

The complaint

Mrs R is unhappy that HSBC UK Bank Plc has only refunded some of the money she lost to a scam.

What happened

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

- In February 2022 Mrs R received a text from, what appeared to be, the NHS about covid-19 contact tracing which asked her to get tested. She clicked a link to buy a test and, as part of that process, provided various personal details as well as her bank and credit card details. A discussion with a friend soon afterwards helped her release this might actually have been a scam. So she called HSBC who arranged for her credit card to be stopped and a replacement issued. A discussion took place about the scam and some warnings were given by the bank.
- The next day Mrs R received a phone call from someone who said they worked for HSBC's fraud team. This individual, who turned out to be a scammer, persuaded Mrs R that her account had been compromised and the money in it needed to be moved to a safe account. He told Mrs R to move £7,000 into her current account from her savings account. He then guided her through the process to create a new payee for an account which was supposedly in her name. And he persuaded her to make a payment of £3,950 and then £3,850 to this account. The call disconnected after the second payment and Mrs R soon realised she'd been scammed, so called HSBC to report the fraud.
- HSBC considered Mrs R's claim under the Contingent Reimbursement Model Code. The bank said Mrs R had been given effective warnings while processing the first payment and during the previous day's conversation, but no warnings were given in connection with the second payment. It also said Mrs R ought to have done more to check the caller was a genuine bank employee. So the bank refunded 50%, or £1,925 of the second payment. Mrs R didn't think she'd been treated fairly, so asked us to look into her complaint.

I issued a provisional decision earlier this month setting out why I was minded to uphold Mrs R's complaint in part. I have reproduced my provisional findings here:

There's no dispute that Mrs R made the two payments to the scammer from her HSBC account. That means they were authorised by her. So the starting point under the Payment Services Regulations 2017 and the account terms and conditions is that Mrs R is responsible for the payments along with any resulting losses.

But the matter doesn't end there. I've also considered whether Mrs R should have received a refund of the money she lost under the provisions of the voluntary Contingent Reimbursement Model Code ("the Code"). HSBC has signed up to the Code, which is designed to reimburse victims of authorised push payment scams. But the Code places a level of care on Mrs R too.

Under the CRM Code, and relevant to this particular complaint, a bank may choose not to reimburse a customer if it can establish that:

- The customer ignored what the Code refers to as 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.*

The Code defines the requirements for a scam warning to be considered “effective” and I’m not currently satisfied those requirements were met. As a result, Mrs R can’t be said to have ignored an effective warning. I say this because:

- HSBC has pointed to the warnings given to Mrs R in a call that took place the day before the safe account scam was actually perpetrated. The Code requires that the warning must be delivered in a timely manner “at points in the payment journey most likely to have impact on the Customer’s decision-making.” So I don’t think HSBC can fairly rely on a warning given the day before the payment was made. Although I do think the discussions that took place during that call should be taken into account when deciding if Mrs R had a reasonable basis of belief and I will speak more about that below.*
- HSBC has provided various screen shots of the process Mrs R would have followed to set up the new payee. And I see a warning is given that criminals may pretend to be people the customer trusts (like HSBC), but it will never ask the customer to move money. But this warning is located at the bottom of the screen below six fields where the payee’s details must be entered and below the button the customer must press to move to the next part of the process. I think this message could be missed, particularly in Mrs R’s situation where she was being coached by a scammer. And, in any event, the warning doesn’t explain that the payment would be irrevocable or mentions the consequences of proceeding. So it doesn’t meet the requirements of an effective warning.*
- HSBC has provided screen shots of the various payment reasons it says it presents to customers after it identified a high risk transaction, along with a warning about fraudsters pretending to be from places you trust, like your bank. But I don’t think this warning goes far enough given the requirements of the Code. And, in any event, HSBC hasn’t shown me which payment reason Mrs R selected so I can’t be sure she was shown this message.*
- HSBC has already accepted that it ought to have identified a scam risk and given an effective warning when Mrs R made the second payment. I agree with this position.*

I currently think HSBC has done enough to establish that Mrs R didn’t have a reasonable basis for believing the person she was sending money to was legitimate. I say this having taken the following into account:

Mrs R realised she’d been scammed the day before she made these two payments to the fraudster. I’ve listened to a recording of the conversation she had with the bank when she reported this. She explained, unprompted, what had happened and commented that the scam was very clever – she’d thought it was a bit strange but still provided her personal and bank details. Mrs R also asked HSBC specifically if her debt card was at risk because although she hadn’t given away those details, she had given her bank account details. The

bank reassured Mrs R that the debit card details hadn't been compromised and a scammer couldn't make transfers from her account just by being in possession of her bank account details.

The call-handler went on to explain that:

- Criminals were becoming more sophisticated and Mrs R might get one or more phone calls from someone pretending to be HSBC or the Police.
- These callers might use various tactic including saying that her account is unsafe and/or that she would need to move her money to a safe account.
- HSBC would never ask for her security credentials or ask her to move her money.
- If Mrs R received this type of call then she should hang up and call the bank, preferably from a different phone.

Mrs R did sound slightly distracted at the end of this call when the call-handler asked if he could help with anything else. But I think she'd seemed engaged prior to this including during the warnings, agreeing several times with what the call-handler was saying. And, importantly, when she called to report the scam the next day she mentioned, unprompted and very early on in the call, that she's been told the previous day not to take the call if she did receive one from the bank.

Mrs R also tells us she was anxious and unsure about what the scammer was saying at various times during the call. She asked the scammer lots of questions and made the first payment nervously. For example, she asked the scammer how she could be sure he was a genuine employee and he pointed to the number he was calling from which was one digit different to the one on the back of Mrs R's card. It's not clear to me why, given the warnings given the previous day, Mrs R didn't just hang up and call the actual number on the back of her card.

Mrs R also says the scammer told her that her current account was being hacked and she needed to make two payments that amounted to more than to £7,000 to activate her new account. And, when Mrs R questioned this, the scammer said that amount had something to do with HSBC's policy and retaining her Premier Customer status. Mrs R says the scammer was calm and confident but also rushing her and I know these are common tactics that scammers will use. But I also have some difficulty understanding why Mrs R accepted what she was being told. The £7,000 was in her savings account and she doesn't suggest the scammer told her this account was similarly compromised – so why was it necessary to move this money out? But even if that was the case, there's been no suggestion that was the full amount held in her account and I note there was more than £1,000 left in her current account after making the two payments out. And if Mrs R thought her money was at risk then I don't understand why she didn't move all of her money out.

I appreciate the scammer was able to give confident answers to each of Mrs R's questions and likely stressed the urgency of the situation. But I also wonder if her nervousness stemmed, in part, from having been scammed just the day before. Those events and the warnings given by the genuine bank's employee may still have been in her mind. In the circumstances, I currently think Mrs R too readily accepted the scammer's explanations. Overall, as both parties ought to have done more here, I currently consider a fair outcome in this case is for HSBC to reimburse 50% of both payments. As noted above, the bank has already refunded 50% of the £3,850 payment.

I'm satisfied that when HSBC was made aware of what had happened it tried to recover the money. Unfortunately, those attempts seem to have been unsuccessful.

Putting things right

For the reasons outlined above, I currently think HSBC UK Bank Plc should:

- *Refund £1,975 (equal to 50% of first payment she made to the scammer).*
- *Add interest on the above refund calculated using the rate applicable to Mrs R's savings account. I say this because I think it's more likely than not that, if Mrs R hadn't fallen victim to this scam, she would've left that money in her savings account.*

Mrs R and HSBC both accepted my provisional findings.

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.

Having done so, and as neither party has sent any new evidence or arguments for me to consider, I see no reason to depart from the conclusions set out in my provisional decision and reproduced above.

My final decision

My provisional decision is that I uphold this complaint in part and I instruct HSBC UK Bank Plc to settle the matter as follows:

- Refund £1,975 (equal to 50% of first payment Mrs R made to the scammer).
- Add interest on the above refund calculated using the rate applicable to Mrs R's savings account.

If HSBC considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Mrs R how much it's taken off. It should also give her a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

HSBC should settle the matter within 28 days of receiving notification of Mrs R's acceptance of my final decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs R to accept or reject my decision before 18 April 2023.

Ruth Hersey
Ombudsman