DRN-4283271

The complaint

Mr S complains Santander UK Plc didn't do enough to protect him when he fell victim to an investment scam.

What happened

Mr S has a current account and a debit card with Santander and says he has been a customer Santander customer for over 30 years.

Mr S says he was added to a group on a social media platform discussing investment and trading. He says he'd been looking into the possibility of investing at the time, was interested in what the group were talking about and asked how to get started. He says he received an email from someone who turned out to be a scammer who explained that he'd need to buy cryptocurrency which he'd then use to invest on a trading platform. Mr S says he checked the companies involved and didn't see anything to suggest that there were scams. Having done so, he went ahead and started to invest.

Mr S says he sent three payments in total, namely £500 on 18 October 2022, £2,340.95 on 22 October 2022 and £4,973.59 on 29 October 2022, to cryptocurrency wallets set up in his own name for onward investment. He says he initially made a loss and was told he'd get help recovering his losses, but when he was asked for more money to bring the total amount he'd deposited to £10,000 he said he didn't have any more. And he says that he was then told he'd need to made further payments to withdraw the profits he'd made. Mr S says at this point – when he couldn't make any withdrawals – he realised he'd been scammed. He contacted Santander.

Santander looked into Mr S's claim and initially treated it as a chargeback as a result of which he got the original £500 he'd sent refunded. Mr S complained about the remaining £7,314.54 Santander hadn't recovered for him. Santander looked into his complaint and said that it should have treated his claim as a scam and not a card dispute and that Mr S had got £500 back that he ordinarily wouldn't have got back as a result. Santander said that it couldn't help with the remaining £7,314.54 and couldn't offer a refund as the payments had been sent to an account in his own name. Mr S was unhappy with Santander's response and so complained to our service.

One of our investigators looked into Mr S's complaint and said that Santander should have intervened when Mr S attempted to make the third payment he made. In other words, when he attempted to make a payment of £4,973.59. Our investigator said that this payment was unusual when compared to Mr S's normal usage. Had Santander done so, our investigator didn't think Mr S would have gone ahead and made the payment. Our investigator also thought that Mr S should share some responsibility for what had happened as he hadn't done enough due diligence and there were clear warning signs hat this was likely to be a scam. So, they recommended that Santander refund 50% of the third payment and pay the rate of interest that Mr S would have received had the funds remained in his savings account. Mr S's representative accepted our investigator's recommendation. Santander didn't. Santander said that Mr S had made a payment to a wallet in his own name and that any losses he made occurred after that, so it shouldn't be held responsible for them, nor

should it have had reason to intervene. Santander said that it had received clear and unequivocal instructions from Mr S – the payments were made using Mr S's genuine card and had been authenticated in-app and this had been done from his usual IP address. In short, Santander asked for Mr S's complaint to be referred to an ombudsman for decision. His complaint was, as a result, passed to me.

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.

No-one appears to be disputing the fact that Mr S has been the victim of a scam and that the scam payments happened after he'd bought cryptocurrency using his Santander debit card. I'll come to whether or not it's fair to hold Santander liable for that in a moment. Santander doesn't agree, however, that it should have intervened or could have done more in this case.

Having looked through his statements, I agree with our investigator that the final payment that Mr S made – just under £5,000 – was sufficiently unusual to warrant intervention from Santander. That's because the payment was unusually high when compared to Mr S's normal usage, was a large payment and was going to a new beneficiary and to cryptocurrency. I agree that all of these factors should have alerted Santander to the possibility that Mr S was at risk of financial harm.

I agree with our investigator that in a case like this I would have expected Santander to warn Mr S of the risks of investing in cryptocurrency given the prevalence of these types of scams at the time, but there's no evidence it did. Had Santander done so, I agree with our investigator that this would have led to Mr S discovering he was being scammed and would have stopped him going ahead with the third payment. Santander has said that Mr S's instructions were clear – in an apparent reference to a bank's duty to execute a customer's instructions if they're clear and leave no room for interpretation. Or, to put it another way, an apparent reference to Philipp v Barclays Bank UK PLC, so I'll go on and address that now.

what fairly and reasonably should Santander do?

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr S's account is that Mr S is responsible for payments Mr S has authorised himself. And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, banks generally have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, the bank must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.

- The express terms of the current account contract may modify or alter that position. For example, in Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a duty to do so.

In this case, Santander's terms and conditions at the time gave it rights (but not obligations)

to:

1. Refuse any transaction that appears unusual compared to the customer's normal spending pattern or if it suspects fraud.

2. Delay payments while fraud prevention checks take place and explained that it might need to contact the account holder if Santander suspects that a payment is fraudulent. It said contact could be by phone.

So, the starting position at law was that:

- Santander was under an implied duty at law to make payments promptly.

- It had a contractual right not to make payments where a transaction appeared unusual compared to a customer's normal spending pattern or it suspected fraud.

- It had a contractual right to delay payments to make enquiries where it suspected fraud.

- It could therefore refuse payments, or make enquiries, where it suspected fraud, but it was not under a contractual duty to do either of those things.

Whilst the current account terms did not oblige Santander to make fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded Santander from making fraud checks before making a payment.

And, whilst Santander was not required or obliged under the contract to make checks, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good practice at the time, it should fairly and reasonably have been on the look-out for the possibility of APP fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances – as in practice all banks, including Santander, do.

I am mindful in reaching my conclusions about what Santander ought fairly and reasonably to have done that:

- FCA regulated banks are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6).

- Banks have a longstanding regulatory duty "to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime" (SYSC 3.2.6R of the Financial Conduct Authority Handbook, which has applied since 2001).

- Over the years, the FSA, and its successor the FCA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the "Financial crime: a guide for firms".

- Regulated banks are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the

scrutiny of transactions undertaken throughout the course of the relationship).

- The October 2017, BSI Code, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code, but in my view the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now.

- Santander has agreed to abide by the principles CRM Code. This sets out both standards for firms and situations where signatory firms will reimburse consumers. The CRM Code does not cover all authorised push payments (APP) in every circumstances (and it does not apply to the circumstances of this payment), but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a fair articulation of what I consider to be good industry practice generally for payment service providers carrying out any APP transactions.

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Santander should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.

- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.

- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Santander have fairly and reasonably made further enquiries before it processed Mr S's payments?

In this case, for the reasons I have explained, I'm satisfied Santander should have intervened.

if Santander had intervened …

The key questions I have to decide is:

- whether or not that would have made a difference had Santander intervened; and
- in the event that it would have made a difference, whether or not Santander should be responsible for refunding the payment Mr S made from the time that Santander should have intervened.

Mr S has told us that he carried out limited independent due diligence before he started to invest. And there were also some red flags in this case. His representatives have accepted our investigator's recommendation that liability be shared on a 50/50 basis. I don't think that's an unreasonable or unfair outcome. That's because I agree with our investigator that had Santander intervened when Mr S made his third payment, I'm satisfied he would have realised he was being scammed. That means Santander missed an opportunity to prevent further loss to Mr W. So, I think it's fair it should refund some of that loss.

Putting things right

Given what I've just said, I think the fair outcome in this case is to require Santander to refund 50% of the third payment Mr S made plus our usual interest award. So that's the award I'm going to make.

My final decision

My final decision is that I'm upholding this complaint and require Santander UK Plc to refund 50% of the third payment Mr S made – in other words, 50% of £4,973.59 – plus 8% simple interest from the date of payment to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 15 April 2024.

Nicolas Atkinson
Ombudsman