DRN-4604128

The complaint

Mrs A complains Santander UK Plc didn't do enough to protect her when she fell victim to a scam.

What happened

Mrs A had a current account and a credit card with Santander – she's closed her accounts following what happened – and accounts elsewhere with another business who I'll refer to as "B" in the rest of this decision.

Mrs A says she was looking for work when she received a message on a well-known app offering her an opportunity to work remotely. She replied to say she was interested and was given details of the company she'd be working for – she checked the company and it appeared to be genuine – and says was told she could earn £800 a week and would get back £10,000 if she invested £400. Mrs A says she was given training and shown how to buy cryptocurrency as she was told she'd need this to re-charge her account from time to time when completing tasks that she'd ultimately be paid for. She says was added to a group of people who were working for the company who talked about the profits they were making.

Mrs A says things went well at first and then the amounts she needed to re-charge her account increased considerably. She says she ended up using up her credit cards and borrowed money in order to fund the payments she was told she'd need to make. She says she realised she'd been scammed when she was told she'd have to pay another £6,200 in order to withdraw her earnings. She contacted Santander to say she'd been scammed and said that she was really unhappy Santander hadn't warned her at all.

Santander looked into Mrs A's complaint and the scam she's said she'd fallen victim to. Having done so, Santander said that it couldn't offer a refund. Mrs A was very unhappy with Santander, closed her account and complained to us. She said she was unhappy that Santander hadn't told her this was a scam or how to check for a scam. She also said that she was very unhappy that Santander had carried on charging her interest on her credit card balance despite knowing that she'd been scammed.

One of our investigator's looked into Mrs A's complaint and said that Santander couldn't fairly and reasonably have been expected to intervene so it wouldn't be fair to say it should offer a refund. Mrs A disagreed and sent us material showing that Santander had promised to protect its customers from fraud and that it also owed a duty of care. Mrs A said Santander had done neither in her case and that she wanted her complaint to be referred to an ombudsman for a decision. Her 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.

Between 30 September 2023 and 2 October 2023 Mrs A made two payments from her Santander current account and three payments using her Santander credit card to two

different cryptocurrency exchanges. She made two payments of £600, two payments of £1,000 and one payment of £1,200. In other words, she sent a total of £4,400. None of these payments were caught by the Contingent Reimbursement Model – for various reasons – which is why Santander didn't offer Mrs A an automatic refund or decline to do so on the grounds that she'd been negligent. I'm mentioning this now because when Mrs A first complained to us it's clear she thought she should be getting a refund because she'd been scammed and hadn't been negligent. The Contingent Reimbursement Model might be what she had in mind when she said this.

I can see that Santander introduced limits on payments going to cryptocurrency exchanges on 9 October 2023 – from that date it introduced a limit of £1,000 per transaction and a total of £3,000 in any rolling 30-day period. Had those limits been in place when Mrs A had made the payments she did then they would have almost certainly had an impact. The limits weren't, however, in place at the time. Her last payment was on 2 October 2023. That doesn't mean Santander didn't fairly and reasonably have to take steps to protect its customers from the risk of fraud. It did. I do, however, agree with our investigator – for the reasons I'm about to give – that it wouldn't be fair and reasonable to expect Santander to have intervened in this case. I'll explain why.

Mrs A has said that Santander owed her a duty of care and has referred us to the case of Philipp v Barclays Bank UK PLC saying that this case proves Santander had a duty to protect her from fraud. Normally it's the business who refers to Philipp v Barclays Bank UK PLC saying that this case says it has a duty to execute a customer's instructions if they are clear and leave no room for interpretation. But consumers mention it from time to time too. So, I think it's worth explaining the relevance of the Philipp v Barclays case, and what this means for what Santander ought to have fairly and reasonable done in this case. Before I do so, I should add that Mrs A has told us other banks sends her notifications or restrict her payments until she's confirmed they're genuine, but that Santander didn't. And she's also told us that B calls to check and inform her every time they notice a transaction that might be a scam. I can, however, see that Mrs A has complained to us about B not doing enough when she fell victim to this scam, so it seems B doesn't always do so. I'm not going to say more about that complaint, however, as it's one that has only recently been referred to us and is one we're still investigating.

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 Mrs A's account is that Mrs A is responsible for payments Mrs A has authorised herself. 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 Mrs A's payments?

Having looked through Mrs A's current account statements and credit card statements in the period leading up to the scam, I agree with our investigator that none of the payments would have appeared unusual on account of their size when compared to Mrs A's normal usage. That's because I can see, for example, she'd made several payments of around £2,000 in the months leading up to the scam. I accept that these were the first payments Mrs A had made towards cryptocurrency, and had they been made a short time later they would have been flagged for the reasons I gave earlier. But the fact that they were payments to cryptocurrency is not enough in this case in my opinion to turn what are payments that aren't unusual in size into a payment that should have been a cause for concern for Santander.

As I'm satisfied Santander wasn't interacting with Mrs A for any other reason at the time, it follows that I don't think it missed an opportunity to prevent Mrs A from falling victim to a scam. So, it wouldn't be fair and reasonable to hold Santander liable for Mrs A's losses given everything else I've already said, including what I've said about the Contingent Reimbursement Model.

My final decision

My final decision is that I'm not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 28 March 2024.

Nicolas Atkinson
Ombudsman