DRN-4751748

The complaint

Mrs M complains that HSBC UK Bank Plc (HSBC) won't refund money she lost in a safe account scam.

What happened

What Mrs M says:

Mrs M got a 'phishing' text purporting to be from a delivery company. She clicked on it. She was then contacted by someone claiming to be from HSBC who said her HSBC account had been compromised as a result. And told her to move her HSBC money into a 'safe account' at another bank (which I will call bank A). She already had an account at bank A.

After the funds arrived at bank A, she was then told to move the funds to another 'safe account' – which she did. She only moved half of the funds in that way, and paid the rest back to HSBC, so reducing her loss.

The payments were:

Date	Payment	Amount
13 September 2023 – 19.26	Faster payment	£860
13 September 2023 – 19.28	Faster payment	£890
13 September 2023 – 19.29	Faster payment	£920
13 September 2023 – 19.31	Faster payment	£960
13 September 2023 – 19.32	Faster payment	£980
14 September 2023	Credit from bank A	(£2,606.66)
Total		**£2,003.34**

(continued)

Mrs M complained that HSBC should've done more to protect her. The payments were made in rapid succession on the same day and were out of character for her. And when the scammer called and posed as being from HSBC, she checked the number and it was shown as HSBC's real number. So – HSBC should take precautions against this happening. All this meant that this was HSBC's fault. She says HSBC should refund the money she's lost. She said she needs to the money to live – e.g. to pay bills and the mortgage. It was a huge

amount of money for her to lose, but a small amount for HSBC and bank A.

What HSBC said:

- HSBC said the Contingent Reimbursement Model (CRM) code didn't apply as the money was sent to an account in Mrs M's name (at bank A).

- Mrs A should contact bank A – from where the funds were sent to the scammer as that was where her losses took place.

Our investigation so far:

Mrs M brought her complaint to us. Our investigator didn't uphold it. He said:

- HSBC showed 'safe account' warnings to Mrs M when she made the payments.

- The payments were of a low value and Mrs M had transferred money from her HSBC account to bank A before.

- It was a common tactic for scammers to 'spoof' a bank's number to give the impression they were calling from that bank – that wasn't something HSBC could be held responsible for.

Mrs M didn't accept this and asked that an ombudsman look at her complaint, and so it has come to me to make 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.

I'm sorry to hear that Mrs M has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although Mrs M didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I need to decide whether HSBC acted fairly and reasonably in its dealings with Mrs M when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary – and in this case, the payments were made to Mrs M's own account with bank A.

In this case, I don't consider HSBC acted unfairly or unreasonably in allowing the payments to be made. Whilst I understand the loss has had a big impact on Mrs M (as she's explained), I don't consider the payments were so out of character that HSBC ought reasonably to have had concerns that Mrs M may be the victim of fraud. For example, I can see the following large payments from her account leading up to the scam:

August 2023: £10,000; £5,000.
July 2023: £2,000.
April 2023: £2,600.

Mrs M has argued that the payments were made in rapid succession, and I considered this point. But unfortunately, we can't expect firms to question every payment of a relatively low value, even in those circumstances.

There's a balance to be made: HSBC has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments.

So, in this case, I think HSBC acted reasonably in processing the payments.

I'm also mindful that HSBC did send Mrs M a warning about safe account scams when the payments were made, but she went ahead. This said *"Don't proceed if you're being asked to move money for safekeeping purposes. Call HSBC using the number on the back of your card to verify the request."*

Mrs M has argued that it's HSBC's responsibility to prevent the HSBC phone number from being spoofed – as she checked the number and it was HSBC's. Unfortunately we can't reasonably expect firms to do this – it is sadly typical of a tactic that criminals use. The best thing that Mrs M could've done was to hang up the call from the scammer and call HSBC's number herself – as HSBC's warning said. This would've revealed that HSBC hadn't called her. (**continued)**

Recovery
We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether HSBC took the necessary steps in contacting the bank (bank A) that received the funds – in an effort to recover the lost money.

I couldn't see that HSBC did that. So I looked at what happened at bank A (as this is also a complaint brought to our service). And – this shows that the funds were moved out of bank A to the scammer's account at 20.39 on the same day. Mrs M contacted HSBC at 20.33 (and the call took about 35 minutes). So, by that time, the money had been paid away by bank A. It's in the nature of such scams, that the money is removed within minutes and that's what happened here.

So anything HSBC could've done wouldn't have been able to get any of Mrs M's money back.

Mrs M has lost a lot of money. She's explained why the money was important to her, and the impact her losses have had. I was sorry to learn of her circumstances. She will therefore be disappointed by my decision, but I'm not going to ask HSBC to do anything here.

My final decision

I do not 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 30 May 2024.

Martin Lord
Ombudsman