DRN-4271220

The complaint

Mrs M complains that HSBC UK Bank Plc won't refund money she lost, as the result of an Authorised Push Payment (APP) scam.

What happened

Briefly, Mrs M was showed by a relative a shop advertising items on a social media platform that claimed to be closing down. The shop was advertising various items, such as jewellery, electronics and mobile phones. Mrs M enquired with the seller via messages about a mobile phone, which the seller said was available for £145 including delivery. Mrs M's close relative decided to purchase this item, which I understand Mrs M helped make the payment for from the relative's own bank account. However, I understand that Mrs M and her relative were told the payment was being returned due to them selecting business account at the time of making that payment, when the account details were for a personal account. Mrs M says the £145 was returned to the relative's account.

Mrs M agreed to send the payment again. She also agreed with the seller to purchase jewellery/gold (necklaces, bracelets and rings) which they were selling for £380. For all the items (gold and mobile phone), Mrs M and the seller agreed to a total purchase price of £450.

Mrs M then received further communications from the seller saying the money was being returned in error by the seller's bank. It was agreed between Mrs M and the seller that the price would be slightly cheaper, and she proceeded to make another payment for £430.

Mrs M was in contact with the seller about the delivery of the items, as she'd not received a tracking number or the items despite her requests. The seller then informed Mrs M that due to further errors on their end, all the payments had been sent back – to Mrs M's account and her relatives (I understand Mrs M's relative had also made an order). For Mrs M, the seller referred to the payments of £450 and £430.

Between this time, Mrs M told us she contacted HSBC via its chat function to ask the bank if it could see any pending refunds on the account. At this time, the bank's agent said they couldn't see any pending refunds for the amounts Mrs M had said but that as she said the merchant had issued the refund the day before, it could take up to five working days to reflect on the account. The agent suggested waiting until then. Mrs M shared that the seller was requesting payment again as they were saying the payments had been sent back in error. She commented that she didn't want to pay so much money and for them to scam her. She was told a dispute could be raised and was given some details about the process. Mrs M said she would wait.

In the further communication between the seller and Mrs M she was told that all items would return to their original prices and if she wanted to proceed with the order they would agree a reduced price of £700 for all the items (her and her relative's). Mrs M proceeded to make a further payment of £700 to the account details provided.

Unfortunately, Mrs M was interacting with a fraudster and had been duped into paying a total of £1,580 (made up of three payments for £450, £430 and £700, which she made between 6 March 2023 and 9 March 2023 from her HSBC account). Mrs M didn't receive the phone or jewellery she thought she was purchasing. Mrs M contacted HSBC to report the scam on 23 March 2023.

HSBC is a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code). This means HSBC has made a commitment to reimburse customers who are victims of authorised push payment scams like this one except in limited circumstances. HSBC investigated Mrs M's fraud claim and it issued its final response on 3 May 2023 not upholding it. In summary, it didn't think Mrs M had carried out sufficient checks to satisfy herself of the credibility of the company or seller, it considered Mrs M ought to have questioned the cost of the items she thought she was buying as to whether they were in line with the market value and, that she failed to check payments one and two had been returned to her before making a further payment. HSBC also considered there to be appropriate fraud warnings in place at the time she made the payments. HSBC attempted to recover Mrs M's funds from the receiving bank, however, no funds were recoverable.

Unhappy with HSBC's response, Mrs M brought her complaint to our service. One of our Investigator's looked into the complaint and didn't uphold it. In summary, she thought Mrs M had been the victim of a scam, but, when considering the CRM code, she didn't think HSBC was liable to refund her the money she'd lost. She said this because she thought there was enough going on for Mrs M to have had concerns about the payments she was making.

Mrs M didn't agree with our Investigator's view. As agreement couldn't be reached the complaint 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.

There's no dispute that Mrs M authorised the payments that are the subject of this complaint. Broadly speaking, under the account terms and conditions and the Payment Service Regulations 2017, she would normally be liable for it. But that isn't the end of the story.

Where a customer has been the victim of a scam it may be appropriate for the bank to reimburse the customer, even though payments have been properly authorised. Of particular relevance to the question of what is fair and reasonable in this case is the CRM Code. As I've said above, the CRM Code requires firms to reimburse customers who have been the victims of APP scams like this, in all but a limited number of circumstances. A Firm may choose not to reimburse a customer if it can establish that*:

- 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.

**Further exceptions outlined in the CRM Code do not apply to this case.*

Taking into account all of the circumstances of this case, including the characteristics and complexity of the scam, I don't think Mrs M had a reasonable basis for believing the payments were for genuine goods or services; and/or the person or business with whom they transacted was legitimate. I'll explain why.

I think a key factor here is the price Mrs M was paying for the items she was looking to buy - the mobile phone and the jewellery/gold. And whether the prices were 'too good to be true' and to such an extent that it should have given Mrs M cause for concern that it might not be a legitimate sale or that the items might not even exist.

Mrs M agreed a total price of £450 for all the items with the mobile phone being priced at £145. The various gold items, Mrs M confirmed with the seller were 22 carat gold. When taking into account the make and specification of the mobile phone Mrs M had agreed to purchase, I find the price offered too good to be true, based on the searches I have completed. I recognise Mrs M says the prices were claimed to be wholesale prices, but I'm not persuaded the seller telling Mrs M that the items were being sold at wholesale prices due to it closing down in and of itself persuasive.

I note Mrs M in her submissions to our Investigator, has referred to having a business and that she said she knows when you want to get rid of stock it can be sold at the buying rate – with no profit being made. But on balance, based on what I've seen, I'm not persuaded the prices the items were offered at to Mrs M were in line with the market value and therefore, I think this ought reasonably to have given Mrs M pause for thought – although I do acknowledge Mrs M will not agree with this point. She's further told us that in January 2023, she bought a brand-new phone (same make and model) for £250. I've not seen evidence of this, however, I still find the seller offering the item at £105 cheaper than this, to have been a factor that should have given Mrs M some cause for concern.

Further, based on what I've seen and been told, I think Mrs M herself had some concerns from the outset. Looking at the messages between Mrs M and the seller, I note after she'd enquired about the mobile phone and asked for the bank details, she commented, 'if it's a scam can very easily get my money back'. I can also see a further comment of 'if that reaches and everything's okay and you haven't run off with my money lol then I'll think about ordering more things'. To my mind, this strongly suggests that Mrs M at the time of making the payments, herself wasn't convinced that whom she was transacting with was legitimate or that the she was making a payment for genuine goods or services. I can also see Mrs M questioned why the items were so cheap.

With all this in mind, while I've carefully taken into account what Mrs M has told us about the items and why she disagrees the prices were too good to be true, for the reasons set out above, I'm afraid I don't agree.

When reporting the scam to HSBC Mrs M explained she'd searched the unit the seller said they operated from online and said it existed at the location the business claimed to be at. She added that her relative had told her it was genuine, although in the call with the bank she didn't state what it was that had convinced the relative of this. Mrs M didn't receive any invoice/paperwork for the items she was purchasing from the seller. I do note Mrs M says she's purchased items over social media platforms previously and not been provided with a receipt. Mrs M maintains that this is not unusual for businesses on social media platforms and added that many businesses on such platforms don't have/show an address.

Whilst I can appreciate that making purchases over such platforms has and continues to increase, given the items Mrs M was looking to purchase in this case – mobile phone and numerous items of 22 carat gold jewellery, I think the lack of documentation ought to have led Mrs M to proceed more cautiously than she did. I'm mindful that other than the advert/ pictures of the items on the platform which Mrs M says were deleted once sold, she doesn't appear to have been provided with anything that supported the seller did have the items in question for sale.

After Mrs M made the payment of £450, the seller contacted her to say the funds were being returned. It said the reason for this related to the first payment being sent to one of its business accounts. The seller said as its business accounts are linked and the same payment has come in from Mrs M's account, the bank has returned this payment. I think what the seller was telling Mrs M ought to have caused her some concern and that she should have fairly and reasonably have paused to think about the plausibility of what she was being told. It was after Mrs M was told again about an error with the seller's bank in which both payments – the £450 and £430 were being returned that she contacted HSBC via its chat function to see if there were any pending refunds to her account. At this time, the bank informed Mrs M that it couldn't see any pending credits to the account but that it could take five working days and so advised her to wait. I'm persuaded Mrs M ought to have waited to have received the payments back into her account before proceeding to make further payments – especially when taking into account the messages she'd received from the seller about the delays with the delivery and the bank issues being communicated by the seller.

I also think there were further red flags that ought to have given Mrs M pause for thought as the scam progressed. I will explain why. Whilst it is not the clearest, based on what I've seen and been told, it appears that when the seller informed Mrs M that all three payments had been sent back, this also included a payment her relative had made for an order. Due to the further issues, the seller then offered to sell all the items (again, it appears to have included the relatives order) for £700. Given that the three payments the seller refers to in the chat messages were £450, £680 and £430, I think this ought to have caused Mrs M some concern. I acknowledge the seller had previously made a reduction in the price agreed with Mrs M due to the issue it claims occurred with its bank when making the payment for £430. But I find the new price offered for all the items ought to have appeared unusual to Mrs M and led her to question what she was being told. I say this because, Mrs M agreed a price of £430 for her items and the other payment the seller referred to as being returned is for £680 (I understand this to be the relative's order). So, all the items being offered at £700 to my mind ought to have been a flag here as this represented around a further £400 reduction in the prices previously agreed and which Mrs M believed were already being sold at wholesale prices.

I'm mindful that, taking any of the individual factors above in isolation, they may not have been enough to have prevented Mrs M from proceeding to make the payments. But when taken collectively and considering the specific circumstances of this case and the factors in the round, on balance, I think that there was enough going on and sufficient red flags that Mrs M ought reasonably to have been concerned that things weren't as they seemed.

Overall, I don't think I can fairly conclude that Mrs M had a reasonable basis for believing that she was making payments towards genuine goods, or that the person she was dealing with was legitimate. So, I'm not persuaded that HSBC should have reimbursed Mrs M's loss because of any obligation under the CRM Code.

I've also carefully taken into account what Mrs M has told me about being vulnerable at the time. I'd like to assure her that I don't underestimate the impact the whole experience will have had on her and her family and that I've thought carefully about what she's said. But I don't think what I've been told was significant enough to have meant Mrs M couldn't have taken steps to protect herself from the scam she fell victim to.

I want to emphasise though that this is not to underestimate the circumstances she was in at the time, or the subsequent impact the scam has had on her. It is simply that I don't find the evidence would justify a finding that Mrs M was unable to have taken further steps to protect herself here.

Should HSBC have done anything else to prevent the scam?

Good industry practice requires that regulated firms such as HSBC engage in the monitoring of customer accounts and to be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. And under the CRM Code, where it identified a risk of a customer falling victim to an APP scam, it was required to provide that customer with an "effective warning".

We now know, with the benefit of hindsight, that Mrs M was falling victim to a scam. But based on the information that was available to it at the time, I don't consider HSBC would've had any reasonable basis for coming to that conclusion. I say this because the payments wouldn't have appeared so out of character or unusual. Whilst I recognise the payments were a lot of money to Mrs M, I don't find them to be particularly large or remarkable. So I don't think the CRM Code required that HSBC display an effective warning as part of the payment process, and I'm not persuaded it would've had any grounds for intervening to question the payments with Mrs M before allowing them to be processed.

Recovery of funds

I've also considered whether HSBC did all it could to try and recover the money Mrs M lost, once she had reported the scam to it. From what I've seen, I think the bank could've acted quicker than it did in contacting the receiving bank. However, I don't find any possible delay made a difference in this case. I say this because, the funds had unfortunately already left the receiving account before Mrs M had reported the matter to HSBC. So overall, I don't think there was anything more HSBC could've done to recover Mrs M's funds.

It's very unfortunate Mrs M has lost this money in this way, and I understand the whole experience has been deeply upsetting and I have a great deal of sympathy for her and I don't underestimate the impact this has had. But in the circumstances, I don't think I can fairly or reasonably ask HSBC to refund her the money she sadly lost.

My final decision

For the reasons I've set out above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 6 October 2023.

Staci Rowland
Ombudsman