DRN-5258743

The complaint

Mr M complains that Metro Bank PLC hasn't reimbursed a payment that was made from his account to a safe account scam.

What happened

Mr M received a call from someone he thought was part of Metro's fraud team. They told him there was suspicious activity on his account and he needed to move his money to a new account to keep it safe. Mr M has explained that while he begun the payment now in dispute, he didn't complete it as he saw the payment details and had concerns. He says he went into branch to report the call and discovered a £3,950 payment had been made.

Mr M asked Metro to reimburse him, but it didn't agree to this. It said that Mr M received a code to his mobile to complete the payment and that only his device had accessed his account. As he said he hadn't allowed anyone else access to the device, either in person or by remote access, it concluded it must've been him that made the payment and so it was authorised and he wasn't due a refund.

Mr M came to our Service and asked us to investigate his case. Our Investigator also determined it was Mr M who made the payment, but they said he was due 50% back under a reimbursement code Metro was signed up to. Mr M accepted the assessment, but Metro disagreed. It said Mr M couldn't be covered by this code if he hadn't made the payment. Our Investigator reiterated that they were agreeing with Metro that it was Mr M who made the payment, so then the code could apply, but Metro asked for a 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.

When considering what is fair and reasonable, I'm required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

In broad terms, the starting position in law is that a payment service provider is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (PSRs) 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 provider to reimburse the customer even though they authorised the payment. I accept there is debate in this case around whether the payment is authorised and I will address this in my decision.

I consider the Contingent Reimbursement Model (CRM) code (or 'the Code') is of particular relevance to this case. It's a voluntary code which requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams in all but a limited number of circumstances. Metro was a signatory to the Code at the time the payment in dispute was made.

Has Mr M been the victim of a scam, as defined by the CRM Code?

In order for me to conclude whether the CRM Code applies in this case, I must first consider whether the payment in question meets the Code's definition of a scam. An "APP scam" is defined by DS1(2)(a) as:

> *"Authorised Push Payment scam, that is, a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer, authorised by a Customer in accordance with regulation 67 of the PSRs, where:*
>
> > *(i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*
> > *(ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent."*

If I conclude that the payment here meets the required definition of a scam then Mr M would be entitled to reimbursement, unless Metro has shown that any of the exceptions as set out in R2(1) of the Code apply.

I don't consider the first part of the definition quoted above is met in this case. This doesn't seem to be in dispute. But what is in dispute is whether Mr M's payment meets DS1(2)(a)(ii). As Mr M was adamant he didn't make the payment, I accept why Metro then initially concluded his situation didn't meet the definition above and went on to consider his claim that the payment was unauthorised. Mr M would need to have made the transfer for it to be covered by the Code – as per the reference to regulation 67.

However, following its investigation, Metro did then reject Mr M's claim that the payment was unauthorised and concluded that either he made the payment or that it was made by someone else with his consent – as supported by its technical evidence. So at this time, its own finding that the payment was authorised (in accordance with regulation 67) would mean it *could* fall under the scope of the Code – and it had already had more time than the rules set out to investigate and decide Mr M's case. I also note it contacted the receiving bank and recovered £10 of Mr M's money which it let him keep – so this also indicates it recognised he was a scam victim.

Metro has however maintained to us that this isn't an APP scam based on Mr M's testimony. But I think it's important to look at the full situation Mr M has described as well as the technical evidence Metro holds. Considering the situation here and what Metro knew in this particular case, I'm satisfied it ought to have considered this payment under the Code. I'll explain why.

Setting aside what he's said about who confirmed the payment, Mr M's testimony has been consistent. He received a call from someone he believed was from Metro and was persuaded his account was at risk. Mr M has also accepted he started the payment process in app and took it through to the 'confirm payment' screen. We also know that only his device had access to his account and was the one that received the code which was input for the payment. There's no evidence that a payment was declined or of any other payment attempts. So the evidence Metro holds shows Mr M was involved in the processing of the successful payment. This alongside the fact its complaint outcome was that this payment was authorised means it must be concluding Mr M – *"The Customer"* here – made the transfer. There are also a number of reasons a customer may not be forthcoming about all the steps taken. While I accept this is unhelpful and does hinder any investigation, in the individual circumstances of this case, I'm satisfied Metro had enough to be confident that despite his testimony, Mr M did complete the payment process.

As Metro concluded it was Mr M making the transfer – this then left the second part of DS1(2)(a)(ii) to be met. And as set out, since Mr M first reported the disputed payment, he has consistently explained he was the victim of a safe account scam and that the payment process was initiated to protect his funds – and we know the payment he started is the same payment that left his account.

I'm satisfied Mr M believed this hiss purpose was legitimate at the time the payment was made – but that the person who rang him was actually a scammer. So I consider this payment does meet the definition above and can be considered an APP scam payment under the Code. And our Investigator also reached this conclusion, determining it was Mr M who made the payment as the result of a scam, for the same reasons as Metro said it was authorised. Mr M accepted the view in December 2024.

Is Mr M entitled to a refund under the CRM code?

Under the Code, the starting principle is that a firm should reimburse a customer who is the victim of an APP scam. It sets out standards that firms must meet to protect customers from APP scams. And the circumstances where a firm may choose not to reimburse, which are limited and it is for the firm to establish those exceptions apply. R2(1) of the Code outlines those exceptions.

One such circumstance might be when a customer has ignored an Effective Warning. A second circumstance in which a bank might decline to reimburse, is if it can be demonstrated that the customer made the payments without having a reasonable basis for belief in a specific set of things.

Metro has argued that it provided an Effective Warning in this case, so met its standards, but it says Mr M then ignored this. However, it has been unable to confirm which option Mr M selected when making his payment, so it doesn't know which of its warnings were displayed, but says one was. Due to this it has provided us with a copy of all the warnings it could've showed him at the time of the payment.

I'm in agreement with our Investigator that as Metro can't evidence it showed a warning *and* which warning it showed, it's then difficult to understand how it can be sure it gave Mr M an 'Effective Warning'. The CRM Code sets out the warning should be tailored where possible to the scam type identified and has a minimum criteria that a warning must meet to be an 'Effective Warning' which includes the warning being Clear, Impactful and Specific.

Reading the warnings provided, I'm not persuaded that any would meet this criteria given their content. But as set out, considering we don't know what Mr M selected or was shown, I'm not satisfied Metro can fairly rely on the exception that he was presented with, but then ignored, an Effective Warning. And as it identified a scam risk and hasn't been able to evidence it provided an Effective Warning, it has then failed to meet the standards expected of it to protect its customers under the Code.

I've then gone on to consider whether Mr M made the payment without a reasonable basis for belief – and I'm satisfied this exception does apply.

Mr M has explained that he thought his account was at risk because the caller told him about suspicious payments that had been attempted. But Mr M has told us he was using his banking app at the time he got the call – so he could have reasonably seen there were no payments being attempted on his account.

Metro has also evidenced to us that the screens Mr M was presented with for the payment were clear on where it was going – and this was to an account with another bank. Mr M

understood the money was being moved to a safe account in his name – and he's not indicated he questioned why Metro would need to use a different bank to protect his funds. The involvement of another bank should have been concerning to him and indicated that he wasn't about to pay the person he expected, in the way expected. But the evidence we hold indicates he went ahead and authorised the payment anyway.

Considering this, I think an exception to reimbursement does apply here and Mr M did make the payment without a reasonable basis for belief, as set out under the Code.

As I've identified failings by both Metro and Mr M under the Code, this means Mr M is due back 50% of the payment he sent. Mr M is also due 8% simple interest on this reimbursement and our Investigator said this should be paid from the date the claim was declined, but they didn't set out exactly when this was.

Mr M reported the scam in June 2023, at the time it happened. So Metro ought to have begun investigating straight away. I accept that Mr M's testimony that he didn't make the payment did then change how his case was investigated and cause a delay. But by 10 August 2023, when Metro responded to his fraud claim finding him liable and declining it, enough time had passed that it could've investigated both the unauthorised claim as well as considered the transaction under the Code. So this is the date that was intended and should be used.

Putting things right

Metro Bank PLC should:

- Refund Mr M 50% of the outstanding loss (which I understand would be £1,970)
- Apply 8% simple interest per year to this refund from the claim decline letter on 10 August 2023 to the date of settlement

My final decision

For the reasons given, my final decision is that I uphold this complaint. Metro Bank PLC needs to put things right for Mr M as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 24 October 2025.

Amy Osborne
Ombudsman