DRN-4285580

## The complaint

A company which I will refer to as 'F', complains that The Royal Bank of Scotland Plc won't reimburse the money they lost following an Authorised Push Payment (APP) scam.

## What happened

The background to the complaint is known to both parties and so I won't repeat it at length here.

Briefly, in July 2019, F was in correspondence with one of their suppliers about some pending payments to them. The supplier emailed F stating that they made an error in the final invoice, and they enclosed a revised one along with details of the bank account to which the payment should be made.

The following day F received another email purportedly from the supplier stating that they made another error in the invoice which they sent the previous day. The email said that the suppler had 'updated' their bank account details, which they failed to amend in the invoice. The email provided new bank account details.

Unfortunately, unknown to F, this email was from a scammer who had intercepted the previous email exchange between F and the supplier. The scammer also provided a revised invoice with the new bank account details. One of F's staff attempted to make the payment to this account, but it appears that they encountered some difficulties. So, they emailed back asking for confirmation of the account details. The scammer reconfirmed but also said that if F had any issues, they could provide details of a different account with another bank to send the money to. However, it seems that meanwhile the staff managed to resolve the issue and proceeded to make the payment.

The scam came to light about two weeks later when the genuine supplier pursued F for the payment. F contacted their bank RBS, who in turn contacted the recipient's bank. Unfortunately, no funds reminded in the recipient's account.

In early 2022, F complained to RBS through their representative. The representative said that the payment was out of character and therefore the bank should have intervened. And had the bank made an appropriate intervention, the scam could have been prevented. Therefore, they said that the bank should reimburse F the loss they incurred. RBS did not agree.

One of our investigators reviewed the complaint and concluded that it couldn't be upheld. They said that RBS correctly followed F's payment instructions. The payment wasn't particularly unusual or suspicious in appearance to the bank at the time, considering the company's normal account and payments activity. In addition, F isn't covered by the CRM Code as it is not a 'micro-enterprise'. The investigator also noted that RBS took action swiftly on being advised of the scam. In view of all this, the investigator concluded that RBS hadn't done anything wrong in this instance and so it doesn't have to take any further action.

F did not agree. Their representative reiterated that the payment was out of character to normal account activity and so the bank ought to have intervened. They said that the payment was the largest to a new payee over a one-year period. All other large transactions were regular payments with low fraud risk, such as to HMRC. They further said that had the bank intervened, with proper questioning of the payer, the bank would have understood that the account details were provided via email which it would have recognised as a potential scam. In such an instance, the bank would then have advised the payer to call the supplier and confirm the account details before making the payment. At that point the scam would have come to light.

**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 agree with the Investigator, essentially for the same reasons.

As the Investigator has said, in broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that its customer authorises it to make. However, there are circumstances where it might be appropriate for the banks to take additional steps – as for example have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud.

I have reviewed F's account statements for several months prior to the payment to the scammer, to understand the general account activity. Over the period, I see that this was an active account. There were several large payments in and out of the account. F says that many of the large payments were 'low risk' payments such as for wages and to HMRC. Nevertheless, I see that there are several other payments of high value. The disputed transaction was higher in value than these transactions. However, occasional higher payments could happen on an account, and I am not persuaded that the payment stood out as highly unusual compared to the normal account activity for the bank to have intervened.

The payment was to a new payee, but that in itself would not have caused a concern to the bank. Further, as the investigator has said, it didn't consume all or most of the funds in the account – which might have been an indicator the account was at risk of fraud.

Ultimately, it is a matter for RBS as to how it chooses to configure its fraud detection systems and strike a balance between allowing its customers to transact business and questioning transactions to confirm they are legitimate. But where it is alleged that it didn't do enough to prevent a loss which resulted from an authorised push payment fraud, I will look into the circumstances of the case and based on what I have seen, decide whether in that case the bank could have fairly and reasonably done more.

After taking all of the above into account, I can't say that the disputed payment sufficiently stood out from the prior account activity to reasonably have prompted RBS to take further action. I'm not persuaded that there was enough here for me to find that RBS was at fault in carrying out F's payment instruction in line with its primary obligation to do so.

Further, from what I can see, there was no delay on the part of RBS in contacting the recipient's bank on being advised of the scam.

On some occasions, it's possible to consider whether a customer is covered under the Contingent Reimbursement Mode Code which came into effect from May 2019. However, F

aren't not covered by the Code. Where the customer is a business (as in this case), the Code only applies if they were a micro-enterprise at the time the transaction took place. For this purpose, a micro-enterprise is essentially an enterprise which employs fewer than 10 persons. And if they employ fewer than 10 persons, then at least one of their annual turnover or total gross assets should not exceed €2 million. In this case F isn't a *micro-enterprise* as it employed more than 10 persons at the relevant time. So unfortunately, they aren't covered by the CRM Code either.

I know this will come as a disappointment to F given that they had fallen victim to a callous scam. But I can only make an award against a bank if that bank had done something wrong and that led to F's loss. In this case, for the reasons given I am not persuaded that there was any error or omission on the part of RBS which resulted in F's loss. As such I can't fairly or reasonably ask it to refund their loss.

## 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 F to accept or reject my decision before 21 December 2023.

Raj Varadarajan
**Ombudsman**