DRN-4068832

The complaint

Mrs E complains that Metro Bank PLC hasn't refunded her after she fell victim to a scam.

What happened

Mrs E received a WhatsApp message from a number she didn't have saved on her phone. It said, 'Hey mum, I've just broken my phone and this is my temporary number'. Although it was a new number, Mrs E immediately assumed it was her son and replied, 'Oh dear xx'.

What Mrs E didn't realise is that she'd been contacted by a scammer, posing as her son.

The scammer told Mrs E he'd gotten himself 'in a situation' and that he needed her help. He went on to explain that he'd been locked out of his online banking as a result of trying to register it on a new device. He then said that he urgently needed to make a payment.

The scammer also told Mrs E that the microphone and camera weren't working on the broken phone.

Mrs E has explained that her son was in Thailand at the time and so she was concerned about him being in trouble. She said her panic and natural inclination to help her son led her to act. She offered to make the payment for him.

The scammer gave Mrs E account details and asked her to make a payment of £1,400. He said it was for a MacBook that he'd bought and received, having promised to make payment on delivery.

Mrs E tried to make the payment but thought it was going to a Thai account and so was trying to obtain a SWIFT number from the scammer. This meant she couldn't put the payment through to begin with. But the scammer informed Mrs E it was a UK account, and she could send the transfer normally.

Mrs E logged into her online banking and created a new payee using the details provided. She tried to send the money twice, but it was returned both times. The scammer told Mrs E he'd given her the wrong details and gave a different payee name, account number, and sort code. Mrs E set up another new payee and this time successfully transferred the £1,400.

When Mrs E told the scammer the payment had gone through, he asked her to send another £1,140. Mrs E said, 'I hope these are all bargains', to which the scammer replied, 'Yes of course. You know me 😊'. Mrs E went on to send the money.

The scammer made a further request for a payment of £980 which Mrs E sent, before then saying that the amount ought to have been £1,980, so could she send the additional £1,000. She went on to do so. Two further requests followed, one for £1,099 and one for £1,160.

Mrs E sent both of those final payments. Though before the last one she questioned how she could be sure she was talking to her son. So she asked the scammer to confirm the sister's name. The scammer didn't do so, instead sating 'I'm not doing this. If you don't want to pay leave it.' Although Mrs E didn't get an answer to her question, she still sent the money.

Over the course of these payments the scammer had reassured Mrs E he'd pay her back the next day, once he had a working phone and online banking access.

There was one more request for payment. Mrs E again challenged the scammer with questions which weren't answered. It was then that Mrs E realised she'd fallen victim to a scam.

Mrs E reported what had happened to Metro. It considered her scam claim under the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. But it declined to refund her, saying that exceptions to reimbursement set out within the Code applied. It felt Mrs E had ignored effective warnings and hadn't held a reasonable basis for believing she was speaking with her son. Given that answer, Mrs E referred her complaint to this service.

One of our investigators upheld the complaint and said Mrs E ought to be refunded most of the money. He said Metro's warnings didn't meet the standards for firms set out in the Code and so couldn't be used to invoke the applicable exception to reimbursement. And he felt Mrs E did hold a reasonable basis for belief at the time for all but the final payment made. He said by that time Mrs E had clearly grown suspicious and did challenge the scammer. But she proceeded to make a payment despite not receiving an answer to her question. He said it was then fair that liability for the payment ought to be shared as Mrs E's basis of belief ought to have fallen away at that point.

Mrs E accepted the outcome, but Metro did not. As an agreement hasn't been reached the case 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.

I'm upholding Mrs E's complaint for broadly the same reasons as our investigator. Metro is a signatory to the CRM Code which, broadly speaking, is in place to ensure victims of scams are refunded. There are exceptions to reimbursement that a business may choose to apply. The relevant exceptions here can be expressed in the form of two questions:

- Did Mrs E ignore effective warnings presented to her at the time she made the payments?
- Did Mrs E hold a reasonable basis for believing she was dealing with a legitimate party for legitimate purposes?

I'll address each question in turn.

Did Mrs E ignore effective warnings presented to her at the time she made the payments?

To answer this question, the warning presented to Mrs E must first be considered to see whether the exception to reimbursement can be applied, or if Metro ought to bear at least some responsibility for the loss. Was the warning effective and did Metro meet the required standards for firms? I'm satisfied the answer to those questions is no. Which means liability on the bank's part is established.

I've considered the written warning given to Mrs E. I don't consider it to be impactful or specific enough to the scam she fell victim to. That's not to say that Metro could possibly cover every detail and iteration of a scam in a written warning. But here it has failed to bring to life some basic elements of a very common scam. And I'm not persuaded the suggested action for how a customer might protect themselves is particularly clear or helpful in terms of avoiding a scam.

In addition to that, I don't believe Metro did enough in only delivering a written warning. I believe it ought to have stepped in to question the second successful transfer. By this time Mrs E had been in touch with the bank about making an international payment she evidently knew little detail about. She'd then set up a new payee and attempted to send £1,400 to the account twice, with both payments being returned immediately. A further new payee is set

up and a payment of the exact same value is made, before being very quickly followed by a second payment of £1,140. This all happens within two hours. The two successful payments are made within 35 minutes of each other.

I consider this activity to be unusual and it ought to have been identified as a risk by Metro at the time. It ought to have realised Mrs E was at risk of financial harm through fraud. That position is strengthened when considering the historic activity on her account.

Mrs E had made very few faster payments out of her account in the preceding twelve months, and even less to new payees. The value of those payments was almost always low, with the closest comparable payment being for £500. The increase in value of payments, the quick addition of new payees, and the rapid sending of funds to one of those payees ought to have combined to form a picture of suspicious activity that is frequently connected to a scam.

Metro has stated that there was similar activity two years prior to the scam. I'm not sure exactly what activity it's referring to, but I don't consider anything that took place such a long time before the scam can be said to paint a picture of regular or normal account activity.

All of this means that Metro ought to have stopped the second payment and questioned Mrs E about it. I'd have expected the bank to have a discussion with Mrs E about the payment and to deliver an effective warning verbally. I'm persuaded such a warning, linked with a discussion about the purpose of the payments and possible scams, would have revealed the deception and prevented any further loss.

Did Mrs E hold a reasonable basis for believing she was dealing with a legitimate party for legitimate purposes?

When dealing with scams of this nature, and other types of scams too, it's important to remember that customers aren't going about their lives expecting to be scammed. People don't have their guard constantly up. It's easy to lose sight of that when in a position of dealing with scams every day and a heightened sense of awareness is present. Furthermore, it's important not to be obfuscated by hindsight. The expectation can't be that all details of any interaction ought to be questioned by a customer. That isn't a realistic view of how individuals go about their lives and the expectation is set too high.

Unless there is something within an interaction that clearly seems out of place or unusual, people will often not detect that something might be wrong. Scams like this succeed because fraudsters are adept at exploiting human nature and behaviours.

Mrs E was contacted on a new number by who she believed was her son. That his phone might have become damaged seemed entirely plausible, particularly as she knew he was travelling in Thailand.

What followed, whilst not detailed, appeared to be a normal conversation about needing to borrow some money urgently. This kind of scam is designed to prey on a parent's instinct to help their child and, here, prevent negative financial impacts. And so, it's fair to say, the rationale or circumstances may not be questioned as much as they otherwise might be. The fraudster is playing on an emotional response, that the parent themselves is unlikely to be particularly aware of at the time.

Where there isn't anything within the messages that appears off or unusual, I find it's fair to say that Mrs E held a reasonable basis of belief that she was dealing with, and helping, her son from the outset.

Mrs E has said she hasn't necessarily lent her son money before, but she was confident he could pay the money back. Given the nature of the request and the explanation for needing to make the first payment I don't think there was anything to put Mrs E on notice that she was dealing with a scammer.

The scammer clearly and confidently explained the money was for a MacBook that had already been received and needed to be paid for. And he also confirmed that it was bought from a personal seller, rather than from a business.

What Metro has argued is true. Mrs E might have tried contacting her son by other means. Or she might have tried another person that could verify what she was being told. And doing so might well have avoided the scam altogether. But that isn't the test here. It's whether Mrs E's basis for belief was reasonable, and I'm satisfied it was.

I think it's fair to say that each new request for payment does make the circumstances more unusual and suspicious, even though there was nothing particularly alarming in what was being said. That's reflected in how events unfold, where Mrs E does question the scammer before making the final payment, asking for the name of the sister. Mrs E clearly had doubts at this point. And so, I don't think it was reasonable for her to proceed with a further payment, having not had an answer to her question. That means her responsibility for her losses comes in for the final payment and liability for it ought to be shared.

Putting things right

Metro should now:

- Refund 100% of payments one through five (£5,619);
- Refund 50% of payment six (£580);
- Pay simple interest on the refund of payment one at 8% simple per year, from the date Metro rejected the claim under the Code to the date of settlement; *and*
- Pay simple interest on the refund of payments two through six at 8% simple per year, from the date of loss to the date of settlement (on the basis proper intervention from Metro would have avoided the losses).

My final decision

I uphold this complaint against Metro Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs E to accept or reject my decision before 2 November 2023.

Ben Murray
Ombudsman