DRN-4323044

The complaint

Miss T is unhappy that Santander UK Plc ("Santander") has not refunded her money after she became the victim of a safe account scam.

What happened

The circumstances that led to this complaint are well known to both parties, so I won't repeat them in detail here. But, in summary:

On 10 October 2021, Miss T entered her card details into a phishing email after clicking on a link. Soon afterwards she realised it was a scam and called the bank who blocked her card and reissued a new one. A few days later (13 October 2021) Miss T was contacted by someone purporting to be a bank employee and explaining her account had been compromised. Miss T subsequently transferred £1,774.80 and £2,883.88 from her current account and £1,973.67 from her savings account (a total of £6,632.35) into what she believed was a safe account. The bank tried to recover Miss T's funds once she notified it of the scam but only £6.77 remained in the beneficiary account.

The bank did not uphold the complaint. It said she authorised the transactions without completing appropriate checks to ensure the veracity of the call. It had provided her with appropriate warnings about this exact scam during a call on 10 October 2021.

Our investigator didn't uphold the complaint. She felt there was cause for concern before Miss T made the payments and that she didn't have a reasonable basis for believing the transactions were genuine. She also didn't think the payments were so out of character that Santander ought to have intervened.

Miss T did not agree. As the complaint could not be resolved informally, it's been passed to me for a 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.

I have carefully noted the representations made by all the parties, but I won't be addressing every single point that's been raised. It doesn't follow that the points haven't been considered, simply that I don't need to particularise every point in reaching an outcome I consider to be fair and reasonable in all the circumstances. I've instead concentrated on the issues I think are central to the outcome of this complaint.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Where the evidence is incomplete, inconclusive or contradictory, I reach my decision on the balance of probabilities – in other words, on what I consider is most likely to have happened in light of the available evidence and the wider circumstances.

There is no dispute that Miss T has been a victim of fraud and I am deeply sorry for that, but it doesn't automatically mean Santander is liable for some or all of her losses.

Did Miss T authorise the transactions?

The question of authorisation is a key one in a case of this kind. Because, although it's not in dispute that Miss T didn't set out to be scammed, under the Payment Services Regulations 2017 (PSRs), and general banking terms and conditions, she is presumed liable in the first instance if she authorised the transactions.

When Miss T reported the scam to Santander it wasn't clear whether she was accepting that she authorised the payments herself or whether she was saying someone else made them. Miss T was called by someone purporting to be from the bank and the evidence from the bank does suggest these were authorised payments. Whether Miss T made the transactions herself or was tricked into allowing them to be made (for example by providing secure account details or access via sharing computer screens) – means they are authorised, even though Miss T may have been tricked into doing so and was the victim of a scam.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

However, where a customer makes a payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though they authorised the payment.

The CRM Code

When thinking about what is fair and reasonable in this case, I've considered whether Santander should have reimbursed Miss T in line with the provisions of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) it has signed up to and whether it ought to have done more to protect Miss T from the possibility of financial harm from fraud.

There's no dispute here that Miss T was tricked into making the payments. She thought she was protecting her savings, but this wasn't the case. But this isn't enough, in itself, for Miss T to receive a full refund of the money under the CRM Code.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances.

One such circumstance might be when a customer has ignored an effective warning.

A second circumstance in which a bank might decline a refund is, if it can be demonstrated that the customer made the payments without having a reasonable basis for believing that:

- the payee was the person the customer was expecting to pay;
- the payment was for genuine goods or services; and/or
- the person or business with whom they transacted was legitimate

There are further exceptions within the CRM Code, but they do not apply in this case.

The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

I am also mindful that when Miss T made these payments, Santander should fairly and reasonably also 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). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Did Santander meet its obligations under the CRM Code and did Miss T ignore an effective warning?

The Code says that where firms identify APP scam risks in a payment journey, they should take reasonable steps to provide their customers with effective warnings. It also says that effective warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the customer is initiating the payment instructions.

The individual transfers were relatively small, (although I appreciate it's a lot of money to Miss T) and I don't think Santander ought reasonably to have identified a risk on the individual payments through the user interface. Banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

That said, it seems that Santander did provide a warning for 'friends or family' which is what Miss T selected at the time the payment was processed.

I haven't repeated the warning that was shown during the online payment process because Miss T's choice (albeit I appreciate this may have been under the scammer's influence) made it very difficult for Santander to give a tailored and impactful warning. It's also the case that, had answering 'transfer to own account' led to a warning that met the definition of 'effective' under the CRM Code (that's not a finding I need to make here), it would be irrelevant because Miss T didn't see that particular warning – so I can't say Miss T ignored an effective warning either.

Did Miss T have a reasonable basis for belief or could she have done more to mitigate her losses?

I need to consider not just whether Miss T believed she was sending money under instruction from the bank's fraud department, but whether it was reasonable for her to do so. I've thought about the steps Miss T took to reassure herself about the legitimacy of the transactions and whether it was reasonable for her to proceed with the payments.
Miss T teaches people not to fall for scams so has more awareness in general. The call with the bank three days before does highlight that Miss T reasonably ought to have been more cautious and taken further steps when she received the call from the scammer.

There were warnings within the call on 10 October 2021 about the exact scenario that followed. The security officer made it clear exactly what would happen next following clicking on a phishing email link as Miss T had done. In particular he said "*imagine you get a call telling you your account is not safe and that you need to transfer your money from one account to another for safety reasons*". He went on to say that criminals are calling

customers pretending to be from there bank or other organisations and advising to move money from their account for security reasons.

The security officer reassured Miss T her account was secure and made it clear this would be the premise on which a scammers call would be based. He said never transfer money to another account and that if someone tells you to do so - *it's a scam*. He covered off number spoofing and repeated warnings to never transfer money out of your account for security reasons. During this call Miss T confirmed she would not be moving money by phone and that she wouldn't do what a caller in this scenario was telling her to do.

The security officer told Miss T that if she was concerned, she should call the number on the back of her bank card.

There was no indication during this call that there would be any follow up call from Santander, or any further action was needed. And I feel the bank did all it could to reassure Miss T her bank account was safe - which it was – certainly from any unauthorised transactions connected with the phishing email. And Santander had warned Miss T about being tricked into authorising a transaction herself – which was now the only risk to the account on the back of the phishing email.

There were other signs that things were not quite right during the payment journey. The confirmation of payee warnings for all three payments warned '*account name does not match'.* I appreciate Miss T does not recall these and I also appreciate calls like this do create pressure – but overall given everything I've said above, I don't think Miss T had a reasonable basis for belief.

Vulnerability under the code

There are provisions under the code which might lead to a refund, even when a customer doesn't have a reasonable basis for belief. The relevant part of the Code, says:

A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis.

So, this is the definition of vulnerability in relation to the Code. It isn't about being medically ill or medically vulnerable – although that may be a factor. What's key is whether Miss T was vulnerable to the extent that she wasn't in a position to protect herself from the particular scam she fell victim to.

It's clear from all that has been said Miss T was going through a lot – in particular she has some serious medical issues from which she was slowly recovering from at the time. I'm sorry to hear of all Miss T has been through. Not just in terms of this scam, but also what's happened to her prior to the scam.

But I've considered whether there were vulnerabilities present at the time to such an extent that Miss T was unable to take steps to identify the scam she fell victim to or to recognise steps she might take to test the legitimacy of what she was being told by the fraudster. To do so I must consider the details of the scam, Miss T's actions throughout, and the wider circumstances of what was happening in her life at the time.

I don't doubt Miss T has suffered as a result of her physical well-being. But there is also evidence within the circumstances that suggests she was capable of taking steps to protect herself from fraud and financial harm. For example, she was quickly able to

identify the email she had clicked on the link for was fraudulent and she was able to call the bank to notify it. She engaged with the adviser during this call and did not come across as vulnerable. After her claim was declined Miss T told Santander she was struggling to breathe at the time of the transactions. I don't have any indication of what happened on the call with the scammer but on the call three days earlier (other than some audible coughing) Miss T was clearly able to articulate herself and there were no signs of breathing difficulties then. The medical letter of 6 October 2021 (a week before the scam call) indicates mild shortness of breath.

Miss T even explained she helps the elderly with fraud and scams. Overall, I think there was more she might reasonably have done that would have led to the scam being uncovered when she was called a few days later. For example, she could have called the number on the back of her bank card as agreed in the call with Santander three days before.

Having thought very carefully about everything Miss T has told us, whilst I'm not saying Miss T's circumstances had no impact on her at the time, I'm not persuaded that it would be unreasonable to expect her to have protected herself against the particular scam she fell victim to. And so, I don't find that Santander need refund Miss T's entire loss under the vulnerability clause of the code.

Should Santander have done more to try and prevent the scam and protect Miss T?

As well as the CRM Code, a bank still has wider obligations and a duty to protect its customers, as far as is reasonably possible, against the risk of financial harm from fraud and scams. As such, there are circumstances where it might be appropriate for a bank to take additional steps or make additional checks before processing a payment to help protect its customers from the possibility of financial harm from fraud.

Miss T has commented on other banks and systems where transactions have been reversed but I can't comment on that. I am looking at Miss T's case against Santander. Every case is judged on its own merits and what may appear (on the face of it) to be a similar set of circumstances, may often transpire not to be the case.

As I've already mentioned above, Banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

There is no documented threshold for intervening on a payment, but it is for me to decide when assessing this particular case - what I think is fair and reasonable in all the circumstances. The amount of money Miss T sent, while clearly not insignificant to her, doesn't in and of itself suggest to me any heightened risk of fraud. Santander did stop a fourth payment.

Did Santander do enough to recover Miss T's funds?

I've thought about whether Santander took reasonable steps to recover Miss T's funds once it was made aware she was the victim of a scam. The scam payments were made on 13 October 2021 between 19:14 and 19:32 and Miss T reported the scam to Santander on 14 October 2021. Santander contacted the receiving bank the same day but all except £6.77 (which I can see was returned to Miss T a week or so later) remained. I have seen the evidence which shows, all but a further £1 had left the scammers account within minutes of the final transfer on 13 October 2021 and the remaining £1 withdrawn two hour later. So before Miss T had a chance to report it to Santander. This is not unusual as scammers usually remove funds within hours. I don't think Santander couldn't reasonably have done

any more to try and recover Miss T's money.

I realise my decision will be a significant disappointment to Miss T. I sympathise with her circumstances, and I am sorry she has fallen victim to a scam. But having considered all the evidence and arguments, I'm not upholding her complaint.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 3 November 2023.

Kathryn Milne
Ombudsman