DRN-4767060

The complaint

Ms T complains that Santander UK Plc didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'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.

Ms T received a WhatsApp message from a woman who I'll refer to as "the scammer" who claimed to work for a company I'll refer to as "W". The scammer said she had an opportunity for part time work, explaining the role involved clicking on different products to submit product data which would automatically generate a rating and recommend the products to their respective marketplace, which in turn would improve the algorithm of each product.

Ms T had uploaded her CV to different recruitment sites so it wasn't surprising that she'd been contacted. She was told she'd have to add deposits to the platform to simulate 'buying' items, and that each task would use up some of the deposit, but she would earn a commission that would be added to the account. At the end of a 'set' of 40 tasks, the employee has the opportunity to withdraw their commission as well as the original deposit that was used to 'purchase' the items.

She was told she would earn a basic salary of 1,000 USDT a week and that she would have to top up the account using cryptocurrency. The scammer asked her to purchase the cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet.

Before she put any funds in, Ms T was able to withdraw a small amount back to her cryptocurrency wallet. She reviewed the website, which looked very professional and provided ID as part of W's verification checks. She was added to a group chat with other freelancers who regularly posted about their profits. She was also told to download AnyDesk remote access software.

Between 21 January 2023 and 7 March 2023, Ms T made seven payments to two cryptocurrency merchants totalling £6,720 using a debit card connected to her Santander account. She realised she'd been the victim of a scam when she tried to withdraw her profits and was told she'd need to deposit an additional £53,000 on top of the money she'd already paid.

She complained to Santander but it refused to refund any of the money she'd lost. It said the transactions were authorised to debit the account and they wouldn't be covered under the Contingent Reimbursement Model ("CRM") code because the code doesn't cover debit card payments.

Ms T wasn't satisfied and so she complained to this service with the assistance of a representative. The representative said Santander should have intervened and that the

scam would have been uncovered with some basic questioning. They said it should have asked Ms T about purpose of the payments and she would have explained that it was for a job, she'd been contacted on WhatsApp, she'd received small returns and she'd been asked to top up the account with cryptocurrency in return for commission. As these types of 'task based scams' are very common Santander would have known she was being scammed and warned her that a scam was taking place.

The representative explained Ms T had never purchased cryptocurrency before and the largest transaction from the account in the 12 months prior to the scam was a monthly standing order of £1,500 for her mortgage. Further, the account was taken into an overdraft after the final payment of £4,000 and Mr T had never been in an overdraft before, so it was out of character to suddenly began making large and frequent transfers to multiple different cryptocurrency exchanges.

Our investigator recommended that the complaint should be upheld. He said there wasn't a reasonable prospect of a successful chargeback as the funds went to legitimate merchants who had provided a service.

But he felt the £4,000 payment to B on 7 March 2023 should have been flagged as it was a large payment to a cryptocurrency merchant. He said Santander should have intervened and provided a tailored warning and as Ms T had already expressed some concerns to the scammer, he thought this would have prevented her loss.

However, he felt Ms T should share some responsibility for her loss because there was no evidence that she'd carried out checks before she sent the payments and it should have struck her as unusual that she was being asked to pay money for a job she was expecting to paid for. So, he recommended that Santander should refund the money she'd lost from 7 March 2023 onwards, less 50% for contributory negligence.

Santander asked for the complaint to be reviewed by an Ombudsman. It argued Ms T should pursue a claim against B given the loss was from the account she held with them. It didn't accept it should have intervened on 7 March 2023 because Ms T's account was in credit and the payment was made using her registered device via the Mobile Banking app from known IP addresses. It also argued that B is a genuine company which isn't on the Financial Conduct Authority ("FCA") warning list and she was paying an account in her own name having made previous payments to other cryptocurrency merchants. Further, she frequently made large payments and she had built a history of paying funds to cryptocurrency merchants, so £4000 wasn't unusual when compared with the transaction history for the previous 12 months.

Santander also argued that there was a call on 29 January 2023 when Ms T was warned about cryptocurrency scams. It argued that on this occasion she didn't discuss or seek advice about her concerns, which would have allowed it to provide more tailed guidance and education, suggesting any further scam chats wouldn't have prevented the scam. It also argued it's not fair or reasonable to predict what might have happened during a conversation if it had intervened.

It also argued there were a number of red flags indicating the job wasn't genuine including the fact she was contacted via WhatsApp, she had never heard of B, she couldn't find it online or on Companies House and she didn't question why she was being asked to make payments in cryptocurrency.

Finally, it 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 / 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”.

My provisional findings

I thought about whether Santander could have done more to recover Ms T’s payments when she 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 (Ms T).

I explained Ms T’s own testimony supports that she used cryptocurrency exchanges to facilitate the transfers to B. 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 Ms T’s payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail.

There’s no dispute that this was a scam, but although Ms T didn’t intend her money to go to scammers, she 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 Ms T'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 didn't 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 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 forfirms 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 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 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 Ms T when she 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 Ms T from financial harm due to fraud.

I considered the nature of the payments in the context of whether they were unusual or suspicious and I didn't think they were. All the payments were to legitimate cryptocurrency merchants, they were all to accounts in Ms T's own name and the first six payments were relatively low value and not unusual for the account, so there would have been no reason for Santander to intervene before the first six payments.

Our investigator felt the £4,000 payment on 7 March 2023 was unusual and that Santander ought to have intervened. I agreed B was a new payee which was a cryptocurrency merchant. But I didn't think the amount was high enough to have been concerning or that it was unusual for the account. This is because Ms T had recently made several high value payments to an account in her own name most notably £8,525.50 on 28 February 2023 and 6 March 2023, and £50,000 on 22 February 2023. I accepted these larger payments were to an account in Ms T's name, but this was also the case for the scam payments. And by the time she made the payment to B, she'd been making payments to a cryptocurrency

merchant since 21 January 2023, so this wouldn't have been unusual or concerning. Therefore I didn't think Santander missed an opportunity to intervene.

Compensation

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.

Recovery

Ms T had described that she paid an account in her 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

Ms T has said that she doesn't agree with the findings in my provisional decision. She has questioned why she wasn't asked about the outgoing payments and maintains Santander should refund her loss as it failed to protect her.

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.

I've considered Ms T's further comments but I'm afraid the findings in my final decision will remain the same as the findings in my provisional decision. As I explained above I don't think any of the payments were suspicious or unusual and so I don't think Santander missed any opportunities to intervene or to ask her about the outgoing payments.

Because of this, I remain satisfied Santander took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Ms T has lost money and the effect this has had on her. But for the reasons I've explained, I don't think Santander is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms T to accept or reject my decision before 24 May 2024.

Carolyn Bonnell
Ombudsman