

## **The complaint**

Ms S complains that Metro Bank PLC (“Metro”) will not refund the money she lost after she fell victim to a romance scam.

## **What happened**

The circumstances that led to this complaint are well known to both parties, so I won’t repeat them in detail again here. However, in summary:

In early 2019, Ms S met someone on a social networking website who I will refer to as “M”. The conversation quickly moved to a messaging platform and after around 6 weeks M started to ask Ms S to lend him money. Ms S initially made payments from her other bank account elsewhere before beginning to make payments from her Metro account.

Between January 2020 and February 2022, Ms S made numerous transfers to M totalling over £70,000.

After realising she had been the victim of a scam, Ms S, alongside her representative, wrote to Metro to ask if it would consider refunding Ms S the amount lost as she had been vulnerable at the time the scam occurred. Metro declined to offer Ms S a refund of the total amount lost but it did acknowledge that it could have done more to protect Ms S at the time and so it offered her a refund of 50% of her overall loss.

Ms S didn’t agree with Metro’s response, and she brought her complaint to this service.

One of our Investigators looked into things and recommended the complaint be upheld. He recommended that Metro refund all of the payments made by Ms S under the Contingent Reimbursement Model (CRM) Code. This is because he felt Ms S was vulnerable when making the payments to the scammer. He also recommended Metro pay 8% simple interest from the date Ms S’s claim was declined up until the refund was paid.

Metro acknowledged that Ms S was clearly dealing with some difficult personal circumstances at the time of the scam, but it didn’t feel that these meant she was unable to protect herself from what happened. So, it reiterated that it believed Ms S’s role in the success of the scam should be reflected in the refund now being put forward.

As the case could not be resolved informally, it 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.

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; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

In broad terms, the starting position 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.

There's no dispute here that Ms S authorised the payments herself. However, where a customer makes a 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. When thinking about what is fair and reasonable in this case, I've considered whether Metro should have reimbursed Ms S in line with the provisions of the Lending Standards Board Contingent Reimbursement Model (the CRM Code) it has signed up to and whether it ought to have done more to protect Ms S from the possibility of financial harm from fraud.

There's no dispute here that Ms S was tricked into making the payments. She thought she was helping someone she believed she was in a loving relationship with, and this wasn't the case. But this isn't enough, in and of itself, for Ms S to receive a full refund of the money under the CRM Code.

### *The CRM Code*

Metro has signed up to the CRM Code. Under the CRM Code the starting principle is that a firm should reimburse a customer who is the victim of an APP scam, like Ms S.

The circumstances where a firm may choose not to reimburse are limited and it is for the firm to establish those exceptions apply. R2(1) of the Code outlines those exceptions. I haven't outlined them here as they are not relevant in this particular case.

### *Vulnerability under the CRM Code*

Section R2(3) of The Code requires firms to assess whether a customer is vulnerable to the APP scam they fell victim to. It says:

*"A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis."*

The CRM Code also says that in these circumstances, the customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the firm had previously identified the customer as vulnerable.

As this provision under the CRM Code might lead to a full refund, notwithstanding the provisions in R2(1), this is the starting point for my decision in this particular case.

Metro has argued that, whilst Ms S may have been dealing with some very difficult personal circumstances, it would be unreasonable to say she was wholly unable to protect herself from the scam she fell victim to. It feels Ms S could have taken steps to verify what she was

being told by the scammer and had she done so, she would've realised she was likely falling victim to a scam.

The Code says vulnerability should be considered on a case-by-case basis. It also outlines some factors for firms such as Metro to consider.

Whilst I consider the factors to be indicators of potential vulnerability and a non-exhaustive list, I am persuaded that it is readily apparent from what Ms S has said of her personal circumstances at the time that she was vulnerable and, in my view, specifically vulnerable to a romance scam. I do not think it would be reasonable for Metro to have expected Ms S to be able to protect herself from this particular scam, especially given its timing and nature. From the information Ms S has provided to both us and the bank, it's clear that she was experiencing a particularly difficult time in her personal life when she fell victim to the scam.

Ms S had been with her husband for over 20 years. Ms S's husband was coercive and controlling and even after they decided to split, he refused to move out of the home she was paying for and was still living in. Ms S started divorce proceedings in 2017 which were ultimately resolved in 2019 and throughout this period, Ms S's husband remained in her home resulting in an uncomfortable home life for Ms S. Ms S's mother also passed away in 2019 and Ms S was alone when the Covid pandemic hit in 2020 when she became furloughed during lockdown. She was dealing with things on her own and she has told us she was lonely, and the 'relationship' soon became her only outlet from her loneliness. Ms S was deceived into a false relationship by the scammer. He gained her trust by communicating with her for an extended period of time. He alluded to wanting the same things. He used Ms S's hope that he would be able to come home from a US mission and build a better life with her to manipulate and extort money from her.

I'm persuaded Ms S was particularly susceptible to detriment at this time. In my view, Ms S was significantly less able to represent her own interests and I think this is something the scammer picked up on. At the time, he was the only outlet for her hopes of a happier future. Ms S has shared some of the messages she exchanged with the scammer with us. It's clear that the scammer exploited Ms S. Her state of mind coupled with her desire to have a loving relationship again - meant she wasn't in a position to protect herself from falling victim to the scam. The impact of this scam both financially and non-financially has been significant for Ms S. She has been left emotionally devastated by the betrayal in her trust.

I don't agree with Metro that Ms S could've readily identified that what she was being told might not be true. And so, for the reasons I have already explained, I do not think it would be reasonable to have expected Ms S to protect herself from becoming the victim of this particular romance scam in her circumstances. As a result, I find Ms S was vulnerable to this particular APP scam and I think Metro should have identified that when it considered her claim under the CRM Code.

Metro mentioned in its response to our Investigators view that it wasn't aware of any vulnerabilities until the scam report was made. But as I've mentioned above - the CRM Code is clear that where the consumer meets the definition of vulnerability under the CRM Code – they should be reimbursed in full whether or not the firm previously identified the customer as vulnerable or not. It is also the case that if a customer meets the definition of vulnerability set out under the CRM Code that exceptions to reimbursement (such as reasonable basis for belief, ignoring effective warnings and gross negligence) do not apply. So, I haven't gone on to consider whether any of the exceptions under the CRM Code would have (otherwise) applied in this case.

Finally, I want to say how deeply sorry I am to hear of the situation Ms S has found herself in. She has been the victim of the cruel and callous actions of what appears to be a professional fraudster. I understand moving on from the scam has been difficult for her. I hope that she is now able to draw a line under what happened and move forward.

### **Putting things right**

In order to put things right for Ms S, Metro Bank PLC should:

- Refund Ms S the total amount lost to the scam, taking into account any refunds previously paid
- Compensate Ms S for being deprived of the money she lost by adding simple interest at the rate of 8% per annum to the above, from the date her claim was declined to the date of settlement.

### **My final decision**

My final decision is I uphold this complaint and require Metro Bank PLC to put things right for Ms S as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 20 September 2024.

Emly Hanley Hayes  
**Ombudsman**