

The complaint

Ms R complains that Santander UK Plc won't refund her the money she lost after she fell victim to an Authorised Push Payment (APP) email intercept scam.

What happened

Both parties are aware of the circumstances surrounding this complaint, so I won't repeat them in full here.

But briefly, both parties accept that, on 8 December 2023, Ms R made a payment for £6,000 that she believed was to a building firm for electrical works that had been completed on her home. But unknown to her at the time, a scammer had managed to intercept a genuine email from the building firm and add their account details on to the message, requesting the payment.

Ms R has explained that she was having extensive renovation works carried out and that the electricians had been recommended to her by her builder, who had worked with them over many years. She was also aware that a payment was due for £6,000 to cover 'first fix' work.

As the fraudsters intercepted a genuine message, the email address it was received from appeared to be from the same employer of the electrical firm, with whom Ms R had already been corresponding. The emails from the fraudster explained that the firm were transitioning to a new company name and were changing their financial provider and went on to provide bank details that Ms R should use for her payment.

Believing everything to be genuine, Ms R went ahead and made the payment. Ms R realised something was wrong when, a few days later, the genuine electrical firm contacted her and asked when the payment would be made. On speaking to her builder and the electrical firm she realised she'd been scammed.

Ms R raised a fraud claim with Santander. It investigated Ms R's claim and considered its obligations to provide her with a refund. Santander is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Santander says one or more of those exceptions applies in this case.

Santander has said Ms R ignored an 'effective warning' when making the payment to the fraudster. Santander also initially said that Ms R didn't have a reasonable basis for believing she was paying a genuine company and it didn't think Ms R had taken reasonable steps or carried out checks to confirm this.

Unhappy with Santander's response, Ms R brought her complaint to this service. One of our Investigator's looked into things and thought the complaint should be upheld in full. On receiving our Investigator's view, Santander changed its stance and offered a 50% refund to Ms R. This was on the basis that it partially agreed with our Investigator's position – in that it agreed Ms R had proceeded to make the payment with a reasonable basis for belief, but it maintained that it had provided an effective warning.

Ms R declined Santander's offer, so the complaint has been passed to me for a final 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; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

When thinking about what is fair and reasonable in this case, I've considered whether Santander should have reimbursed Ms R under the provisions of the CRM Code and whether it ought to have done more to protect Ms R from the possibility of financial harm from fraud.

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

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning.
- The customer made 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 these don't apply here.

Santander has already accepted that Ms R had a reasonable basis for belief when making the payment. So, all that's left for me to consider is Santander's representations about whether Ms R ignored an effective warning(s) when making this payment.

Having considered this complaint, I am satisfied that under the terms of the CRM Code, Santander should have refunded the money Ms R lost in full. I am not persuaded any of the permitted exceptions to reimbursement apply in the circumstances of this case. I'll explain why.

Santander has said the following warning was presented to Ms R at the time she made the payment.

'Paying for a service

Criminals can intercept communications between you and businesses you trust. They give you their account details, but this account belongs to the fraudster. If this happens, it means you'll send your money to them and it can't be recovered.

It's important you choose the true reason for this payment and answer all questions honestly. This is so we can help protect you from fraud. If anyone has asked you to lie or mislead the bank, or to choose a different payment reason, this is a scam and you must stop now.

We now need to ask you some specific questions before you send your money.

Paying for a service

Criminals can intercept communications between you and businesses you trust. They can pretend to be almost anyone, including your bank, a business, the police, HMRC or even a family member. They give you their account details, but this account belongs to the fraudster.

You must check the account details with the business you're paying in person or by calling them. You must do this even if you've been in regular contact with them. Don't use the number in the message requesting payment. Use a trusted number or one that's publicly available.

If you're not comfortable or want to complete further checks, stop and cancel the payment now.'

Ms R was then asked to confirm where her payment was going, which she confirmed was 'To pay for building work'. Santander then provided this further information;

'Rogue traders and doorstep scammers

A rogue trader may offer you a service you don't need. They may claim to have noticed something about your property that needs work or improvement. They tell you the work is urgent and often ask for payment upfront.

Do your own checks to make sure the work's needed. You must be sure the person you're dealing with is genuine and reputable. You can speak to someone you trust for a second opinion, use online reviews and get other quotes.

Don't make this payment without being sure who you're dealing with.'

Ms R is then asked whether she has carried out checks to make sure the person is genuine and reputable and answered 'yes'. Following this Santander go on to provide the following;

'Be aware of payment redirection scams

Criminals can intercept communications between you and your builder and replace genuine account details with those belonging to the fraudster. If this happens, it means you'll send money to them and it can't be recovered.

You must check the account details you receive with your builder. This is to make sure they're legitimate before you send your money. You must do this even if you've been in regular contact with your builder.

Check the account details in person or by calling. Don't use the number in a message requesting payment. Use a trusted number or one that's publicly available.'

Ms R is then asked whether she has carried out checks on the account details and answered 'yes'.

She was then asked whether the account she was paying money to was in the builder's business name. Again, Ms R answered 'yes'. Following which a 'Confirmation of Payee' check advised the details matched.

Lastly Santander asked if Ms R was comfortable making this payment and confirmed she'd be unlikely to get the money back if the payment was part of a scam. She confirmed she was and the payment was then processed.

Having considered the information that Santander has submitted carefully, it does not persuade me to reach a different view to that of our Investigator. I appreciate Santander has made attempts to tailor its questioning here and that further advice it provided would've been impacted by Ms R's answers to the questions asked. However, I don't think the warning it provided was sufficiently impactful, or brought email intercept scams to life enough to make Ms R question if she was at risk of financial harm.

A key element to this scam was that it was a genuine chain of emails that had been intercepted. At the time, this method of interception would have been well known to Santander, yet nowhere in the warning does it mention email interception specifically or question how Ms R had received the bank details, to which she was asked to send her payment.

I don't think the warning Santander provided went far enough in explaining how an intercepted email might look (and how well hidden the interception can be, including being received from the genuine email address, alongside a genuine message) and as a result, the warning hasn't covered the key hallmarks of this scam and therefore has lost its impact.

I also don't think the 'rogue trader' element of the warning would have resonated with Ms R. By the time she was making this payment work, had been carried out and the scenarios detailed in this part of the warning weren't reflective of what was happening in her circumstances.

I'm mindful Santander has argued that Ms R wasn't truthful when answering 'yes' to a question as to whether she had carried out the checks it had set out in its warning. But while the warning advises Ms R to confirm the account details by phone or face to face, without the additional information on how intercepted emails can appear, I think it's understandable why Ms R didn't feel she needed to conduct these additional checks, as the potential risk she was facing was less apparent to her.

Therefore, overall and when considering the CRM code, I don't think the warnings Santander has provided can be said to be 'effective'. It didn't go far enough in describing and bringing to life the specific risk that faced Ms R and therefore she shouldn't be held liable for her losses on this basis.

Putting things right

For reasons explained above, I now direct Santander UK Plc to:

- Refund Ms R the £6,000 she lost to the fraudsters.
- Pay 8% interest on this amount, from the date it declined her claim until the date of settlement.

My final decision

My final decision is that I uphold this complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 23 December 2024.

Stephen Wise
Ombudsman