DRN-4694539

The complaint

Mr A 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.

On 9 February 2021 Mr A saw online advert for an investment company, which I'll refer to as "E". The advert featured endorsements from two well-known celebrities and claimed the investment could be started with an initial deposit of £250.

Mr A followed the link in the advert and was taken to an enquiry page where he submitted his contact details. He then received a call from somebody who I'll refer to as "the scammer" who claimed to work for "E". The scammer said they were a senior account manager and that they would help Mr A to reach his financial goals by helping him to invest in cryptocurrency.

Mr A did a google search and couldn't see anything which indicated E might be a scam, so he decided to go ahead. He was asked to provide a copy of his photo ID and proof of address which was required to open an account on the trading platform. He was also told to open an account with a cryptocurrency exchange company which I'll refer to as "L" and encouraged by the scammer to download AnyDesk remote access software so that he could ensure his account was managed effectively.

Once the account had been verified, Mr A was able to log in and change the password. He was assigned a dedicated account manager, who claimed to be a Blockchain expert and sent emails featuring the company logo and contact details in the footer of the email
The account manager asked Mr A to first purchase cryptocurrency through L and then load it onto online wallet. Between 16 February 2021 and 8 June 2021, he made ten faster payments to three cryptocurrency exchange companies totalling £80,170.99. He also made three withdrawals totalling £11,934.38.

Mr A remained in regular contact with the scammer by phone and email and was kept updated on how the investment was performing. Each time they spoke, he could hear background noise which made it seem as though the scammer was working in a call centre. He was also able to log into the trading account and see what he thought were his profits.

On 27 May 2021, Mr A asked the scammer if he could make a full withdrawal as he believed there was enough on the account for his retirement fund. He was then sent a release authorisation form advising that fees and taxes were due to be paid on the eligible profits of £168,572.88. He made five further payments and received a withdrawal for £4,884.87, but he realised he'd been scammed when he didn't receive any further funds and lost contact with the scammer.

He complained to Santander, but it refused to refund any of the money he'd lost. It said it intervened on 8th June 2021 when Mr A tried to make a payment of £4,950 and he confirmed he was happy for payment to leave his account and the restrictions were lifted. It said he should have done more to protect himself by carrying out checks to verify who he was speaking to and who he was paying. It also said it had tried to recover the funds, but the attempt was unsuccessful as no funds remained.

Mr A wasn't satisfied and so he complained to this service with the assistance of a representative. He explained he'd believed the scam was genuine as the advert contained a celebrity endorsement and E's compliance department had required him to provide ID to verify his identity. He was also able to make withdrawals and could log into his trading account whenever he wished. He said Santander didn't block or question any of the payments and if he had any inclination E was a scam he wouldn't have gone through with the payments. He said he wanted Santander to refund the money he'd lost with interest and £500 compensation and legal costs.

The representative said Mr A didn't receive any effective pop-up warnings which would have indicated that he was being scammed. They said Santander should have intervened on 24 February 2021 when Mr A paid £6,000 to L because the payment was significantly higher than any other payments that had been made from the account. They explained that in November 2020, December 2020 and January 2021, the largest payments from the account were £644, £885.29, and £445.42, the account was mostly used for small direct debit payments, and he hadn't previously made payments to cryptocurrency merchants.

They further argued there were several fraud indictors present including the fact Mr A was making payments to multiple high-risk payees with links to cryptocurrency, there was a rapid depletion of funds from the account, a sudden increase in spending and multiple payments made in quick succession. Santander should have contacted Mr A and asked him who he was trading with, how he found out about the company, whether he'd done any research, whether he'd checked the FCA register, whether he'd been promised unrealistic returns and whether he'd received any withdrawals. Had it done so, as Mr A hadn't been coached to give false answers, it would have realised he was likely falling victim to an elaborate investment scam, particularly as he was taking instructions from a broker who had told him to download AnyDesk, and the online advert included celebrity endorsements, all of which are red flags for fraud.

Santander said the first transaction of £3,000 on 16 February 2023 was detected and a text message was sent Mr A who confirmed the payment was genuine. He was also required to authorise £13,655.37 on 28 May 2023 via an OTP sent to his mobile phone. It maintained Mr A didn't perform sufficient checks which would reasonably include checking the FCA website. It also argued that a celebrity endorsement doesn't prove a company is legitimate and the profits were unrealistic based on the deposits made.

Our investigator recommended that the complaint should be upheld. She said the Contingent Reimbursement Model (CRM") code didn't apply because Mr A made payments to accounts in his own name, and she acknowledged that Santander had sent Mr A a text message when he made the first payment and an OTP on payment seven.

She didn't think the text message Santander sent when Mr A made the first payment was proportionate to the risk, but she didn't think it should be held liable for that payment because the funds remained in the cryptocurrency wallet for a further two days. But she thought it should have intervened when Mr A made the second payment and that its failure to do so represented a missed opportunity to have prevented his loss.

She explained it should have asked him what the payment was for, how he heard about the investment, whether there was a third party involved, whether he'd been promised unrealistic returns and whether he'd done any checks, and had it done so she thought it was likely he'd have disclosed that he was being advised by a broker he'd found online via an advert with a celebrity endorsement. Santander should then have provided a meaningful scam warning including a warning that a celebrity endorsement is a known fraud indicator.

She further explained that she didn't think there should be a reduction for contributory negligence because Mr A was an inexperienced investor, he believed E was legitimate, she didn't think it was unreasonable for him to expect high returns and there weren't any negative reviews online about E. So, she thought Santander should refund the money he'd lost from the second payment onwards.

Mr A was happy with our investigator's findings, but Santander has asked for the complaint to be reviewed by an Ombudsman. It has argued that Mr A is liable because he authorised payments to his own cryptocurrency account and what he chose to do beyond that point isn't a matter for the bank.

It has argued in the call on 8 June 2021, Mr A said he'd checked the FCA website and had been actively investing since February 2021. But on 15 June 2021, he confirmed he hadn't traded before and didn't check the FCA website.

It said it didn't intervene on 24 February 2021 because it had already detected the first payment and the second payment was made via an existing bill payment to the same account. And he was asked questions as part of the scam chat on 8 June 2021.

Santander has also said the Supreme Court's binding 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 argued that Mr A's account was in credit, so he was able to make the payments from his account and it executed the payments in accordance with the bank's duty to the customer. Furthermore, the payments were being sent to Mr A's own account with another regulated entity such that there would have been little (if any) reason to question that the payment instruction was unclear and / or open to interpretation. The current FOS position suggests that the bank ought to have acted in breach of its strict legal duty to the customer by refusing to make the payments which is completely untenable given the Philipp decision.

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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons.
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 A says he's fallen victim to, in all but a limited number of circumstances. But the code didn't apply to these payments because Mr A was paying accounts in his own name.

I'm satisfied that E was likely operating a scam, but although Mr A didn't intend his 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.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr K'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 December 2020 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 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.

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 [u]— 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.

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.

Prevention

I've 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've seen, the payments were made to genuine cryptocurrency exchange companies. However, Santander ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have done more to warn Mr A 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 A from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr A normally ran his account, and I think they were. The first payment was relatively low value and so I'm satisfied that the text message Santander sent requiring Mr a to verify the payment was proportionate to the risk. But the second payment was higher value and even though Mr A had verified a payment to the same payee eight days previously, the amount was unusual when compared to the normal spending on the account and he was paying a cryptocurrency merchant, so I think Santander should have intervened.

It should have contacted Mr A and asked him why he was making the payment, whether there was a third party involved and if so how he'd met them, whether he'd downloaded remote access software, whether he'd been promised unrealistic returns, whether he'd made any withdrawals, whether he'd been coached to lie, whether he'd done any due diligence and whether he'd been advised to make an onwards payment from the cryptocurrency exchange.

Santander has suggested that Mr A wouldn't have been open in his responses because he gave different accounts in the calls it had with him on 8 June 2021 when it intercepted a payment to B for £4950 and on 15 June 2021 when he reported the scam, so I've considered what was said during the calls.

I accept that on 8 June 2021 Mr A said he'd been investing since February and that on 15 June 2021 he said he hadn't invested before, but I don't consider this is an inconsistency because both responses mean he hadn't invested before the scam, which began in February 2021.

Further, on 8 June 2021, Mr A said he'd done his own research and that he'd seen the warnings about cryptocurrency on the FCA website. And when he was asked if he'd done any checks on 15 June 2021 he said "no, I did look online…I read it was a good company'. Again, I don't consider these responses are inconsistent because they both suggest he did some very basic research.

On 8 June 2021, Mr A was also asked whether he'd been cold called, which he had not. He was also asked whether anyone had recommended the investment, again the correct answer that was that the investment hadn't been recommended. The call handler fell short of asking Mr A whether he was being advised by a broker or any other third party, which might have uncovered the scam.

Critically, I don't think there is any evidence that Mr A lied to Santander or that he wouldn't have answered questions honestly if it had intervened on 24 February 2021. Consequently, I'm satisfied he would likely have disclosed that he was being advised by a broker who he'd found online through a celebrity endorsement and who had advised him to download AnyDesk. And I think there were enough red flags present for Santander to have detected the scam.

It should then have brought those red flags to Mr A's attention and provided a tailored cryptocurrency investment warning. At this point, Mr A hadn't yet received any withdrawals from the platform and as I haven't seen any evidence that he was keen to take risks or that he ignored any previous warnings, I think he'd have listened to the bank and decided not to make any further payments to the scam.

Because of this I'm satisfied that Santander's failure to intervene on 24 February 2021 represented a missed opportunity to have prevented his loss and so it should refund the money he lost from the second payment onwards, less any credits received.

Contributory negligence

I accept there's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mr A is to blame for the fact he didn't foresee the risk.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Mr A to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

Mr A hadn't invested in cryptocurrency before and so this was an area with which he was unfamiliar. I accept he only did very basic due diligence and that this was ineffective, but he was an inexperienced investor, and he wouldn't have known that a celebrity endorsement was a red flag or how to check the investment was genuine without having been told what to do by Santander. 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 that he had been able to make some withdrawals.

So, I don't think he can fairly be held responsible for his own loss.

Compensation

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

Recovery

Mr A 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'm satisfied there was no prospect of a successful recovery.

My final decision

My final decision is that Santander UK Plc should:

- refund the money Mr A lost from the second payment onwards, 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 Mrs S with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 27 July 2024.

Carolyn Bonnell
Ombudsman