DRN-4365377

The complaint

Mr C complains that Santander UK Plc didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

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

In June 2022 Mr C came across an advert promoting an investment opportunity. He completed an enquiry form and received a call from someone I'll refer to as "the scammer" who claimed to work for a company I'll refer to as "R".

Mr C researched R online and found many positive reviews. The scammer presented himself as professional, friendly, polite, knowledgeable, and helpful. He told Mr C he'd been an account manager for many years and that he would assist him with the investments until he felt comfortable to do it on his own. He told him the more he invested, the great his profit would be.

The scammer gave Mr C a username and password to a trading account and guided him over the phone on how to make a deposit. The scammer asked him to first purchase cryptocurrency through a cryptocurrency exchange company I'll refer to as "F" and told him that from there it would be loaded onto an online wallet. On 13 June 2022, Mr C transferred £10 to the scam and could immediately see the balance on his trading account, which made him comfortable to make further payments.

Between 13 June 2022 and 4 January 2023, Mr C made seven transfers to F from his Santander account totalling £18,284.55. During this period he made two withdrawals for £466 and £509.45.

Mr C could see his account balance increasing and received regular updates from the scammer. But at the end of January 2023 the scammer pressured him to make more payments to keep his account open and became aggressive towards him. They eventually lost touch and Mr C realised he'd been scammed.

Mr C complained to Santander with the assistance of a representative who said he'd made the payments with no intervention and that it should have stopped the transactions and provided scam advice which would have prevented financial hardship.

But Santander refused to refund any of the money Mr C had lost. It said there was no attempt to recover the funds because he didn't report the scam to it. It explained the payments weren't covered under the Contingent Reimbursement Model ("CRM") code because they were to an account held by Mr C with another financial institution, so they weren't within the scope of the code.

Mr C wasn't satisfied and so he complained to this service with the assistance of a representative. He explained he'd thought the investment was genuine and if he'd known it could be a scam he wouldn't have gone ahead with the payments. He said he wanted Santander to refund the money he'd lost plus £500 compensation and legal costs.

Mr C's representative said Santander had failed to raise a chargeback request. They also said the second payment to F was processed without an intervention, which was a missed opportunity to provide an effective warning and that it had missed red flags including the rapid depletion of funds, high-value transactions, and a new payee linked to cryptocurrency.

They said the payment was unusual compared to the usual account activity and Santander should have identified the unusually large and suspicious payments. They said it should have asked Mr C why he was making the payment, who he was trading with, how he found out about the company, whether he'd researched the company, whether he'd checked the Financial Conduct Authority ("FCA") website, whether he'd been promised unrealistic returns, whether he'd received any withdrawals and whether he'd discussed the investment with anyone. And had it done so, as he hadn't been coached to lie he'd have told it about thebroker and it would have been clear that he was falling victim to an investment scam. It could then have provided a tailored warning and advice on how to check the investment was genuine and Mr C wouldn't have gone ahead with the payment.

Our investigator thought Santander ought to have intervened on 28 October 2020 when Mr C paid £5,000 to F. He said that in the six months prior to being scammed, Mr C's typical spending rarely exceeded £1,500, so the increasing amounts and the frequency of the payments was unusual. He said it should have asked Mr C if he was receiving advice from a third party and had it done so he was satisfied he'd have mentioned the scammer. So even though he was paying a legitimate cryptocurrency platform Santander should still have alerted him to the common issues arising in relation to cryptocurrency brokers, which in turn would have stopped the scam. Because of this he felt Santander should refund the money Mr C had lost from 28 October 2020 onwards.

Santander has asked for the complaint to be reviewed by an Ombudsman. It maintains Mr C should complain to F given the loss was from his account with them.

It has argued that other than the value of the payments, there was nothing else to suggest that they were being made in relation to a scam and as the payments were being sent to Mr C's own account, there would have been little reason to question that the payment instruction was unclear.

It maintains it acted in line with industry standards while following Mr C's instructions to transfer the money and it hasn't breached any duty of care as its primary duty is to execute a customer's payment orders promptly in accordance with their instructions.

It has argued that we can't predict what would have happened if it had intervened as the questions would be proportionate to the situation and the responses and it was significant that he'd received credits from F.

It has also commented that Mr C selected 'Transfer to an Investment' when prompted to provide a reason for the payments and was warned to check the details of the company before transferring any funds. It has stated that there's no evidence that this was done and that he has indicated that after speaking to the scammer, he transferred the funds with no further investigation. It has questioned whether Mr C did any research or checked the reviews.

Finally, Santander has explained that the Supreme Court's decision in Philipp v Barclays Bank plc confirmed that where the bank receives a payment instruction from a customer which is clear and / or leaves no room for interpretation, if the customer's account is in credit, the bank's primary duty is to execute the payment instruction. This is a strict duty, and the bank must carry out the instruction promptly without concerning itself with the "wisdom or risks of [the] customer's payment decisions". It has commented that Mr C's account was in credit so he was able to make the payment from the account and it executed the payment in accordance with its duty.

My provisional findings

I explained the Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr C says he's fallen victim to, in all but a limited number of circumstances. Santander had said the CRM code didn't apply in this case because he was paying an account in his own name, and I was satisfied that's fair.

I was satisfied Mr C 'authorised' the payments for the purposes of the 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 his bank account, Mr C is presumed liable for the loss in the first instance.

There's no dispute that this was a scam but although Mr C didn't intend him 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.

I explained the starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr C'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 was satisfied that, taking into account longstanding regulatory expectations and requirements and what I considered 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.

I was 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 considered 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 considered 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 considered 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 considered 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.

Prevention

I thought about whether Santander could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I'd seen, the payments were made to a genuine cryptocurrency exchange company. However, Santander ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed 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 from financial harm due to fraud.

The payments didn't flag as suspicious on Santander's systems. I considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr C normally ran the account and as F was a legitimate cryptocurrency exchange, the payments were relatively low value and they weren't made in quick succession, I didn't think Santander needed to intervene in any of the first four payments. But by the time Mr C paid £5,000 to F on 28 October 2022, I was satisfied the amount was unusual for the account and the increasing payment amounts was a pattern of payments which ought to have raised concerns. So I thought Santander missed an opportunity to intervene.

Santander should have contacted Mr C and asked him why he was making the payments, whether there was a third party involved and if so how he met them, whether he'd been told

to download remote access software, whether he'd been promised unrealistic returns, whether he'd made any withdrawals and whether he'd been told to make an onwards payment from the cryptocurrency exchange. Had it done so, as there's no evidence he'd been told to lie I was satisfied Mr C would have told it he was being advised by someone who worked for a company he'd seen advertised online. He could have also told it he'd been allowed to make two small withdrawals and that he'd been advised to make an onwards payment from the cryptocurrency exchange.

I was satisfied that there were enough red flags present for Santander to have identified that Mr C was probably being scammed and so it should have provided a tailored warning and advice on additional due diligence, which would likely have uncovered the scam. And as I hadn't seen any evidence that he was keen to take risks, even though Mr C had received two credits from the investment, I thought he'd have listened to a strong warning and decided not to make any more payments. Consequently I was satisfied that Santander's failure to intervene on 28 October 2022 represented a missed opportunity to have prevented Mr C's loss and so it should refund the money he lost from that point onwards.

Contributory negligence

I explained there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I didn't think Mr C was to blame for the fact he didn't foresee the risk. Santander had argued that Mr C was warned to check the details of the company before transferring any funds, but I was satisfied he did what he thought was realistic due diligence.

I hadn't seen any evidence he was promised unrealistic returns or that there were any negative reviews available online about R around the time Mr C decided to go ahead with the investment and while there was an FCA warning, it wasn't added until 21 November 2022, so it post-dated the first payment.

Mr C hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. He wouldn't have known it was so risky to take investment advice from someone he'd found online or how to check the information he'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he trusted the broker and the fact he believed the trading platform was genuine and was reflecting the fact his investments were doing well. So, while there may be cases where a reduction for contributory negligence is appropriate, I didn't think this was one of them.

Compensation

I thought carefully about everything that has happened, and with all the circumstances of this complaint in mind, I didn't think Santander needed to pay any compensation given that I didn't think it acted unreasonably when it was made aware of the scam. And he wasn't entitled to compensation for legal fees, as our service is free to access.

Recovery

Mr C has described that he paid an account in his own name and from there the funds were moved to an online wallet in the scammer's control, so I was satisfied there was no prospect of a successful recovery.

Developments

Mr C has indicated that he's happy to accept the findings in my provisional decision, and Santander hasn't responded.

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.

Because neither party has made any additional comments or submitted any further evidence for me to consider, the findings in my final decision will be the same as the findings in my provisional decision.

My final decision

For the reasons I've outlined above, my final decision is that Santander UK Plc should:

- refund the money Mr C lost from 28 October 2022, less any credits received during the scam period.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Santander UK Plc deducts tax in relation to the interest element of this award it should provide Mr C with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 20 April 2024.

Carolyn Bonnell
Ombudsman