DRN-3237571

The complaint

Mr P complains that HSBC UK Bank Plc won't refund the money he lost when he was the victim of a scam.

What happened

Mr P received a call from someone claiming to be from HSBC. The caller asked Mr P if he recognised a transaction that had been attempted on his account in Aberdeen and, when he said he didn't, told him there had been fraud on his account. The caller then told Mr P his account would have to be closed and he should move his money to another account they'd opened for him as soon as possible, to avoid losing it.

Mr P says he checked the number he was called from, and it was the genuine HSBC fraud team number. And he was sent a text by the caller, which showed as coming from HSBC. So he believed the call was genuine. He then transferred £8,000 out of his account, to the new account details the caller gave him. Unfortunately, we now know the caller was a scammer.

HSBC is a signatory of the Lending Standards Board Contingent Reimbursement Model (the CRM code) which requires firms to reimburse customers who have been the victims of authorised push payment scams like this, except in limited circumstances. HSBC investigated Mr P's case but said one or more of the exceptions applies. It said Mr P had ignored an effective warning and had made the transfer without a reasonable basis for believing it was legitimate, so he wasn't entitled to a full refund under the CRM code. Mr P wasn't satisfied with HSBC's response, so brought a complaint to our service.

One of our investigators looked at Mr P's complaint. They didn't think HSBC had established that Mr P had ignored an effective warning, or made the transfer without a reasonable basis for believing it was legitimate. So they felt Mr P was entitled to a full refund under the CRM code. 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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

In broad terms, the starting position at 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 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've considered whether HSBC should have reimbursed Mr P under the provisions of the CRM code and whether it ought to have done more to protect him from the possibility of financial harm from fraud. The CRM code places a level of care on Mr P too, so I've considered whether he met this.

The CRM code

As I mentioned above, HSBC is a signatory to the CRM code. The CRM code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances. And it is for the firm to establish that a customer failed to meet their requisite level of care under one of the listed exceptions set out in the CRM code.

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 Mr P ignore an effective warning?

The CRM code sets out 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. As a minimum, the CRM code sets out that an effective warning should be understandable, clear, impactful, timely and specific.

HSBC has sent us a copy of the warning message Mr P would have seen before making the transfer, and it says:

"Take care when sending money

Fraudsters can pretend to be from places you trust, like your bank, the police or HMRC. They can call from a number that appears valid when checked. If they ask you to move your account or repay an overpayment, it could be a scam.

If you're not sure, hang up and call the contact number on your card or an official phone number. We may not be able to recover payments that turn out to be fraudulent."

While the warning message does say fraudsters can pretend to be from places you trust and can call from a number that appears valid, it only talks about someone asking you *"to move your account"*. And I don't think this wording is specific enough about what the scam would look or sound like, to make it clear to Mr P that this was the type of scam he could be falling victim to. It doesn't mention the caller saying the account is at risk of fraud or the need to move money to a safe account, which are common features of this type of scam.

The warning message also relies on Mr P himself having doubts about the transfer by saying *"If you're not sure"* and only says that this *"could"* be a scam. And I don't think this wording was impactful enough about the likelihood that this was a scam, and stronger wording here could have made Mr P question the situation more thoroughly.

So I don't think this warning was specific or impactful enough to be effective in Mr P's circumstances. And so I don't think Mr P ignored an effective warning in relation to this transfer.

Did Mr P have a reasonable basis for belief?

Mr P was called by someone claiming to be from HSBC. He says the caller knew his name, contact details, post code and date of birth, and went through security questions with him similar to those he'd expect from a genuine bank. Mr P also says he asked the caller to confirm who they were and they told him to check the number the call showed as from on his phone – which was a genuine HSBC number. So, given the information the caller had, the professional nature of the call and that I've not seen anything to suggest Mr P was previously aware that scammers could spoof phone numbers in this way, I think it's reasonable that he thought the call was legitimate.

The warning message Mr P saw before making the payment did mention that fraudsters can call from a number that appears valid when checked. But after seeing the warning message, Mr P asked the caller to verify themselves and was then sent a text message that appeared to be from HSBC. Mr P says this text further convinced him the call was genuine and, as the warning message doesn't mention spoofed text messages as a possibility, I don't think this was unreasonable. Mr P was also shown a separate warning that the details he'd entered didn't match those on the account the money was going to. But he asked the caller about this as well and was told this was because the account wasn't set up yet – which I don't think it was unreasonable for him to believe, particularly given the previously convincing nature of the call.

Mr P therefore read and understood the warnings, tried to take further action to check the call was genuine and received additional verification and explanations. And he says the caller told him he would lose all his money if he didn't move it, and so was putting pressure on him to follow their instructions quickly. So I don't think it would be reasonable to say Mr P lacked a reasonable basis for belief because he navigated past the warning messages and I still think it's reasonable he thought the call was legitimate.

And so I think Mr P did have a reasonable basis for belief that the caller was legitimate and that the payment he was making was genuine.

Should HSBC have done more to protect Mr P?

In addition to its responsibilities under the CRM code, when Mr P made this payment, HSBC should fairly and reasonably 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).

The payment Mr P made was for a large amount, was for a significantly larger amount than any other payment made out of his account in the previous twelve months, and was to a new payee he'd never sent money to before. So I think HSBC should have identified that he could be at risk of fraud and so carried out further checks before processing the payment.

Due to the amount of the payment, I think it's reasonable to expect these checks to include questions about the purpose of the payment. And I've not seen anything to suggest Mr P had been given a cover story or told to lie about the payment. So, if asked, I think he would have said that he thought he was already speaking to HSBC and had been told he needed to move his money as fraud had been attempted on his account. HSBC should then have identified that Mr P was likely the victim of a scam and explained this to him, which I think would have uncovered the scam and stopped Mr P sending the payment.

So if HSBC had carried out further checks before processing the payment, as I think it should have done, the scam would have been uncovered and Mr P wouldn't have lost the money. And as Mr P has now been without that money for a period of time, I think HSBC should pay him compensatory interest at the rate of 8% simple a year, from the date of the transfer until the date it is refunded.

My final decision

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

- Refund Mr P the £8,000 he lost as a result of the scam
- Pay 8% simple interest on this refund from the date of the payment until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 24 June 2022.
Alan Millward
Ombudsman