

The complaint

Mr B complains that Metro Bank Ltd hasn't refunded all the money he lost when he fell victim to a friendship scam in 2021. Mr B has a representative who has made submissions on his behalf, but for clarity in what follows I will refer only to Mr B.

What happened

In mid-2021 Mr B says he was contacted through social media by someone who claimed to work on a ship – I'll refer to this person as S. Mr B chatted to S for a while and then S said they wouldn't be able to be in contact as they were embarking on a voyage.

Mr B says he was then contacted in September 2021 by S, saying her ship had been attacked by pirates. S said she had a strongbox onboard containing a large amount of cash. She said she wanted to have this shipped to Mr B to avoid it being stolen by the pirates.

Mr B provided his address, but S explained she didn't have enough money to pay for the shipment. She asked him if he could pay for this.

When Mr B asked S why she couldn't use the money in the strongbox, S explained she didn't want to open the box in front of the shipping company. Mr B was told he'd be contacted by the shipping company to arrange payment. He was told not to divulge the contents of the box to avoid the risk of its theft.

Mr B made a payment of £1,300 from his Metro Bank account by Faster Payments transfer on 6 October 2021. He believed this was to pay for the shipment of the strongbox. He sent this payment to a personal account (as opposed to an account held by a company).

S then told Mr B the shipping company had scanned the box and identified that it contained money. It now needed a "diplomatic immunity tag" which would cost a further £23,580. Mr B visited his Metro branch, and from there he sent an initial payment of £12,000, again to the same personal account.

Metro noted that the payment was unusual for Mr B and questioned him about it. Mr B gave the story that this was for a shipment of clothing. Metro accepted this story, and the payment was sent.

A few days later Mr B returned to the branch and paid the balance of £11,580. This time the payment was sent by international transfer to an account in the Philippines. Mr B was again spoken to by Metro. On this occasion he told Metro the payment was going to his partner in the Philippines. Metro accepted this story and allowed the payment to go through.

However, S began to ask Mr B for more money, and after she failed to verify what she was saying, Mr B realised this had been a scam. He reported the matter to Metro. Metro was unable to recover the funds Mr B had sent.

Metro is a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code) which can provide additional protection to scam victims against the impact

of Authorised Push Payment scams (APP scams). The CRM Code doesn't apply to international payments such as the third payment made here. But it would apply to the first and second payment Mr B had sent.

Metro considered the first two payments under the CRM Code. Metro didn't think Mr B had held a reasonable basis for believing the payments were for a legitimate purpose or that he was paying who he expected to pay. So it didn't think Mr B was due a full refund of these payments under the CRM Code. It said it would reimburse 50% of the first payment, because it could have done more to protect Mr B. But Metro said it had provided Mr B with an effective scam warning for payment two, and so wouldn't be refunding any of that sum.

The CRM Code didn't apply to payment three. Metro didn't accept it was at fault for that final payment and didn't think it could reasonably have prevented the loss. It did not reimburse Mr B for that payment.

In total, Metro refunded £650 (half of payment one). This left Mr B with a loss of £24,230.

Mr B asked our service to look into the matter. Our Investigator agreed with Metro that Mr B hadn't had a reasonable basis for believing the payments were legitimate. That meant she didn't think payments one and two needed to be refunded in full under the CRM Code. But she didn't think Metro had evidenced that the warning it gave was "effective" for payment two. So the bank needed to reimburse 50% of that payment.

For payment three, the Investigator thought Metro could have prevented the payment, but again thought it was fair that Mr B should equally share the responsibility for the resulting loss. She said Metro should also refund him half that payment.

Mr B accepted the Investigator's proposed settlement. However, Metro didn't agree so I have been asked to make a final decision on the matter.

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 have reached the same outcome as that of our Investigator and for broadly similar reasons.

Firstly, Metro has a primary obligation to carry out the payment instructions its customers give it. As a starting point, a customer will therefore be assumed liable for a payment they have instructed to be made. There is no dispute that Mr B authorised these payments, albeit having been deceived into believing he was paying for various shipping costs which later turned out to be false. So, on the face of it he is liable for the resultant losses.

As I've mentioned above, the CRM Code can provide additional protection for the victims of APP scams such as this was. I'm satisfied that the first two payments made here fall within the scope of the CRM Code.

However, the last payment was an international payment which means it is not within the scope of the CRM Code, and so I cannot fairly apply the terms of the Code to that payment.

Payments covered by the CRM Code

While the CRM Code offers additional protection to the victims of an APP scam, it includes provisions allowing a firm not to fully refund APP scam losses in some situations.

Relevant here, this includes an exception to full reimbursement where the customer made a payment without a reasonable basis for believing that they were paying for genuine goods or services, dealing with a legitimate person or business, or paying the person they believed they were paying.

Metro says this exception applies here. It says Mr B made these payments without holding a reasonable basis for believing he was dealing with a legitimate person or making a payment to a shipping company for genuine services.

I have considered whether Mr B made these payments without having a reasonable basis for believing what he did.

I appreciate that the scam unfolded over a period of time. During that time the scammer was able to build trust with Mr B. And the story had features that undoubtedly made it seem believable to Mr B at the time.

But I also think the underlying story was at its heart highly implausible. I think Mr B should reasonably have doubted what he was being told. Had Mr B searched the name of the shipping company online, he'd have found reports indicating it was a scam, and none indicating it was legitimate. I also find that the evidence he was later given (an X-ray purportedly showing money in a crate) wasn't evidence to show that the person he was dealing with had the money they claimed to. And I think he should have had significant doubts about the instruction to send these large payments to personal accounts rather than accounts in the name of a shipping business.

Overall, while I've carefully considered everything Mr B has said about why he thought what he did and why he believed the story at the time, on balance it is my finding that Mr B made these payments without having a reasonable basis for believing what he did. So I find Metro is entitled to rely on that exception to full reimbursement under the terms of the CRM Code, in relation to both payment one and payment two.

The CRM Code sets out standards that firms are required to meet. Where these are not met, the firm may still be liable to reimburse a victim in part, even where it has been able to establish that an exception to full reimbursement may be fairly applied (as I am satisfied Metro has established here).

Relevant here, those requirements include the provision of what the Code defines as an Effective Warning when a firm identifies an APP scam risk in relation to a payment.

For payment one, Metro has already accepted it must share liability under the code. It has already refunded Mr B 50% in respect of that payment. I consider that is the fair outcome under the terms of the CRM Code, so I have not considered that payment further.

In relation to payment two, Metro says it gave Mr B an Effective Warning, in line with the provisions of the CRM Code. I have considered the evidence provided by Metro to determine whether I am persuaded it has established that it met its standards under the terms of the CRM Code in this respect.

Metro has provided a copy of the text of the warning message it says Mr B received. As Mr B was making the payment in branch, it appears the message would have been delivered verbally, but the staff member was required to say: *"Have you spoken to the person you are sending these funds to verify its them and their account. Always confirm new bank details by speaking to the person. You could lose your money if this payment results in a scam."*

Metro's system records that this message was read to Mr B at the time of payment two.

I appreciate that, in reading Mr B this message, Metro took steps to provide him with a scam warning during the payment journey. However, despite this, I'm not persuaded Metro has demonstrated that it met the minimum requirements to provide an Effective Warning under the CRM Code.

The CRM Code sets out minimum criteria that a warning must meet to be an 'Effective Warning'. That includes the requirements to be both specific to the scam risk identified and to be impactful – to positively affect customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. The code goes on to say this should include steps to ensure that the customer can reasonably understand the consequences of continuing with an irrevocable payment.

The warning does set out that the customer might lose their money if the payment resulted in a scam. So, it did set out the consequences and in an understandable way.

The scam warning information appears tailored to the risk of an invoice interception scam – where a genuine invoice had been intercepted and the payment details altered to misdirect the customer's payment.

In this instance though, I'm satisfied that Metro should reasonably have identified that the scam risk might be something else. Metro's notes record that Mr B was paying *"a shipping company to buy goods which are clothes"*. But I find this implausible. This answer should have concerned Metro that Mr B might be falling victim to a different type of scam than an invoice interception scam.

Firstly, it is unclear why someone would be paying a personal account, when the payment was meant to be going to an international shipping company. And it seems very unusual to be paying £12,000 for clothing to be shipped, or even to be paying £12,000 for clothing items. As Metro noted at the time the payment was not in line with what was usual for Mr B – I agree. I think this payment and this explanation of it were both significantly out of character considering Mr B's prior history with Metro.

I think Metro should have had serious concerns that what Mr B was telling it wasn't likely to be true – in other words it was a cover story. I find the story was particularly implausible given what Metro knew about Mr B's normal usage of the account. Relevant here, it's long been recognised by, for example the Banking Protocol, that sometimes scam victims will have been given a cover story to use. As a matter of good industry practice, I'd expect branch staff to have been alert to the risk of this.

In summary, while Metro identified a scam risk from its interaction with Mr B, I'm not persuaded it identified an appropriate scam risk based on what it could reasonably have identified in the circumstances (even though Mr B was using a false story). I'm not satisfied that the provision of the warning it gave was sufficient to show Metro complied with the requirements of the CRM Code in relation to this payment.

As I have found Metro failed to meet its requirements under the CRM code in relation to payment two, Metro should share liability for the resultant loss with Mr B and should have reimbursed him 50% of that payment.

Payment three - not covered by the CRM Code

As I've noted above, payment three was an international payment – and consequently the CRM Code does not apply.

Nevertheless, as a matter of good industry practice at the time, I'd expect Metro to have

been on the lookout for unusual or out of character transactions - intervening in the event it had concerns a payment might result in financial harm through fraud or scam.

Metro's notes from this transaction say that the payment again was not in line with what was usual for Mr B's account. I consider Metro was correct in identifying this was an out of character and unusual payment for Mr B. He was making a payment of over £10,000 to an international payee whom he'd never paid before. Indeed, it doesn't appear, based on the account history provided by Metro, that Mr B had made any international payments previously.

Metro says it again read Mr B a warning message. This time, as Mr B had said the payment was going to his partner, the warning message was slightly different saying "[...] *always speak to the person and verify the bank details you have been given*" and *"If you haven't spoken to them it could be that it isn't them requesting the payment"*.

I don't think this went far enough. By this point, Mr B was attempting to make a second large and out of character payment within the space of a few days. Again, the story here wasn't particularly persuasive or detailed. I don't think Metro should reasonably have been reassured by what Mr B was telling it that he wasn't about to fall victim to a fraud or scam as a result of the payment.

As a matter of good industry practice, Metro should have followed the Banking Protocol in these circumstances. Its records do not show that this happened. The Banking Protocol reflects an industry awareness that a feature of some scams will be that the consumer has been given a cover story to use. I do not find that Metro should have considered the payment reason Mr B gave was sufficient to establish that he wasn't about to lose the money to a scam. For example, if this was his supposedly his partner, that doesn't seem consistent with him never having sent money to the Philippines before.

I think Metro should have pressed Mr B further about the purpose of the payment. Had it done so, I'm not persuaded his cover story would have held up to further enquiry. I've seen nothing to persuade me that Mr B's cover story here was anything more than superficial in depth or that he'd prepared a more detailed set of circumstances that might have enabled him to convince the bank that the story wasn't fabricated. I think, given further enquiry in line with the expectations of the Banking Protocol, the scam may well have come to light then and there. But even if it didn't, I am satisfied that the further steps available under the Banking Protocol would have led to the scam being identified (through the involvement of the Police).

In summary, I find that as a matter of good industry practice, Metro should have prevented this payment from being made. That it did not do so has led to the loss.

However, I consider that it would be fair and reasonable in all the circumstances that a reduction for contributory negligence should apply here. I consider that for similar reasons to those I have set out above, Mr B should have identified that what he was being asked to do by the scammer was not legitimate. All considered I find it fair that Metro and Mr B should equally share the loss caused by payment three.

Putting things right

As explained above, I find that Metro should have reimbursed Mr B 50% of payment two in line with the provisions of the CRM Code. I also find that Metro should have prevented payment three and that it should be held liable for 50% of that payment.

Had Mr B been refunded these sums when he should have been, it is not clear how he

would have used the money. In the circumstances, I consider it fair that Metro should add interest at the rate of 8% simple per year to reflect the time that Mr B has been deprived of the use of these funds.

Therefore, within 28 days of receiving notification of Mr B's acceptance of my final decision, Metro should:

- Pay Mr B 50% of payments two and three, equating to amounts of £6,000 and £5,790 respectively. Metro may deduct any sums it has already recovered or reimbursed in respect of these two payments; and,
- Add interest to those amounts at the rate of 8% simple per year. In respect of payment two, this interest should be calculated from the date Metro declined to reimburse Mr B under the CRM Code until the date of settlement. In respect of payment three, the interest should be calculated from the date of the payment until the date of settlement.

My final decision

For the reasons given above, I uphold Mr B's complaint about Metro Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 11 October 2023.

Stephen Dickie
Ombudsman