DRN-5511997

The complaint

S, a limited company, has complained The Royal Bank of Scotland plc did nothing to stop four payments being made by the business to fraudsters.

What happened

S is a limited company with two directors, Mr A and Mr W. Mr A, along with professional representatives, has brought S's complaint to the ombudsman service. Ms S was the financial controller for S and was authorised to set up and make payments from S's account with RBS. Their working arrangements were that invoices were passed from the directors to Ms S for payment. At the time of this fraud both Mr A and Mr W were overseas for work.

On 17 November 2022 S received an email from Mr W confirming an invoice required payment. This met their normal working arrangements. The invoice had been sent by Mr A to Mr W and forwarded to Ms S. Ms S arranged payment of £42,000 to this company.

This first payment provoked an alert within RBS who blocked the payment. Payment was then made following a phone conversation between RBS and Ms S.

A series of emails from Mr W followed, including another invoice from a different company. This was for £98,400 and Ms S arranged payment. The same day she also arranged payment of a (bona fide) invoice for £220,539.60, which required additional authorisation provided by Mr A later that evening.

On 24 November the payment for £98,400 was returned to S. Emails between (the fraudster impersonating) Mr W and Ms S confirmed it would be best to split the payment into two. On 24 and 25 November, S paid this invoice by making two payments of £49,200.

A further invoice was sent. Ms S was concerned at the amount of money leaving S's account and sent Mr W a WhatsApp message querying this. Mr W confirmed he'd not passed any of these invoices to her for payment.

It became clear that S was a victim of a sophisticated scam where scammers had cloned Mr W's email address, imitated his style and shared invoices which appeared genuine. Mr A's email address had been disguised by the change of one letter for a digit, so he'd also been unaware of what was going on.

S contacted RBS and asked for their assistance in tracking their money down and ensuring all was done so they could be refunded. RBS contacted the beneficiary bank, but they were only able to recover £8,544.45 from the beneficiary account which was returned to S on 11 January 2023. They confirmed they didn't intend to refund S any further.

S remained unhappy with RBS's lack of refund so brought their complaint to the ombudsman service.

Our investigator reviewed the evidence. There was no dispute S had authorised the payments. He could see that RBS had intervened during the journey of the first payment and

had asked Ms S whether she'd undertaken checks about the payment. He didn't believe anything different would have happened if they'd raised further questions to Ms S.

He wasn't going to ask RBS to do anything further.

S have asked an ombudsman to consider their complaint.

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.

Having done so, I've reached the same conclusion as our investigator. I'll explain why.

Where there is a dispute about what happened, I have based my decision on the balance of probabilities. In other words, on what I consider is most likely to have happened in the light of the evidence.

S was scammed. This has had an impact on employees and the directors and has caused considerable distress. I am very sorry about this.

I won't be writing in detail about the different aspects of what happened. I hope neither party thinks I'm being disrespectful but much of what happened isn't in dispute. There's no doubt S was scammed. I've seen the emails which formed the fraud. I can't see how S would have identified any real differences. And it's clear that the email address mirrors Mr W's.

S also undertook confirmation of payee checks before setting up new payees for the two invoices they paid.

I've also noted the detailed view – laying out the different steps of what happened – our investigator provided in March 2025. I see no need to repeat some of this, but I have obviously taken all of the evidence into account in coming to my decision.

There's no dispute that S made and authorised four payments totalling nearly £240,000 from S's account. I'm therefore satisfied the transactions were authorised under the Payment Services Regulations 2017. S's total loss is £131,855.55, taking into account the small amount RBS was able to recover from the beneficiary bank.

Our starting point is that banks and electronic money institutions are required to follow their customer's instructions. But, as RBS will be aware we take into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time of the payments.

In this case I have also noted:

- S had a considerable financial turnover in 2022 so there were many payments in and out of their main account. Payments of around £50,000 in value were not unusual and considerably higher-value payments were also made and received. S makes very large payments to two or three businesses they have a regular payment relationship with.

- S had only held a business account with RBS since January 2022, but I would still have expected RBS to have built up a reasonable understanding of B's business and normal account usage.

- There's an email from RBS timed at 11:40 on 18 November 2022. Their fraud monitoring service had identified the payment for £42,000 as potentially fraudulent and the payment was put on hold until Ms S contacted the banking security team. There was then a phone call between Ms S and RBS. In response to a question, she confirmed the invoice had been received by email and that she'd undertaken checks with the director on the back of this to ensure it was genuine. It's clear from listening to the call, RBS were looking for Ms S to confirm she'd either checked by phone or in-person. I suspect Ms S felt that the email conversations she'd been having with Mr W (and where Mr A was copied in) amounted to proper checks.

- There were no further checks carried out by RBS for the other three payments made for the second fraudulent invoice. Based on the fact the amount for this payment was just under £100,000, I may have expected further intervention. RBS has confirmed their checks aren't based on value alone. I see this is true as the payment S made for more than £220,000 on 22 November (a few hours after the payment for £98,400 was made) was not subject to any intervention by RBS. They have stated that payments genuinely made by a customer using their debit card or secure online banking that do not meet any known fraud or scam trends at the time won't necessarily trigger a security check.

- After reviewing the emails between Ms S and Mr W, I am sure her response to any further intervention would have been the same as it was to the first conversation between herself and RBS on 18 November. In any case, this second payment was returned. The two further payments would not, I believe have merited further intervention. I note Ms S only became concerned when a third invoice was received and she knew that payment for this would be leaving the account considerably less healthy.

- I specifically asked S about the payment made for over £220,000 and why this required additional authorisation by Mr A. They confirmed at the time Ms S exercised her discretion and only asked for further authorisation for payments that were large or with which she was unfamiliar. Asking for further authorisation generally involved a call or WhatsApp message alerting the director to what was needed. In this case I can see this transaction was finally authorised at 19:15 by Mr A.

- I did consider whether Mr A (whilst authorising this large transaction) would have had an opportunity to review other transactions on the account and would therefore have noticed a transaction for £98,400 made that day to a new service provider. I'm not convinced he'd have specifically noticed this when I consider the number, type and value of transactions normally made from this account. It's also worth stating that when authorising a payment, I don't think Mr A would have generally been checking other account activity.

In my review of the evidence, I've considered whether RBS should have recognised that this business was at risk of financial harm from fraud and done more.

I'm very aware that S is a small business so I have not used the criteria I may have considered appropriate for an individual consumer but in this case, I don't believe RBS should have done more.

It's clear from the procedure I can see after they identified the first payment as potentially fraudulent that RBS would be contacting Ms S, rather than one of the two directors. I've asked RBS whether there were any circumstances in which they'd have reached out to any of the two directors. They've confirmed their general approach would be to contact the person who keyed the transaction into the system. This is specifically to rule out scams

which are based on a variation of the Chief Executive scam and to see how the financial controller received this message. Based on what I've stated above, I'm not sure that any further intervention by RBS would have resulted in the payments made to scammers not occurring.

Overall, I don't think it would be fair and reasonable to expect RBS to have done anything further.

I am sure S, and its directors, will be disappointed in this outcome. I can see there's been some consideration about pursuing the beneficiary bank and that avenue remains open to them.

My final decision

For the reasons given, my final decision is not to uphold S's complaint against The Royal Bank of Scotland plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask S to accept or reject my decision before 10 November 2025.

Sandra Quinn
Ombudsman