

Complaint

Ms L is unhappy that Santander UK Plc didn't reimburse her after she fell victim to a scam.

Background

In March 2023, Ms L fell victim to a safe account scam. She received a text message that appeared to be from Santander asking her to confirm whether she made a payment for a £865.37. It asked her to reply 'N' if she hadn't. She replied to confirm that she hadn't made the payment in question.

Shortly afterwards, she received a phone call from someone who claimed to be an employee of the Santander fraud team. Ms L tells us that the scammers knew some of her personal information and so she thought it was plausible that the call was genuinely from Santander. They told her that the security of her account had been compromised and that it was necessary for her to move her money to another account. She made six payments of £7,122 in total.

Once she realised that she'd fallen victim to a scam, she notified Santander. It didn't agree to refund her. Ms L wasn't happy with that response and so she referred her complaint to this service. It was looked at by an Investigator who upheld it. Santander didn't agree with the Investigator's opinion and so the complaint has been passed to me to consider and come to a final decision.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law 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, that isn't the end of the story. Santander is a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM code"). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams, like the one Ms L fell victim to, in all but a limited number of circumstances.

Under the CRM Code, a firm may choose not to reimburse a customer if it can establish that:

- The customer made the payment without a reasonable basis for believing that ... the person or business with whom they transacted was legitimate; or
- The customer ignored an effective warning in relation to the payment being made.¹

I'm satisfied that Ms L did have a reasonable basis of belief here. The way the relevant test

¹ There are further exceptions within the CRM code, but they don't apply here.

is written in the CRM Code means it's not entirely objective. I'm able to consider the wider circumstances in deciding whether the customer's belief was reasonable. In view of that, it's worth pointing out that Ms L had made a complaint to this service in 2022 about unauthorised activity on her Santander account. In March 2023, her case was being looked into by one of our Investigators who was exploring the possibility that one of her devices had been compromised by malware. Ms L had recently downloaded software to her device to check it for malware threats and had found several things that were, potentially, of concern.

As a result, she was more receptive to the plausibility of the message she received from the fraudster – i.e., that the security of her account had been compromised. She's told us that being contacted about potential fraud put her in a state of panic. I don't think it's far-fetched to think that this would've impaired her ability to critically judge whether there was a real threat or not.

Santander has pointed out several factors which it says make clear that this wasn't a legitimate enquiry from its fraud team. In particular, it has pointed out that she was called from a mobile number, rather than an official Santander number and that the text message didn't appear in an existing chain of messages from the bank. It's also argued that the fraudsters don't appear to have gone through the standard security question process with Ms L. It says this is something she would've been familiar with because she'd made a fraud claim to the bank the previous year. I'm not persuaded by those arguments. In the cold light of day, Ms L might have recognised that the message and the call couldn't have been from Santander. But her state of mind at the time meant that she was significantly more receptive to the likelihood that it was.

I've also considered whether the second exception applies here. The CRM Code sets out specific criteria that a warning needs to meet if it is to be considered an "*effective warning*." Santander did display warnings to Ms L when she made these payments. However, those warnings were dynamic – their contents were generated based on the answers she gave to its questions while making the payments.

At the direction of the scammer, Ms L gave misleading information about why she was making the payments. That meant that the warnings displayed weren't relevant to her circumstances and so couldn't meet the requirements under the CRM Code to be effective. Ms L has said that she answered the questions the way she did because the fraudsters told her it was necessary to do so. I don't think it was unreasonable for her to have followed their guidance once she'd accepted in her own mind that she was genuinely dealing with her bank's fraud team.

This meant the bank's efforts to protect Ms L from fraud risk were hamstrung. I recognise that's not Santander's fault. It couldn't have known the real reason Ms L was making the payments and displayed a relevant warning. Nonetheless, it still means that it can't rely on the effective warning exception to reimbursement here.

Final decision

For the reasons I've set out above, I uphold this complaint.

If Ms L accepts my decision, Santander UK Plc needs to:

- Refund the payments she made in connection with the scam
- Add 8% simple interest per annum to those payments calculated to run from the date it declined her claim under the CRM Code until the date it pays her a settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or

reject my decision before 11 October 2024.

James Kimmitt
Ombudsman