DRN-4684944

The complaint

Mrs N complains that HSBC UK Bank Plc won't refund all the money she lost when she was the victim of a scam.

What happened

In March 2023, Mrs N received a text message which appeared to come from HSBC saying there had been suspicious activity on her account and someone would contact her. She then received a phone call from someone who said they worked for HSBC and said her account had been compromised, so she needed to move her money to two new accounts in order to protect it.

Over the next few days, Mrs N then made a number of payments out of her HSBC account to the new bank details the caller gave her. I've set out the payments she made below:

Date	Details	Amount
8 March 2023	1st account details	£2,540.89
8 March 2023	1st account details	£2,436.11
8 March 2023	1st account details	£950
9 March 2023	1st account details	£2,410.66
9 March 2023	**1st account details**	**£2,400.22**
10 March 2023	2nd account details	£2,960.11
10 March 2023	**2nd account details**	**£2,954.33**
10 March 2023	**2nd account details**	**£2,430.66**

Mrs N was also told she needed a replacement debit card, and that she needed to disclose her PIN and give her existing card to a courier who would come and collect it – which she did. A number of card transactions were then also made from Mrs N's HSBC account over the following days.

Unfortunately, we now know the caller was a scammer. The scam was uncovered when Mrs N wasn't contacted again after moving the money. She then contacted HSBC herself, and was told she had been the victim of a scam. Mrs N then reported the payments and card transactions made from her account and asked HSBC to refund the money she had lost.

HSBC investigated and didn't initially agree to refund any of the money Mrs N lost. But it then reviewed its decision and said it could have done more to protect Mrs N when she made three of the payments, highlighted in bold in the table above, so it agreed to refund these. It also agreed to refund all of the card transactions, as it accepted Mrs N hadn't made these herself. But it said it had taken sufficient steps to protect Mrs N before the remaining five payments, so didn't agree to refund these.

Mrs N wasn't satisfied with HSBC's response, so asked our service to investigate her complaint. One of our investigators looked at the complaint and said they felt it was reasonable for Mrs N to think she was genuinely talking to HSBC when the payments were made. They also didn't think the warnings HSBC had shown Mrs N before the remaining five

payments were effective. So they thought HSBC should refund the remaining payments to Mrs N. HSBC disagreed with our investigator, so the complaint has been passed to me.

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.

HSBC has already refunded all the card transactions made after Mrs N gave her card to the courier, as well as the three payments highlighted in bold in the table above. And so I haven't considered these further and have focused on the payments that haven't yet been refunded.

In broad terms, the starting position in law 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. However, where the customer 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 customer even though they authorised the payment.

HSBC is a signatory of the Lending Standards Boards Contingent Reimbursement Model (the CRM code). This code requires firms to reimburse customers who have been the victim of authorised push payment scams, like the one Mrs N fell victim to, in all but a limited number of circumstances. And it is for the firm to establish that one of those exceptions to reimbursement applies.

Under the CRM code, a firm may choose not to reimburse a customer if it can establish that:

- 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 these don't apply here.

Did Mrs N ignore an effective warning in relation to the payments?

The CRM code says that an effective warning should enable a customer to understand what actions they need to take to address a risk and the consequences of not doing so. And it says that, as a minimum, an effective warning should be understandable, clear, impactful, timely and specific.

HSBC has sent us a copy of the warning it says Mrs N was shown when first setting up the payments, which said:

*"**Caution – This could be a scam***

***WARNING** – if someone has told you to mislead us about the reason for your payment and / or choose the wrong payment type, **stop, this is a scam**.*

Fraudsters may use social media to build up a relationship with you and gain your trust before asking you to send them money eg making contact via a dating site. They may also pretend to be a friend or family member by hacking their social media profiles, or ask you to transfer money for safekeeping.

What you need to do before making the payment:

- ***stop and think*** *– have you been asked to send money for emergencies like travel or medical expenses by someone you've only met online?*
- ***don't make a payment*** *to someone you've only met online*
- ***don't move money for safekeeping purposes – call us*** *using the number on the back of your card to check first*
- ***be suspicious*** *if you've been contacted out of the blue, by text or on social media by somebody saying they're a friend or family member*
- ***take time to talk it through with somebody*** *you trust before sending any money"*

But while this warning does mention to not move money for safekeeping purposes, I don't think it was detailed enough about what this kind of scam might look or feel like. It doesn't mention that scammers might pretend to be from a bank or other trusted organisations, or say that the customer's money is at risk if it is not moved elsewhere. The warning also mentions a number of other things, like sending money to someone you've met online, which weren't relevant to Mrs N here. So I don't think it was specific enough to be effective in Mrs N's circumstances.

The warning also says to stop if someone has told you to mislead HSBC or choose the wrong payment type, as Mrs N was told to and did here. But I think the explanation of fraud departments not communicating with each other Mrs N was given about why she shouldn't mention the phone calls she had was plausible. And, at the point she saw this warning, she thought she had called the number back to confirm it was HSBC – similar to the action the warning suggested. So I don't think it was unreasonable that she navigated past the warning without taking any further action.

And so I don't think HSBC has established that Mrs N ignored an effective warning in relation to these payments.

HSBC has argued that Mrs N selecting 'friends and family' when asked what the purpose of the payments was, and so misleading it about the true purpose of the payments, prevented it from showing a more effective warning. But the test under this part of the CRM code is just whether Mrs N ignored an effective warning. And, regardless of why she was shown this particular warning, I don't think the warning she was shown was effective in her circumstances or that she acted unreasonably in moving past it. So I still don't think HSBC has established that Mrs N ignored an effective warning.

Did Mrs N have a reasonable basis for belief when making the payments?

This was a sophisticated scam, where the scammers used a number of different steps and methods to persuade Mrs N that what was happening was genuine.

The first contact Mrs N received was a text message which said suspicious activity had been identified on her account and a member of HSBC's team would contact her shortly. The message displayed on Mrs N's phone as if it had come from HSBC, and included an authentication code – presumably to be used when the team later contacted her. So I think it's reasonable that this message will have seemed genuine to Mrs N.

She then later received a call claiming to be from HSBC, as the text message said she would. And Mrs N says the caller went through an identity verification process with her at the start of the call, similar to ones she has been through in genuine calls with HSBC. She says the caller also knew the long number from her debit card, sounded professional, and used

phrases genuine HSBC staff have used in phone calls with her. So I think it's reasonable that Mrs N thought the phone call was genuinely from HSBC and I don't think there was anything about the call that should have caused her significant concern.

The call Mrs N received also appeared to come from a number that was only one digit different than HSBC's genuine phone number. And, after the initial call she received, Mrs N says she called the number back to check it and that call was answered by someone saying it was HSBC. So I think this will have reasonably reassured Mrs N that the call had genuinely come from HSBC.

And while Mrs N was shown a warning when setting up the payments, as I explained above, I don't think this was specific enough to be effective in her circumstances. And, given the seemingly genuine circumstances of the calls up to that point and the steps she had taken to try to reassure herself the calls were genuine, I don't think it was unreasonable of her to navigate past this warning.

There were some things about what was happening that I think should have caused Mrs N some concern, such as being asked to mislead HSBC about the purpose of the payments and being asked to make a number of small payments, rather than just one large transfer of all of her money. But, from what she's said, the scammers did offer some explanations for why these things were necessary which I think will have sounded plausible. And, by the time these things were happening, Mrs N had been on seemingly genuine calls with the scammers for some time. So I think it's reasonable that the seemingly genuine parts of what was happening were enough to overcome these concerns and I don't think it would be fair to say Mrs N acted unreasonably in still proceeding with the payments.

So I don't think HSBC has established that Mrs N made the payments without a reasonable basis for belief that they were genuine.

Overall then, I don't think HSBC has established that any of the exclusions to reimbursement under the CRM code apply here. So I think it should refund the money Mrs N lost, in full, under the terms of the CRM code.

Customer Service

HSBC has paid Mrs N £50 as compensation for the customer service issues she experienced when she raised this claim. And, from what I've seen, I think this is fair and reasonable compensation for the distress and inconvenience this poor customer service caused her. So I don't think it would be fair to require HSBC to pay any further compensation.

Previous refunds

As part of the refunds it has already provided, HSBC refunded two payments of £17.40 and £27 that Mrs N has said she wasn't disputing. HSBC may therefore either re-debit these refunds or deduct these amounts from the refund set out below.

My final decision

For the reasons set out above, I uphold this complaint and require HSBC UK Bank Plc to:

- Refund Mrs N the remaining £11,297.77 she lost as a result of this scam
- Pay Mrs N 8% simple interest on this refund, from the date it initially responded to her claim, until the date of settlement

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs N to accept or reject my decision before 17 May 2024.

Alan Millward
Ombudsman