DRN-3840734

The complaint

Mr C complains that Metro Bank PLC ('Metro') won't refund the money he lost in a scam.

What happened

Mr C is represented in this case but for ease I'll refer to Mr C throughout this decision.

Mr C says that he received a call from someone who claimed to be from Metro's security team, but he now knows was a scammer. The caller went through a security process and knew Mr C's mother's maiden name which reassured him. The scammer asked Mr C to provide two characters from his password and stressed that he shouldn't reveal the other characters. Once security was complete the scammer referred to an unusual transaction for £2,300 and asked Mr C if he recognised it. As he didn't, the scammer confirmed the payment would be stopped. But as Mr C's account information had been breached, he needed to transfer funds into an account not in his name to keep his funds safe. Mr C says he questioned this and was advised there was a breach of security on an account in his name and the other account belonged to an employee of Metro.

On 9 November 2021 Mr C made three transfers to the account details he was provided with. These transfers were for £998, £1,598.11 and £1,688.95. Mr C was told the amounts had been randomly generated for security reasons. It was only after he'd made the third payment that Mr C realised his funds had been paid into an account with a different bank. His call with the scammer dropped and it was only when he called the genuine Metro number back that he was told he'd been scammed.

Metro considered Mr C's complaint under the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code), which it has signed up to. The CRM Code requires firms to reimburse customers who have been the victims of APP scams like this one in all but a limited number of circumstances. Metro says Mr C made the payments without having a reasonable basis for believing the payee was the person he was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom he transacted was legitimate.

Metro was able to recover £225.48 from the receiving bank which it returned to Mr C. Mr C was unhappy with Metro's response and brought a complaint to this service. He has asked for the remaining funds lost in the scam to be reimbursed and for £500 compensation as he feels the service he has been provided with was poor and added to his distress.

Our investigation so far

The investigator who considered this complaint recommended that Metro reimburse Mr C's remaining loss with interest. She said that Metro hadn't shown Mr C didn't have a reasonable basis for believing he was paying a genuine payee and that Metro hadn't provided an effective warning aimed at this type of scam.

Mr C agreed with the investigator's findings. Metro said that it hadn't provided an effective warning under the CRM Code, but that liability should be shared. This was because Metro felt Mr C missed some warning signs such as the fact that he wasn't asked to transfer funds to an account at Metro and not all of his money was moved at once leaving funds at risk.

The complaint has been passed to me to issue 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.

The starting point for my considerations is that, under the Payment Services Regulations 2017 and the terms of his account, Mr C is liable for transactions he's carried out himself. But Metro are signatories to the CRM Code and also have a longstanding obligation to be on the lookout for unusual and out of character transactions which might indicate their customer is at risk of financial harm from fraud.

There's no dispute here that Mr C was tricked into making the payments. As I said above, the CRM Code requires firms to reimburse victims of APP scams like this one unless it can establish that it can rely on one of the listed exceptions set out in it. 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 other exceptions that are not relevant to this case.

The CRM code says that, where firms identify APP scam risks, they should provide effective warnings to their customers. Metro said in its response to the investigator's view that it didn't provide effective warnings when the payments were made so agreed to refund 50% of Mr C's remaining loss. I'm not persuaded that Metro ought to have recognised a scam risk in this case, so if I don't consider Metro has demonstrated it can reasonably rely on the reasonable basis for belief exception, Mr C should receive a full refund.

Did Mr C have a reasonable basis for belief when he made the payments?

Metro has pointed to a number of warning signs it says Mr C disregarded. I have taken account of all the circumstances it highlights. But, on balance, I am not persuaded these outweigh the other factors that Mr C says led him to believe in the legitimacy of the caller.

Mr C says that the caller knew specific personal information, including his mother's maiden name. He says he thought this information could not be known by anyone besides himself and Metro - helping persuade him it was indeed his bank calling. I consider that reasonable in the circumstances here.

Mr C has also explained that the scammer asked him to disclose only two characters of his password and was very specific that he should not reveal the full password. The scammer followed a process Mr C expected which helped to reassure him he was speaking to Metro.

The scammer told Mr C that his funds needed to be moved to an account not in his name. Mr C questioned this and was provided with an explanation which seemed reasonable to him at the time – that there was a security breach associated with Mr C's name. Mr C was also advised that he was transferring funds to the account of a Metro employee. Whilst those with knowledge of this type of scam understand that what Mr C was told wasn't correct, it's clear Mr C believed what he was told, and I consider his belief was reasonable. It wasn't until the call with the scammer dropped and Mr C called his real bank that the scam was uncovered.

With the benefit of hindsight, I accept Mr C ought to have recognised that his funds weren't being sent to another Metro account. But I must take account of all the circumstances at the time the payments were made. Mr C has explained that he was distracted at the time of the call as he'd received a delivery he needed to deal with. He was also very concerned about the disputed transaction the scammer referred to and the safety of his funds. So I can understand why Mr C overlooked this point until after he'd made the payments and was advised he'd fallen victim to a cruel scam (particularly as he was already persuaded he was talking to his bank).

One of Metro's reasons for not refunding Mr C was the fact that he made three transfers rather than moving the entire balance of his account at once. This meant that the remaining funds were at risk for the intervening periods. Mr C has said that the scammer explained he would provide Mr C with randomly generated amounts to enter, for security reasons. Given that Mr C believed the call was from Metro, he accepted this explanation. And looking at the timing of the transfers I see that they were all made in around four minutes. So I don't consider it reasonable to conclude that Mr C should have had significant concerns about the safety of his remaining funds between transactions.

Mr C also wasn't provided with an effective warning that ought reasonably to have led him to question what he was being told by the scammer.

Overall, I'm not persuaded that Metro has done enough to establish that Mr C made the payments without a reasonable basis for believing that he was transacting with a legitimate employee of the bank.

Finally, I've considered the service Mr C received. He has said that he called Metro within minutes of the last transaction and so feels Metro should have been able to do more to recover his funds. I've seen evidence that shows that Metro contacted the bank that received Mr C's funds within an hour of Mr C's call to report the scam, so I'm satisfied that Metro followed the standard expected in respect of the recovery of funds. So I'm not asking Metro to pay anything more.

My final decision

I require Metro Bank PLC to:

- Refund Mr C's remaining loss (after taking into account the amount recovered and returned to Mr C);
- Pay interest on the above amount at the rate of 8% simple per year from the date Mr C should have been refunded under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 16 February 2023.

Jay Hadfield
Ombudsman