DRN-3603177

The complaint

Mr R and Mr T complain that HSBC UK Bank Plc won't refund money Mr T was tricked into sending to a fraudster.

What happened

Though Mr R and Mr T are now joint account holders, I understand the account was only held by Mr T at the time and he was the only one that interacted with the fraudsters. So, I've referred to Mr T throughout. In July 2021, Mr T received a text message which appeared to come from the postal service. It asked him to arrange a payment for a delivery. Mr T happened to be expecting a delivery from overseas and knew that a fee would be required to receive it. He followed the link and entered his debit card details to make a payment.

Mr T believes that by following the link in the text message, software was installed on his mobile phone that allowed someone to access information on it.

Later that day he received a phone call from a number with a Scottish area code. The caller claimed to represent HSBC's fraud department and suggested that someone had been trying to make payments using his card details. The caller asked whether he had responded to any suspicious messages and, when Mr T confirmed he had, the caller suggested this was the reason for the fraud.

The caller appears to have gone into some considerable detail about the nature of the supposed fraud. They claimed someone had been into Mr T's local branch with a passport and a driving licence issued in another country, but suspicions had been raised because the person did not match Mr T's description. Mr T says he had recently lost his driving licence, which made what he was being told all the more convincing.

Mr T is convinced that the caller had access to his account. He says they were able to precisely confirm the last transaction he made, including the location and the amount. It was even claimed that he hadn't received notifications of any attempted activity because these had been diverted to a different number. Mr T says this resonated with him as it was something he'd recently heard about.

The fraudsters were able to convince Mr T that bank staff might be involved in the fraud from his account and that they required his help in order to catch the perpetrators. In order to do this, it was claimed, a dummy transfer would need to be made from his account. Mr T recalls a message saying the account details he'd input couldn't be matched, but was told that this was normal as the account he was paying didn't actually exist.

At this point, Mr T made a payment of £9,950 to an account at another bank. The payment was stopped by HSBC's fraud team and Mr T had a conversation with the bank. During that call Mr T claimed that he was paying his own account at another bank. He denied being asked to make the payment or having received a call instructing him to do so. HSBC questioned him about moving the entire balance and asked whether he'd have enough money to cover his expenses. He confirmed that he did and that the transaction was genuine.

Following this conversation, the payment was released. Mr T says the fraudster then offered to temporarily credit his account with a loan so that he wouldn't be charged for going into an overdraft. An HSBC loan of £12,500 was applied for and credited to his account. Mr T cites this as further evidence that the fraudster had control of his accounts.

The fraudster said they'd call back the following day with an update and that his accounts were now secure. Mr T didn't wait for the call back. He said that he started to become suspicious because, despite it being quite late at night when the call finished, he was told that his case was being actively worked.

He reported the scam to HSBC the following morning. The fraudster continued to call back, this time from a number associated with HSBC. When Mr T informed the fraudsters that he'd spoken to the real bank, they hung up and he didn't hear from them again.

HSBC were able to recover £4,468 from the bank which received his money. It also paid Mr T £200 in compensation for the way that it handled his claim. However, it refused to reimburse the remaining loss.

HSBC is a signatory of the Lending Standards Board Contingent Reimbursement Model "CRM Code" which requires firms to reimburse customers in all but a limited number of circumstances. In this case, it says that two such exceptions apply – that Mr T ignored an 'Effective Warning' and that he lacked a reasonable basis for belief in making the payment. One of our investigators upheld Mr T's complaint. They thought Mr T had acted reasonably when making the payment and that HSBC hadn't done enough to warn him.

HSBC disagreed. In summary, it said:

- Mr T did nothing to check the validity of the caller and though the text might have been expected, the call wasn't.
- It questioned Mr T's account of events in relation to the loan – arguing that in order for the fraudsters to apply for a loan, they would have had to have been given his online banking details
- He should have found the fact the caller knew his driving license was lost suspicious, given the bank would have had no way of knowing this.
- Mr T was given conflicting information about why his account was at risk – at first his debit card was being used, but later he was asked to catch fraudsters
- Mr T failed to check his account to see if there really had been any attempted transactions
- He failed to adequately question why the payment was going to a different bank
- During the security call, Mr T misled the bank and ignored some of the questions it asked. It also warned Mr T that he wouldn't get his money back if he proceeded with the payment and it turned out to be fraudulent
- It questioned what more it could have done to prevent the scam

As no agreement could be reached, the case was 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.

Did Mr T ignore an Effective Warning?

It's common ground that when Mr T made the payment, he did not choose the most relevant payment reason (Unexpected Request from Bank / Police / Organisation), but rather 'Paying Friends and Family'.

The warning that Mr T did see was not particularly relevant to his circumstances and Mr T can't be said to have ignored a warning he did not see.

HSBC also provided a warning to Mr T during the phone call before the payment was released. The Code requires that as a minimum an Effective Warning should be understandable, clear, impactful, timely and specific.

It's agreed that Mr T misled the bank during the call. This clearly made it harder for the bank to give an Effective Warning, but it did not prevent it from doing so. It, I think, had identified what the primary risk was here – that Mr T might be falling victim to a safe account scam. Mr T was moving the entire contents of his account and this clearly caused some suspicion.

Mr T was asked whether he had been instructed to move the money and, more specifically, whether he had received a call from the bank's fraud department. What the adviser failed to do is describe exactly what the risk was and what that might look like to Mr T. The adviser does not mention that fraudsters call customers impersonating the bank and may ask them to mislead the bank during security checks. And, if this happens, it's a scam.

So, while the adviser does explain the consequences of going ahead with the payment and the warning is somewhat tailored to the risk, it lacks sufficient impact to be Effective under the CRM Code.

Did Mr T make the payment without a reasonable basis for belief?

Mr T strongly believes that the fraudsters had access to his device which allowed them to obtain personal information about him and, later on, apply for the loan which credited his account.

It's difficult for me to establish conclusively whether this is the case or not and no evidence has been provided by Mr T to support this. I'm also conscious that fraudsters can be very good at giving the impression of having prior knowledge of a victim through social engineering and that some of what Mr T has said could be explained in this way or by simple coincidence. On the other hand, the loan application could have only been completed by someone with access to Mr T's online banking.

I have seen and heard Mr T's testimony – both to our service and to the bank and it has been detailed and consistent. He's adamant that certain pieces of information were known to the caller – particularly his balance and last genuine transaction. It's impossible for me to know how this could have been known to the caller and whether they were able to access Mr T's device, with or without his knowledge. Attempting to establish this has not been made any easier by HSBC's inability to provide electronic records to show the activity which took place across Mr T's mobile and internet banking. So, given how adamant and consistent Mr T has been about this and in the absence of that evidence I've concluded that it was more likely than not that this information was known to the caller.

It was unfortunate for Mr T, who says he's otherwise very conscious of scams, including those involving parcel fees, that he happened to be expecting a parcel when he received the scam text. Clearly the scam is designed cleverly, such that the phone call following Mr T's reply to the text is made to appear as if it is the bank's reaction to a breach of his security

information, rather than a continuation of the scam itself. I understand why Mr T, regretting his earlier mistake in responding to the text message would be keen to try and resolve any problem that had arisen from it.

As noted, some of what the caller told him, could have probably been deduced from relatively basic information about him (for example guessing his nationality) or simply made up (like the suggestion someone had been into his nearest branch) and yet the elaborate nature of the story and the small details that Mr T still recalls (such as the fraudster apparently having his driving license, which he'd lost) would, I'm sure, have given the story a significant air of authenticity. Mr T does not, I think, suggest that the caller knew that his licence had been lost, only that a license in his name had been used by someone impersonating him. Neither do I think it relevant whether Mr T checked his account – he'd only been told that transactions had been attempted, not completed.

Mr T clearly was convinced – he was prepared to mislead HSBC when it spoke to him about the payment. It's apparent that he genuinely believed that his accounts were at risk and he has described being overwhelmed with information, stressed, scared and worried about losing his savings. I think this had a part to play in his decision making and perhaps, in part, explains why he didn't question the fact that the fraudster claimed his account was subject to fraud before, and in a way which could not reasonably have resulted from, the text he received.

Many of what, retrospectively, were clear red flags were explained away by the fraudster – it didn't matter what payment reason he chose because it wasn't a 'real' payment he was making, neither did it matter that the destination was another bank or that there was no confirmation that the receiving account was in his own name – the payment wasn't really going to go anywhere.

Turning again to the call Mr T had with the advisor, I've thought about whether it should have shaken Mr T from his belief that he had been speaking to the actual bank. As noted above, I don't think the advisor went far enough to address the risk and the effect of that was not only to render the warning they were trying to give ineffective but it also meant the warning didn't have a significant impact on his belief. In addition, the call was expected by the fraudsters and they prepped Mr T to expect certain questions and for him to give certain answers, so what happened during the call wasn't entirely unexpected.

Overall, while I accept this is quite a finely balanced matter and that there are questions such as how the loan was applied for and why those funds weren't utilised that remain unanswered, HSBC haven't shown that Mr T ignored an Effective Warning or lacked a reasonable basis for believing that the recipient of the payment was legitimate. So, I'm instructing HSBC to refund Mr T's remaining loss.

I note HSBC's point that it doesn't feel it could have done anything more to prevent the scam, but that's not the test I'm applying, it's whether Mr T ignored an Effective Warning and whether he lacked a reasonable basis for belief.

Turning to the interest, though Mr T had a relatively high balance in his account at the time and has described the money as his savings, the transaction did consume all of his balance, which seems to include money he was using for everyday spending.

Taking that into account, the fact I'm not awarding interest on the money Mr T was deprived of between July and October 2021 (when a little under half the funds were returned) and in the interest of being pragmatic, I've decided that HSBC should pay 8% simple interest per annum on the outstanding loss from the date it declined his claim under the CRM Code to the date of settlement.

My final decision

I uphold this complaint and instruct HSBC UK Bank Plc to pay Mr R and Mr T:

- The amount lost minus the amount already recovered and returned - £5,482
- 8% simple interest per annum from the date it declined his claim under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R and Mr T to accept or reject my decision before 18 August 2022.

Rich Drury
Ombudsman