

The complaint

Mrs H and Mr H complain Santander UK Plc didn't do enough to protect them when they feel victim to an investment scam.

What happened

Mrs H and Mr H have a joint account with Santander.

Mrs H and Mr H say they were contacted on a well-known messaging service and invited to join a group that talked about investments. They say that the group talked about stock market investments at first and that – having watched for several months – the activity appeared to be genuine. They say they were then asked if they'd be interested in a cryptocurrency related investment. Mrs H and Mr H say they were then sent information on a specific investment and having done checks they decided to invest. They say they sent £12,000 to a well-known cryptocurrency exchange and then forwarded the cryptocurrency they'd bought to the investment platform they'd been invited to invest in. Mrs H and Mr H says their investment appeared to do well and that they were told they'd need to pay £3,000 in capital gains tax before they could withdraw their profits. They say they realised they'd been scammed shortly afterwards. Mrs H and Mr H contacted Santander to say they'd been scammed and to ask for help getting their money back.

Santander looked into Mrs H and Mr H's claim and said that the Contingent Reimbursement Model didn't apply as they'd sent the £12,000 in question to an account in their own name. Mrs H and Mr H weren't happy with Santander's response and complained with the help of a representative. Santander said that it hadn't done anything wrong, so Mrs H and Mr H referred their complaint to our service.

One of our investigators looked into Mrs H and Mr H's complaint and said that Santander should have intervened as the payment was unusual compared to their normal usage. Had Santander done so, our investigator didn't think Mrs H and Mr H would have gone ahead and made the payment. Our investigator also thought that Mrs H and Mr H should share some responsibility for what had happened as they hadn't done enough due diligence and there were clear warning signs that this was likely to be a scam. So, they recommended that Santander refund 50% of the £12,000 lost.

Mrs H and Mr H's representative accepted our investigator's recommendation. Santander didn't. Santander said that Mrs H and Mr H 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 Mrs H and Mr H – the payments had been authenticated in-app and this had been done from Mrs H and Mr H's usual IP address. In short, Santander asked for Mrs H and Mr H's complaint to be referred to an ombudsman for decision. Their 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 Mrs H and Mr H have been the victims of a scam and that the scam payments happened after they'd sent money from their Santander account to a well-known cryptocurrency platform. In other words, that the scam happened after Mrs H and Mr H bought cryptocurrency and after money had already left their Santander account and been credited to a cryptocurrency wallet in their name. I'll come to whether or not it's fair to hold Santander liable for this 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 £12,000 payment made was sufficiently unusual to warrant intervention from Santander. That's because the payment was unusually high when compared to Mrs H and Mr H'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 Mrs H and Mr H was at risk of financial harm given that this payment took place in December 2022. That's around the time we'd expect most firms to have been aware of the increased risk of scams associated with cryptocurrency and cryptocurrency related investment scams.

I agree with our investigator that in a case like this I would have expected Santander to have given Mrs H and Mr H a tailored written warning relevant to cryptocurrency investment scams. In this case Santander has said that Mrs H and Mr H confirmed the payment was a transfer to an investment were warned that if they'd been cold-called or contacted out of the blue about an investment opportunity then this could be a scam. I don't, however, think this warning went far enough. In other words, I don't agree it was a tailored written warning relevant to cryptocurrency investment scams. Had Santander given such a warning, I agree with our investigator that this would have led to Mrs H and Mr H discovering they were being scammed and would have stopped them going ahead with the payment.

Santander has said that Mrs H and Mr H'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 Mrs H and Mr H's account is that Mrs H and Mr H are responsible for payments they have authorised themselves. 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 H and Mr H's payment?

In this case, for the reasons I have explained, I'm satisfied Santander should have intervened in the way I've described above.

if Santander had intervened appropriately ...

The key questions I have to decide is:

- whether or not that would have made a difference had Santander intervened appropriately; and

- in the event that it would have made a difference, whether or not Santander should be responsible for refunding the payment Mrs H and Mr H made.

Mrs H and Mr H's representatives have accepted our investigator's recommendation that liability be shared on a 50/50 basis given the red flags that were present. I don't think that's an unreasonable or unfair outcome. That's because I agree with our investigator that had Santander intervened when Mrs H and Mr H made their £12,000 payment, I'm satisfied they would have realised they were being scammed. That means Santander missed an opportunity to prevent loss to Mrs H and Mr H. 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 £12,000 payment Mrs H and Mr H 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 £12,000 payment Mrs H and Mr H made 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 Mrs H and Mr H to accept or reject my decision before 21 May 2024.

Nicolas Atkinson
Ombudsman