being frozen but that if he took out another account with a different exchange company (who I'll refer to as "B"), the cryptocurrency could be transferred.

After researching B, Mr C made nine payments to it (and another cryptocurrency exchange) totalling £42,498. The payments were made via online transfer from his Santander account between 23 August 2021 and 8 October 2021, with the money used to purchase cryptocurrency before being loaded onto an online wallet.

After he'd paid the agreed amount, Mr C was told by the broker he'd need to pay a further £4,000 into the account to allow the deposit of the cryptocurrency into the wallet, followed by two payments totalling £4,800 to a personal account nominated by the broker, which he did.

Mr C was given scam warnings on 26 October 2021 when he tried to make the payments to the personal account. Both times he confirmed he was paying for a service and the block was removed. Santander then contacted him on 27 October 2021 to ask questions and give a fraud warning.

During the call Mr C explained he'd been dealing with cryptocurrency for a while and that he'd approached and researched the investment himself. He confirmed he'd not been approached or contacted by anyone and was looking to exchange his cryptocurrency into GBP. Mr C told the call handler he hadn't been asked to pay any upfront fees. He also said there was no third-party or broker involved and that he hadn't allowed remote access to any of his devices. He said only he had access to his wallet, and it was secured with two-factor authentication. During the call, Santander gave a full scam warning and Mr C confirmed he was aware of the risks. As a result, Santander agreed to remove the block.

Mr C realised he'd been the victim of a scam a few days later when he was unable to contact the broker. He contacted Santander who said two payments Mr C had made on 26 October 2021 would be refunded under the Contingent Reimbursement Model ("CRM"), but the other nine payments couldn't be refunded under the CRM as they were paid to an account in his name.

Mr C and Ms S weren't satisfied and so they complained to Santander. But it maintained its position. It said the correct level of security had been used to complete the transactions and

that it would only refund the payments Mr C had made on 26th October 2021. It explained that the nine remaining payments were reviewed as part of the same process but that they didn't fall under the scheme.

Mr C and Mrs S remained dissatisfied and so they complained to this service. They said they wanted Santander to fully reimburse the money they'd lost, and they didn't understand why the nine payments wouldn't come under the same remit as the two payments Santander had agreed to refund. They said they'd offered to send copies of scam emails with the company logos and signatures of the actual companies involved, but it said it wouldn't need them.

Our investigator didn't think the complaint should be upheld. She accepted Mr C and Ms S had been the victims of a scam, but she didn't think Santander should reasonably have been expected to prevent this or that it should have refused to put the payments through.

She thought Santander should have contacted Mr C when he tried to make the second payment. But she didn't think an intervention from Santander would've made a difference to Mr C's decision to make the payments because he'd previously ignored advice about investment scams from another bank. And on 27 October 2021, Santander had contacted him to discuss the two payments he'd made the day before and during that call Mr C gave answers that weren't accurate.

With the help of a representative, Mr C has asked for the complaint to be reviewed by an Ombudsman. The representative has argued that the first payment should have triggered Santander's fraud systems.

They have also argued that this scam was different in nature to the previous scam, which followed a known cryptocurrency investment scam pattern and involved the use of a professional looking online portal where Mr C could monitor his investments and see his deposits in real-time. They explained that Mr C was never told how the scam operated or that his investments had never existed. Consequently, after the previous bank had closed its fraud investigation, Mr C still believed his investments were real, so he approached a different company.

The representative has argued it is reasonable to expect Santander to have been able to uncover the second scam had they sufficiently questioned Mr C as there were multiple red flags that could have been identified e.g. Mr C believing he was making the payments to validate an account in his name at the request of a broker. They've also argued Mr C may have been more likely to listen to advice if Santander had intervened before the first payment.

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. I'm sorry to hear that Mr C and Ms S have been the victims of a cruel scam. I know they feel strongly about this complaint and this will come as a disappointment to them, so I'll explain why.

CRM Code

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr C and Ms S say they've fallen victim to, in all but a limited number of circumstances. Santander has said the CRM code

didn't apply in the case of nine of the payments because they were made to an account Mr C held in his own name. I'm satisfied that's in line with the CRM code.

I'm satisfied Mr C 'authorised' the payments for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of the bank account, Mr C is presumed liable for the loss in the first instance.

I've carefully considered the circumstances, and I am persuaded the broker was operating as part of a scam. But, although Mr C didn't intend the money to go to scammers, he did authorise the disputed payments. 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. While cryptocurrency exchange companies are commonly used by scammers, buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to genuine cryptocurrency exchange companies. However, Santander had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr C when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Santander to intervene with a view to protecting Mr C and Ms S from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr C and Ms S normally ran their account and I think that they were. This is because, when Mr C made the first payment to B, even though he had paid cryptocurrency exchanges before, there had not previously been a transaction greater than £2,000 from the account, and this was the first time he'd paid B. So, I'm satisfied the first payment should have triggered Santander's fraud systems.

This should have prompted a call from Santander, earlier than it did. During this call I would expect Santander to have asked some probing questions around whether there was a third-party or a broker involved, how Mr C had come into contact with the broker and whether he'd been asked to pay any fees or given the broker access to his wallet account.

However, if Santander had asked these questions, I think it's unlikely Mr C would have answered truthfully. I say this because he didn't answer honestly when he was questioned on 27 October 2021 and I don't think an earlier call would have been any different. Because of this, I don't think Santander would have gathered enough information to suggest the investment could be a scam.

Notwithstanding the fact I don't think Mr C would have disclosed enough information to suggest this was a scam, I would still expect Santander to have warned Mr C about the risks associated with the investment and to discuss with him the nature of the checks he'd undertaken and to give some advice on additional due diligence.

Our investigator has said she doesn't believe a call from Santander would have made a difference to Mr C's decision to go ahead with the first payment because there were no warnings about B on the FCA website and it's clear from the fact he withheld information on 27 October 2022, he trusted the broker and was determined to go ahead with the investment.

The fact is, Santander contacted Mr C when he tried to make the payment on 27 October and he still went ahead with the payment, having failed to disclose facts which would likely have alerted Santander to the fact Mr C was the victim of a scam. I'm satisfied that Mr C was asked sufficiently probing questions and that he was clearly and effectively advised about the risks associated with investing in cryptocurrency, including a description of the methods used by scammers.

Overall, I'm satisfied Santander took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. And I don't think it got to the point where Santander ought to have prevented the payments altogether as its most likely C presented them as genuine and would have continued to do so.

I'm sorry to hear Mr C and Ms S have lost money, 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.

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 Mr C and Mrs S to accept or reject my decision before 10 July 2023.

Carolyn Bonnell
Ombudsman