

The complaint

Miss L is unhappy Santander UK Plc (“Santander”) won’t refund the money she lost as the result of a third-party scam.

What happened

I’m not going to cover all the points raised in detail. But, in summary in April 2023, Miss L received a call in which the caller purported to be from the bank but who, ultimately, turned out to be a scammer. The scammer persuaded Miss L that her account was under attack and she needed to move her money to a safe place. Miss L moved £3,000 from her Santander account to what she thought was a ‘safe’ account. Santander blocked a second payment and that was when Miss L realised she’d been the victim of a scam.

Santander felt that Miss L had been provided with an effective warning when making the payment and it said she hadn’t conducted sufficient checks before proceeding. It also felt it took appropriate steps to try and recover Miss L’s funds when she reported the scam, but the funds had already been removed except for £100 it refunded.

Our investigator upheld the complaint in part. She felt that Miss L didn’t have a reasonable basis for belief, but she didn’t think Santander provided an effective warning. So she recommended both parties share in the responsibility for the loss.

Miss L accepted the view. Santander didn’t agree – it felt its warning was effective.

As the case couldn’t be decided 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.

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 have been good industry practice at the time.

It’s important to highlight that with cases like this I can’t know for certain what has happened. So, I need to weigh up the evidence available and make my decision on the balance of probabilities – in other words what I think is more likely than not to have happened in the circumstances.

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

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

When thinking about what is fair and reasonable in this case, I've considered whether Santander should have reimbursed Miss L in line with the provisions of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code) it has signed up to and whether it ought to have done more to protect Miss L from the possibility of financial harm from fraud.

There's no dispute here that Miss L was tricked into making the payment. She thought she was speaking to her bank, and this wasn't the case. But this isn't enough, in itself, for Miss L to receive a full refund of the money under the CRM Code.

The CRM Code

Under the CRM Code the starting principle is that a firm should reimburse a customer who is the victim of an APP scam, like Miss L. The circumstances where a firm may choose not to reimburse are limited and it is for the firm to establish those exceptions apply. They are:

- the customer ignored an 'effective warning' by failing to take appropriate steps in response to that warning; or
- the customer made the payment without a reasonable basis for believing that:
 - o the payee was the person the customer was expecting to pay,
 - o the payment was for genuine good or services, and/or that
 - o the person or business with whom they transacted with 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 L 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 it processed 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?

The CRM Code 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.

Santander did identify a risk with the payment Miss L made (and it successfully blocked a second payment) and provided warnings. It has provided us with the "dynamic" questions Miss L saw, along with the responses Miss L gave.

I appreciate the “dynamic” questioning was relevant to the scam which Miss L fell victim to and included the question, “have you been contacted and told to move money to another account?” but I don’t think this warning is effective – especially in the context of the circumstances of a safe account scam.

There is insufficient evidence of how the scam chat would’ve appeared (visually) to the customer during the payment journey. So I can’t fairly say the warning was visually impactful. There’s also a lot of questions to navigate, which during a safe account scam could be difficult to follow - particularly so given the level of coaching that’s often involved in this type of scam and the fact the consumer genuinely thinks they are speaking to the bank. It’s not specific enough - for example it doesn’t ask specifically whether the bank had contacted her or ask whether she was on the phone to the bank – which is typical of this sort of scam and would more likely have resonated with the circumstances Miss L found herself in.

Overall, Santander hasn’t demonstrated that an effective warning was shown. It therefore follows that I can’t say Miss L ignored an effective warning. In any event, I would question if Miss L would’ve read the warnings if she was being guided by the scammers and also considering that Miss L is dyslexic – certainly her testimony indicates she doesn’t recall them.

In accordance with the CRM Code, if a business fails to meet the standards set out for it, it may be responsible for meeting the cost of reimbursing a customer who has fallen victim to an APP scam. So, I’ve gone on to consider whether any of the other exceptions to reimbursement apply.

Did Miss L make the payments without a reasonable basis for belief?

Miss L has accepted the investigator’s conclusions including on this aspect of the CRM Code but for completeness, I agree with the investigator and broadly for the same reasons.

Miss L says she received a call from a private number and the caller didn’t know any details about her apart from her name. From what Miss L has said – she wasn’t taken through a security process which is something I think she ought to have reasonably expected of her bank. And she didn’t make any attempts to verify the legitimacy of the caller. It seems she did query with the scammer as to the need to transfer her money. She said she told the scammer the bank would normally just block her card. I appreciate calls like this are designed to disrupt a victim’s thinking but overall, I think there were enough signs here that things weren’t quite right and there was more Miss L could have done – which would likely have revealed this was a scam. So I feel it’s fair for Miss L to share in the responsibility for her loss.

Where the business failed to meet its obligations under the CRM Code, but the consumer did not have a reasonable basis for belief, the bank should pay the consumer 50%.

Recovery of funds

I've also thought about whether Santander took reasonable steps to recover Miss L's funds once it was made aware she was the victim of a scam. The first scam payment was made at 17:34 on 9 April 2023. A second payment was blocked at 17:38 and the scam was revealed. Miss L called the bank at 18:36. Although Santander didn't contact the beneficiary bank until the following day at 9:43 all but £100 (which I understand has been returned to Miss L) had left the account within 35 minutes of Miss L's call. Even if Santander had reached out following Miss L's call the previous day – I think it would have been too late for Santander to have recovered any further funds.

Putting things right

In order to put things right for Miss L, Santander UK Plc should:

Refund 50% of Miss L's remaining loss (ie £3,000 less £100 recovered = £2,900) so £1,450

To compensate Miss L for being deprived of the money she lost, Santander should add simple interest¹ at the rate of 8% per annum from the date her claim was declined to the date of settlement.

My final decision

My final decision is that I uphold this complaint in part and require Santander UK Plc to put things right for Miss L as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss L to accept or reject my decision before 5 June 2024.

Kathryn Milne
Ombudsman

¹ If Santander is legally required to deduct tax from the interest it should send Miss L a tax deduction certificate so she can claim it back from HMRC if appropriate.