DRN-4426973

The complaint

Mr H complains that Santander UK Plc didn't do enough to protect him from the financial harm caused by a job 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.

Mr H was searching online for additional employment and submitted his personal details and CV to various recruitment sites. In April 2023, he received a text message from an unknown number from someone claiming to work for a recruitment company I'll refer to as "H". She said she'd got Mr H's details from a recruitment site and asked if he was interested in a remote working opportunity with Company D.

Mr H confirmed his interest and was subsequently contacted by someone claiming to be from Company D, who I'll refer to as "the scammer". The scammer explained Company D was an online advertising company specialising in product optimisation and the role would require him to rate the products sold by its clients. He would be required to rate a minimum of 40 products and he would earn a commission from the sales of the items.

Mr H accessed Company D's website by following a link provided by the scammer, noting it included an about us section, FAQs and a 24/7 live chat option. The website also provided details of the company directors, giving a brief synopsis of their experience and stated the company specialised in 'digital growth'.

When Mr H agreed to take the role, the scammer told him to open an account on Company D's website. He was also added to a group chat with other employees. The 'partnership portal' was extremely professional and showed the value of various hotels and how much commission 'boosting' each property would generate. The balance on Mr H's account was pre-funded and after he'd used the entire balance, the scammer suggested he should purchase additional data to upgrade to a higher tier and increase his income.

The broker asked Mr H to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Between 7 May 2023 and 23 May 2023, he made seven payments to two cryptocurrency exchange companies totalling £4,605 using a debit card connected to his Santander account.

The scammer sent Mr H regular images and reports as his earnings increased. When he logged into the account and discovered a negative balance, the scammer explained he must purchase additional data and complete all the assigned tasks to recover his earnings. At this point, the scammer encouraged him to open an account with an "EMI" I'll refer to as "R", suggesting it was standard practice to dedicate an account for associated fees and costs.

Mr H realised he'd been scammed when the scammer stopped responding and the website disappeared. He complained to Santander but it refused to refund any of the money he'd

lost. It apologised for not having raised a scam claim on his behalf until 27 June 2023 and offered him £100 compensation. But it said he'd authorised the transactions and the claim wasn't eligible for chargeback rights.

Mr H complained to this service with the assistance of a representative. The representative argued that Santander should have intervened as it failed to pick up on numerous fraud indicators including multiple new international payees, the rapid depletion of funds, unusually high payments, a sudden increase in spending, a sudden change to the operation of the account and multiple payments made in quick succession. They also argued the payments were unusual for the account explaining the highest payment in February 2023 was £300, in March it was £1,323.29 and in April it was £700.

They said Santander should have contacted Mr H and asked him why he was making the payments, whether he'd been told to lie to the bank, whether there were any third parties involved, whether he'd been promised plausible returns and whether he'd discussed the position with anyone. And as he was confident the job was genuine he would have answered the questions honestly and it would have been obvious that he was being scammed. Santander further commented that Mr H should have raised a scam claim with the cryptocurrency exchanges he paid because they had a duty to Mr H given the loss was from his account with them.

Our investigator recommended that the complaint should be upheld. He was satisfied the frequency of the payments and sums involved meant it was a highly unusual and uncharacteristic pattern of spending, so Santander ought to have intervened.

He didn't think payments one to four were out of character because they were low value. But he thought payment five on 20 May 2023 was unusual because a payment of the same amount to the same merchant had been blocked shortly before at 4:04, but Santander didn't contact him. He felt Santander should have flagged the payment that followed the blocked payment as it was the same amount to the same merchant as the blocked payment.

He said if Santander had contacted Mr H and questioned him about the payment, it could have provided a scam warning which might have prevented his loss. Consequently, he recommended that Santander should refund the money Mr H had lost from payment five onwards.

He explained he didn't think Mr H could have foreseen the risk that D and H were scam companies because H was a clone of a genuine recruitment agency with offices in the UK, and there is also a consultant with the same name listed on their website. And D was a clone of a genuine marketing agency based in London. He noted that prior to the disputed transactions, Mr H had applied for multiple jobs and his details were on various job platforms, so it wouldn't have seemed unusual to receive a message from a potential recruiter about a job opportunity. So he didn't think the settlement should be reduced for contributory negligence.

Finally he explained Mr H couldn't have a valid chargeback claim against the cryptocurrency exchange companies because they'd provided the services as intended. And he thought £100 compensation was fair.

Mr H was happy with the outcome but Santander has asked for the complaint to be reviewed by an Ombudsman. It has argued that the funds arrived safely in Mr H's cryptocurrency account, so there was no loss to Mr H at the point of the payments. It has argued that he should complaint to the cryptocurrency exchanges as the loss was from those accounts, and it had no direct connection to the fraudulent payments or the actual loss.

Santander has argued 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 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 further argued that it acted in line with industry standards whilst following Mr H's instructions to transfer the money and that liability cannot sit with Santander as he authorised the card payments to an account held in his own name and it wasn't accountable for what he chose to do beyond that point.

It has argued that Mr H's account was in credit and he was paying accounts in his own name which he had access to. And that Mr H should accept liability as he made payments for a highly unusual 'job' which didn't sound like a genuine employment opportunity.

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.

I've thought about whether Santander could have done more to recover Mr H's payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Santander) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr H).

Mr H's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr H's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Santander's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

I'm also satisfied Mr H '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 H is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr H 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 H'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 May 2023 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 — 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 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 need to consider whether it ought to have intervened to warn Mr H 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 H 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 H normally ran his account. I'm satisfied that as he was paying a legitimate cryptocurrency exchange and the payments were for relatively small amounts which weren't unusual when compared to the normal spending on the account, there would have been no reason for Santander to have intervened when he made the first four payments.

Mr H then tried to pay £2,500 to M on 20 May 2023 but Santander blocked that payment for suspected fraud. It has confirmed that it didn't contact Mr H on that occasion due to there being no suitable contact number registered. Less than a minute later, he then made a payment of £2,500 to the same payee with no intervention. There were previous payments on the account for similar amounts for example, £2,500 on 5 September 2022, £2,500 and £1,000 on 27 September 2022, £2,425 on16 January 2023 and 2 March 2023 on £1,343.29, so the amount of the payment wasn't unusual. But I agree with our investigator that having already flagged a payment due to fraud concerns, Santander should reasonably have blocked the second attempt for the same reasons. Significantly, I don't think there having been no suitable contact number was a reason to have released the payment, rather it should have blocked the payment and written to Mr H either by post or email asking him to contact it to discuss the payment.

Santander could then have asked Mr H why he was making the payments and whether there was a third party involved and if so how he met them. And had it done so, I'm satisfied that as he believed the job was genuine and there's no evidence that he'd been coached to lie, he'd have said he was making payments in cryptocurrency for a job which he expected to earn commission for rating products online.

I'm satisfied there were enough red flags present for it to have been obvious to Santander that Mr H was being scammed and so I would expect it to have provided a tailored scam warning and some detailed advice on due diligence, including advice on how to check for cloned companies. And as I haven't seen any evidence that Mr H was keen to take risks, I think it's likely he'd have listened to and acted on that advice and stopped making payments to the scam. Because of this I'm satisfied that Santander's failure to intervene on 20 May 2023 represented a missed opportunity to have prevented Mr H's loss and so it should refund the money he lost from the fifth payment onwards.

Contributory negligence

I think Mr H should reasonably have stopped to consider why he was being asked to make payments in cryptocurrency for a role that he expected to be paid for.

However, he'd been actively seeking work, so there was nothing concerning about the way in which he was contacted. He thought the commission was reasonable and he's explained he had researched both H and D and was satisfied they were both legitimate companies and

that the opportunity was genuine. Unfortunately both companies were clones of the genuine companies. He was also added to a chat group with others he thought were doing the same role.

Having considered the circumstances of this scam, I'm satisfied it was sophisticated and I don't think it was unreasonable for Mr H to have thought it was genuine. He did some basic online research, and this had left him feeling confident about the role and I don't think it was unreasonable or negligent of him not to have contacted the recruiter directly, having already spoken to someone he thought was employed by H. Consequently, while there may be cases where a reduction for contributory negligence is appropriate, I don't think this is one of them.

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 they acted unreasonably when they were made aware of the scam.

My final decision

My final decision is that Santander UK Plc should:

- refund the money Mr H lost from the fifth payment onwards.
- 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 H with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 4 April 2024.

Carolyn Bonnell
Ombudsman