DRN-3734002

The complaint

Mrs A is unhappy because Metro Bank PLC ('Metro') declined to refund £485 which she lost as the result of a scam.

What happened

The details of this complaint are well known to both parties, so I will not go into every detail of what happened here. But, in summary, both parties accept that in December 2021 Mrs A made a payment of £485 to someone for a Samsung mobile phone, which it later transpired was not a legitimate device.

In December 2021, Mrs A was on an online marketplace and found an advert for a Samsung phone. The seller said it was an unwanted gift and they wanted a quick sale, so they would sell it for £485. Mrs A received the phone and on first inspection it looked like the Samsung phone she was expecting, but upon further use she discovered it was not a legitimate Samsung phone – it was a much cheaper and lower quality device made by another company altogether. Mrs A had this confirmed when she had the phone assessed through a mobile application. She tried to contact the seller as she wanted to return the phone and get her money back, but the seller would not respond to her. It was at this point Mrs A realised she had fallen victim to a scam and contacted Metro.

Metro investigated Mrs A's complaint and issued its final response and declined to refund her losses. In summary, they did not accept liability because the funds were sent by bank transfer to the seller which they said meant they could not assess the case as a scam or a card dispute – they said it could better be classified as a buyer/seller dispute.

Unhappy with Metro's response, Mrs A brought her complaint to our service and one of our investigators looked into what had happened. They did not recommend that her complaint be upheld. They did think that Mrs A had most likely fallen victim to a scam, but they did not think the payment was unusual enough for the bank to have provided any warnings or interventions, and did not think that Mrs A had demonstrated that she met her requisite level of care when making the payment. Mrs A remained dissatisfied, so the case has been passed to me to decide.

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 broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Service Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

When thinking about what is fair and reasonable in this case, I have considered whether Metro should reimburse some or all of the money Mrs A lost in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect Mrs A from the possibility of financial harm from fraud.

There appears to be some dispute that Mrs A was the victim of an authorised push payment scam here. The code establishes that an authorised push payment scam can be defined as where the customer transferred funds for what they thought were legitimate purposes, but they were in fact fraudulent. It also explains that the code does not apply in disputes relating to private civil disputes, which can include where a customer pays a legitimate supplier for goods that are defective in some way, or where the customer is otherwise dissatisfied with the supplier. In this case Mrs A thought she was sending funds to purchase a Samsung mobile phone but instead she received a cheaper knock-off phone in a Samsung case. Metro have argued that as Mrs A received a phone, even if it was not the one she wanted, this would not be classed as a scam – that is should be classed as a private civil dispute. But I think on balance that it is most likely that the 'seller' sent Mrs A an illegitimate device in the hope that she didn't notice – which is why she declined to respond to any further communication after Mrs A received the device. So, I am satisfied that this should be considered a scam and therefore that the CRM code applies here.

The CRM Code

Metro has agreed to adhere to the Lending Standards Board Contingent Reimbursement Model ('CRM') Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It sets out standards that banks, such as Metro, are expected to meet in terms of protecting their customers from financial harm. But it also sets out expectations that a customer should meet, too. As a starting point, a customer should receive a full refund if they fall victim to an authorised push payment scam such as this one.

But Mrs A would not be entitled to a full refund if Metro can fairly and reasonably demonstrate that she has failed to meet the requisite level of care under one of more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- The customer ignored an effective warning in relation to the payment being made;
- The customer made the payment without 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 further exceptions within the CRM Code, but they do not apply in this case.*

Did Mrs A have a reasonable basis for belief?

Unfortunately, I think the evidence suggests that Mrs A did not have a reasonable basis for believing that she was buying a legitimate handset when she made the transfer. I say this because at the time of the scam, the specific model of phone Mrs A thought she was buying brand-new retailed for over double the price she thought she was paying for it – she paid £485 and they were selling for over £1,000. I understand the scammer told her it was an unwanted gift which would explain it being sold at a price somewhere below the recommended retail price – but even the second-hand models seemed to go for around £300 more than she was paying (selling averagely for around £800 at the time). So she thought she was being offered a brand new handset at a price significantly below not just the price for a brand new phone – but for significantly below the price of a used phone too. I think this should have appeared unusual to Mrs A. I think this price sounded too good to be true, and so it should have alerted Mrs A to the risk of falling victim to a scam.

The platform Mrs A used is ultimately used to link private sellers to private buyers. It says customers should not part with their funds for goods if they have not been able to verify the goods they are buying in person. I appreciate there are a variety of reasons why Mrs A may not have been unable to do so, but in the first instance I would expect her to look for a device somewhere close to home so she could inspect the goods before parting with any

funds. If this was not possible I would have expected her to use a different purchase method or website, or a different payment method to get the model of phone she wanted. Ultimately here, she sent funds to an unknown third party who was offering her a deal that ought to have seemed too good to be true, via bank transfer, without any particular buyer protections available from the website she was using. So I think it is fair to conclude that Mrs A had not done enough to protect herself here. And by extension, I think Metro acted fairly in saying that this exception to refund under the CRM code was applicable in this case.

Did Mrs A ignore an effective warning?

Under the CRM Code, Metro are required to present an effective warning where they identify a scam risk. But I don't consider that the payment made by Mrs A was so out of the ordinary that the bank ought to have believed there was a scam risk. The amount sent wasn't sufficiently unusual in size, nor do I consider there to have been any concerning features of the payment to put Metro on notice that Mrs A was at risk of financial harm. And so, I don't believe Metro needed to do more than it did in terms of providing warnings about making the payment.

Should Metro have done more to protect Mrs A?

In addition to their responsibilities under the CRM code, when Mrs A made the payments, Metro should fairly and reasonably have had systems in place to look out for unusual and out of character transactions or other signs that might indicate that Mrs A was at risk of fraud or financial harm (amongst other things). However, as outlined above, there was nothing about the payment that ought reasonably to have alerted Metro that Mrs A was at risk of fraud or financial crime – so I do not think that they needed to intervene with the payment at the time it was being made.

Recovery

I have also considered whether Metro could have done more to try to recover the money once it had been told of the scam. We would expect a business to take reasonable steps to try and recover the money from the bank it was sent to, with urgency, after their customer notifies them they fell victim to a scam. Metro did not accept that Mrs A had fallen victim to a scam as they believed this to be a civil dispute, so they did not attempt to recover the funds. However, our investigator reached out the receiving bank who have confirmed that the receiving account was emptied before Mrs A contacted Metro – so even if they had acted in line with how I would expect following a scam report, they would not have been able to recover any of Mrs A's funds. So I cannot say their failure to attempt recovery made any material difference here.

My final decision

My final decision is that I do not uphold this complaint, and require Metro Bank PLC to do nothing further.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 10 November 2023.

Katherine Jones
Ombudsman