

The complaint

R, a limited company, complains that Metro Bank PLC won't refund the money it lost when it was the victim of a scam.

What happened

In early 2023, one of R's employees received an email which appeared to be from one of R's directors. The email asked what the cut-off time for making a same-day payment was and, after the employee replied, the director then asked for a payment to be made from R's company account. As the employee thought the email was from one of R's genuine directors, they made the payment of £5,000 to the account details the director gave.

Unfortunately, we now know the emails weren't coming from the genuine director, but were coming from a scammer. The scam was uncovered when the employee spoke to the genuine director a few days later, and R then reported the payment to Metro and asked it to refund the money it had lost.

Metro investigated but said it felt it had shown R an effective warning before it made the payment and that R hadn't taken reasonable steps to check the payment was genuine. So it didn't agree to refund the money R had lost. R wasn't satisfied with Metro's response, so referred a complaint to our service.

One of our investigators looked at the complaint. They thought R had a reasonable basis for belief when making the payment, and didn't agree the warning Metro had shown was effective. So they thought Metro should refund the money R had lost, in full. Metro didn't agree with our investigator, so the complaint has been passed to me.

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 broad terms, the starting position in 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, where the customer 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 customer even though they authorised the payment.

Metro is a signatory of the Lending Standards Boards Contingent Reimbursement Model (the CRM code). This code requires firms to reimburse customers who have been the victim of authorised push payment scams, like the one R fell victim to, in all but a limited number of circumstances. And it is for the firm to establish that one of those exceptions to reimbursement applies.

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

- The customer ignored an effective warning in relation to the payment being made
- 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 goods or services; and/or
 - o the person or business with whom they transacted was legitimate

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

Did R ignore an effective warning in relation to the payment?

The CRM code says that an effective warning should enable a customer to understand what actions they need to take to address a risk and the consequences of not doing so. And it says that, as a minimum, an effective warning should be understandable, clear, impactful, timely and specific.

Metro has sent us a copy of the warning it says R was shown before it made the payment, which said:

"Payment for a service

If you're paying for a service, even from someone you've used before, double check the payment information has come from them and not a fraudster.

Ways to do this:

- *Contact them in a different way than they contacted you. For example, if they email you, give them a call back instead of replying online.*
- *We also recommend keeping an eye on their phone numbers and email addresses to make sure they're always the same.*

Don't make this payment unless you know your money is going to the right place."

But while this warning does mention checking the payment information has come from the person you're trying to pay, I don't think it's detailed enough about what this kind of scam might look or feel like. I don't think it does enough to help a customer understand the warning signs that could suggest they were the victim of a scam, or to highlight the seriousness of the possible consequences of sending money to a scammer.

I also don't think the appearance of the warning is striking enough to catch a customer's attention, as the colours and layout used look like part of the normal payment process and the ticks used for the bullet points suggest something positive – rather than the potential negative consequences of falling victim to a scam.

So I don't think the warning R was shown was specific or impactful enough to be effective in its circumstances. And so I don't think Metro has established that R ignored an effective warning in relation to the payment.

Did R have a reasonable basis for belief when making the payment?

R has said the employee who received the emails from the scammer often makes payments on its behalf, and so it wasn't unusual for them to be asked to make a payment like this. And the employee had spoken with the company directors about a payment that would need to be made soon, so I don't think it was unreasonable that they then assumed these emails were in relation to that payment and the payment wouldn't have seemed unexpected.

The name the emails appeared to have come from was the same as the name of one R's genuine directors, so I don't think it was unreasonable that the employee thought it was from them. And the style and tone of the emails matched that of previous genuine emails R has sent us. So I don't think there was anything in the language of the emails that should have suggested to the employee that they weren't genuine.

R has said the employee is often asked to make payments before the formal invoice has been sent, and the invoice is then sent later. So being asked to make a payment in this way was not unusual either.

And, as I explained above, I don't think the warning R was shown was impactful in its appearance. And the employee had been given the impression by the emails that the payment was urgent. So I don't think it was unreasonable for R to move past the warning it was shown and continue making the payment.

I appreciate that, with the benefit of hindsight, it's possible to identify a number of things about what was happening that could have caused R some concern. But, based on what I've seen, I don't think it's unreasonable that, in the moment, R either didn't pick up on these things or wasn't caused enough concern by them to overcome the parts of the scam that felt genuine.

So I don't think Metro has established that R made the payment without a reasonable basis for belief that it was genuine.

I therefore don't think Metro has established that any of the exclusions to reimbursement under the CRM code apply here. And so, under the CRM code, I think Metro should refund the money R lost as a result of this scam.

My final decision

I uphold this complaint and require Metro Bank PLC to:

- Refund R the £5,000 it lost as a result of this scam
- Pay 8% simple interest on this refund, from the date it initially responded to R's claim until the date of settlement

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

reject my decision before 12 January 2024.

Alan Millward
Ombudsman