

## The complaint

Mr V complains that Santander UK Plc (Santander) is refusing to refund him the amount he lost as the result of a scam.

Mr V is being represented by a third party. To keep things simple, I will refer to Mr V throughout my decision.

## What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Mr V received a call from the company BitLuna (X). X appeared very professional and knowledgeable. It explained an investment opportunity to Mr V and provided reasonable answers to the questions he had.

Mr V carried out some online research before deciding to invest with X which Mr V said came back positive. To open an account with X Mr V needed to provide identification documents which made the investment look even more legitimate.

Mr V started to invest with the help of X through the remote access software TeamViewer, investing more money on the basis he would receive greater returns.

Mr V then decided to make a withdrawal from the investment and made several payments as directed by X in relation to the withdrawal process. After making the payments, X continued to give reasons why Mr V was unable to make a withdrawal from the investment and it became clear that he had fallen victim to a scam.

Mr V made the following payments from his Santander account in relation to the scam to his Coinbase account:

Date	Payment Method	Amount
4 August 2022	Transfer	£1,000
5 August 2022	Transfer	£2,000
17 August 2022	Transfer	£2,500
17 August 2022	Transfer	£2,500
18 August 2022	Transfer	£2,700
24 August 2022	Transfer	£13,000
30 August 2022	Transfer	£4,000
31 August 2022	Transfer	£5,000
3 September 2022	Transfer	£2,000
14 October 2022	Transfer	£380
16 October 2022	Transfer	£400
18 October 2022	Transfer	£3,100

Our Investigator considered Mr V's complaint and thought it should be upheld in part.

Santander disagreed, so this complaint has been passed to me to decide.

### **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.

It has not been disputed that Mr V has fallen victim to a cruel scam. The evidence provided by both Mr V and Santander sets out what happened. What is in dispute is whether Santander should refund the money Mr V lost due to the scam.

#### *Recovering the payments Mr V made*

Mr V made payments into the scam via the method of transfer. When payments are made by this method Santander has limited options available to it to seek recovery. Santander could speak to the receiving payee, as it did in this case, to see if any funds remain in the account Mr V made the payments to. But as Mr V made the payments into an account in his own name, if any funds did remain, they would continue to be within Mr V's control. Mr V has also told us that he moved the funds to his Coinbase account and then onto the scammer. So, I am satisfied no funds would remain in the account to be recovered anyway.

With the above in mind, I don't think Santander had any reasonable options available to it to recover the payments.

#### *Should Santander have reasonably prevented the payments Mr V made?*

It has been accepted that Mr V authorised the payments that were made from his account with Santander, albeit on X's instruction. So, the starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr V's account is that he is responsible for payments he's 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 June 2022 terms and conditions gave it rights (but not obligations) to:

1. Refuse any payment instruction if it reasonably suspects it relates to fraud or any other criminal act.
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 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, 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 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)<sup>2</sup>.
- 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”.<sup>3</sup>
- 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 is also a signatory of the 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 set of circumstances (and it does not apply to the circumstances of these payments), 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.

---

<sup>2</sup> Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

<sup>3</sup> For example, both the FSA's Financial Crime Guide at 4.2.5G and the FCA's 2015 "Financial crime: a guide for firms" gave examples of good practice in relation to investment fraud saying:

"A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.

A bank contacts customers if it suspects a payment is being made to an investment fraudster.

A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules."

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 V's payments?*

The first five payments Mr V made in relation to the scam were for relatively low amounts to a legitimate business. It would not be reasonable for me to suggest Santander should step in every time one of its customers makes a relatively low value payment to a legitimate business.

But the sixth payment Mr V made in relation to the scam was for the significant value of £13,000 and was out of keeping with the way Mr V usually ran his account. So, I think the payment should have caused Santander concerns and it should have stepped into question Mr V about what the payment was for.

I've not seen anything to suggest Mr V would not have answered Santander's questions truthfully. So, I think it's likely that had Santander stepped in as I think it should, it would have likely found that Mr V was making investments with X via Coinbase, and that X had access to his device via TeamViewer. I think this information would have likely caused Santander concerns, and it would have warned Mr V of the likelihood of the investment being a scam and prevented any further loss.

So, I think Santander is responsible for Mr V's loss from the payment of £13,000 onwards.

*Did Mr V contribute to his loss?*

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances I don't think it would be fair to say Mr V contributed to the loss. I say this because Mr V appears to have had no previous experience in this type of investment and was lulled into a false sense of security by a business that went to great lengths to appear to be legitimate.

Although he carried out online searches at the time, he received mixed reviews as he would expect from a genuine business, and I don't think he would have reasonably been aware that the investment was a scam.

### **Putting things right**

To put things right I require Santander UK Plc to refund Mr V for the amount he lost in relation to the scam from the sixth payment of £13,000 on 24 August 2022 onward and pay 8% simple interest on this amount from the date the payments were made to the date of settlement.

### **My final decision**

I uphold this complaint and require Santander UK Plc to put things right by doing what I've outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr V to accept or reject my decision before 25 April 2024.

Terry Woodham  
**Ombudsman**