DRN-3726182

The complaint

Mr H is unhappy HSBC UK Bank Plc won't refund the money he lost as the result of a scam.

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here. But briefly, both parties accept that Mr H was the victim of a safe account scam.

Mr H says on 6 December 2021, he received a call from scammers posing as HSBC who alerted him that there was unusual activity on his bank account. He says they explained that standing orders were being set up and 'pending' and therefore needed to be pushed through to a safe account.

Mr H says it is likely that during the 'security check' with the scammer, he disclosed information that allowed the scammer to access his online banking – as it was the scammer that made the payments rather than him. The scammer convinced Mr H that his other accounts may also be at risk and to transfer these to his HSBC account for onward movement.

In order to push through these payments, Mr H says he was asked to send funds to one of the named beneficiaries on his account – a friend of Mr H's - I will refer to as C. The plan was that C would send these funds back to HSBC and money placed into a new account for Mr H with HSBC. The scammer then called C and directed her through the payments. A total of £10,000 was sent to C and then C sent a total of £6,715 to the scammers before the rest was stopped by her own bank. C returned the remaining funds to Mr H – so Mr H's total loss is £6,715.

HSBC intervened when a further attempt for another £10,000 was made using the access Mr H had unwittingly given the scammer during the call.

Our investigator upheld the complaint in full. She didn't think HSBC had provided an effective warning or had established Mr H did not have a reasonable basis for belief. She also felt the activity was unusual and ought to have flagged with the bank.

HSBC did not agree this complaint should be considered under the CRM Code – as it felt C's bank was best placed to deal with the case because the money went directly to the scammer. In any event, in terms of the case being considered under the CRM Code, it didn't agree it should be upheld. It said:

- It can only be expected to give an effective warning where a scam risk has been identified and it does not accept that a scam risk had or should have been identified in this case because the money was going to Mr H's friend - a known payee.

- At the time of the call, the balance in Mr H's account was £226.22. It made no plausible sense that in order to protect his money within his HSBC account it should be necessary for Mr H to first transfer funds from an account held with another bank, into the account held with HSBC (which was apparently under threat) and then to another non-HSBC account held by a friend.

I issued my provisional decision on 10 February 2023 explaining why I was reaching a decision that differed in some respects to that of our investigator's opinion.

HSBC said, on a gesture of good will basis, it would accept my decision and refund Mr H in line with it. It added that whilst I rely on a November 2021 Lending Standards Board (LSB) paper as support that the Contingent Reimbursement Model Code' (the "CRM Code") applies, and that it applies so as to hold a paying bank liable in the circumstances of this complaint, the industry in its subsequent discussions with the LSB made clear that it does not concur with this approach. The clear industry view on multi-generational complaints such as this is that, subject to the merits, the payment service provider from which the funds were transferred to the scammer should bear responsibility.

Mr H also responded as follows:

He is disappointed to be offered a partial refund. He feels it is easier to review the evidence with hindsight and take the view he should have realised. Looking back, he can see all the red flags that he didn't question early enough. But in the heat of the moment when you are panicking and thinking someone is trying to hack your account and someone else is trying to help you, you do have that blinded trust to let them help. The scammer did what Mr H considered was a believable security check. The answers to those questions gave the scammer details to access his account - but Mr H feels the scammer was clever making it sound legitimate at the time. The main issue he has is that he doesn't consider HSBC have done anything to help this situation. It wasn't just a few pounds but tens of thousands which - in his 15-year history with the bank – he has never moved so much money - certainly not in such rapid transactions. He understands that a payment to a verified payee makes it more obscure. HSBC only blocked the third £10,000 transaction because he asked them to. They offered him little or no support and put all the responsibility on the beneficiary bank.

Mr H did say he will accept the refund suggested but asked me to really consider whether HSBC did everything they could to help protect and recover his funds.

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, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Did Mr H authorise the transactions?

The question of authorisation is a key one in a case of this kind. Because, although it's not in dispute that Mr H didn't set out to be scammed, under the Payment Services Regulations 2017 (PSRs), and general banking terms and conditions, he is presumed liable in the first instance if he authorised the transactions.

When Mr H first reported the scam to HSBC, he did tell the bank he had shared secure information with the fraudsters. He gave the fraudsters what they asked for under the guise of them facilitating the payments for him.

There's no suggestion of how else the fraudsters were able to obtain this unique set of data. Consequently, it's highly unlikely the payment was executed without Mr H sharing this information – albeit he was tricked into doing so.

By providing his secure account details to the scammer, Mr H provided apparent authority for the disputed transactions to be carried out. The two £5,000 payments were therefore authorised, even though Mr H was the victim of a scam.

Should the case be considered under the Contingent Reimbursement Model Code?

HSBC is signatory to the 'Lending Standards Board (LSB) Contingent Reimbursement Model Code' (the "CRM Code"). But it doesn't agree this case should be considered under the CRM Code. It thinks Mr H's friend's (C) bank is best placed to deal with the case because the money went directly to the scammer from C's account. However, I don't agree.

In my provisional decision I explained why I didn't agree with HSBC – with reference the LSB's 'call for input' findings in November 2021. In this document LSB made it clear that the investigation of multi-generation scams, such as this, should be captured within the scope of the CRM Code.

In its findings, LSB acknowledged that, while the CRM Code may not have been drafted with multigeneration scams in mind, firms should be attempting to investigate and include all parties within this process, ultimately with the aim of reimbursing the customer.

Specifically, with reference to multigeneration scams, the LSB said:

These scams, sometimes referred to as 'friends and family scams', typically involve a customer being duped into increasing the number of transactions and/or payees involved in the scam (for example, being convinced to transfer funds to a family member who in turn is asked to further forward them, onto the scammer's account). While the funds have been moved to a trusted third party, in that they are a friend or family member, the payment has left the control of the payee. This approach seeks to evade the detection and preventative measures of the Code […]

And it went on to say:

When assessing such cases under the Code, firms should take into account that:
A firm's assessment of the case should fully explore the circumstances of the scam which looks beyond where the scam originated to enable the firm to fully consider the individual customer's case……

…. Consideration should be given to the full circumstances of the scam and the point at which the funds moved out of the customer's control, i.e. because the funds were moved to a friend or family member does not, in our view, preclude it from being considered under the Code.

Whether the scam originates at a Code signatory or otherwise, when a customer of Code signatory reports the scam, we would expect signatory firms to be assessing the case under the Code. It is through the assessment of the claim that the firm will be able to establish the full circumstances of what has happened, which includes whether the customer reporting the scam has incurred any loss.

In response to my provisional decision, I have noted what HSBC has said about the industry view to LSB's findings and that it considers, subject to the merits, the bank where the funds were transferred should take responsibility.

But I don't agree with this view - which contradicts the approach set out by LSB. And specifically, when considering the merits of this particular case, I think it fair and reasonable for HSBC to take responsibility. The loss being considered here is Mr H's loss and Mr H was the primary victim of the scam – so I think this is the appropriate place for the case.

Being the party that has suffered a financial loss here, Mr H reported the matter to HSBC. Receiving its customer's report of the scam, and in its capacity as the victim's bank, HSBC then has the principal responsibility for investigating and responding to the scam report. I consider that HSBC is also then responsible under the CRM Code for both the reimbursement decision and for reimbursement of the victim.

Having consider HSBC's response to my provisional decision, I remain of the view, the loss here is Mr H's loss and therefore moving his money to a friend does not preclude it from being considered under the CRM Code. So, I have gone on to consider Mr H's case under the CRM Code.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams in all but a limited number of circumstances. Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that:

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 outlined in the CRM Code that do not apply to this case.

Did Mr H make the payments without a reasonable basis for belief?

I need to consider not just whether Mr H believed he was sending money to a safe account, but whether it was reasonable for him to do so. I've thought about the steps Mr H took to reassure himself about the legitimacy of the transaction and whether it was reasonable for him to proceed with the payments.

I have reconsidered everything in light of Mr H's further submissions. Specifically, I have considered Mr H's circumstances in which he received the call and taken into account the pressure he would likely have been under and lack of time to think clearly in the moment of a call like this.

I accept this is a finely balanced case, but overall, I still don't consider Mr H had a reasonable basis for believing the person he was transacting with was legitimate for the reasons I outlined in my provisional decision. In summary those reasons were:

- C – who I understand had previously worked for another bank and Mr H told us '*deals with things like fraud*' - questioned what Mr H was telling her. She said it was '*a bit weird'* and told Mr H she'd '*never heard of a bank doing this before'.*
- Mr H's HSBC account did not have much in at the time of the call. The premise on which the whole movement of money was based seems odd to me. Whilst I appreciate Mr H may have felt there was urgency to move the money out of his account, once with C it was technically safe again and there ought reasonably to have been time to reflect on the request being made.
- Even if it was reasonable to believe a representative from one bank would know this about the risk to his other bank account - it seems odd to move that money into an allegedly unsecure account before moving it on - rather than direct to C or direct to his new "safe" account.
- Mr H himself says he ought to have hung up and called back, that it was 'blind trust, felt weird and not right.

I accept that M H says he verified the number – which was either spoofed or very similar to HSBC's official number. I also accept that calls like this are designed to create pressure and disrupt the victim's thinking. But there was time to message C and C questioned Mr H about what the bank was asking him to do. C had some knowledge of fraud and I think the movement of money sounded odd. Once the money was with C it was safe and there was time to reflect and question the red flags.

Overall, I'm not satisfied that a reasonable person would've believed this was a genuine situation or would've proceeded without doing more investigation and checks to verify all the information they were given – which I think would've shown inconsistencies and issues in the information provided.

Did HSBC meet its standards under the CRM Code?

HSBC is right that the CRM Code does say a firm only needs to provide an effective warning, where it identifies a scam risk in the payment journey. It seems here HSBC did not provide a warning and doesn't consider it needed to because the payment was going to an existing beneficiary. It feels such payments to friends or family will be deemed as low risk. It says a very significant number of such payments will be genuine payment journeys and providing warnings in these circumstances would be operationally unworkable.

I do accept there is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. And those arrangements do need to accommodate that spending habits alter, unusual needs arise, and it will be impossible to prevent all fraud without a significant number of genuine payments being delayed considerably and inconveniently.

Again, I think this is a finely balanced case in terms of the point at which I think the bank ought reasonably to have identified a potential fraud risk.

As the investigator said – Mr H did not spend large sums on the account. Before the transactions in question he made two deposits for £10,000 a minute apart, followed by the first transfer of £5,000 four minutes later and almost immediately a second transfer of £5,000 is made. I accept that the first payment might be deemed low risk because it was a known beneficiary – but given the overall pattern and activity, I think there was enough going on here (taking into account it was a known beneficiary) that by the second £5,000 transfer, HSBC ought reasonably to have identified a potential scam risk and provided a warning.

I have noted Mr H's comments in response to my provisional decision but as I've said above, I do accept that Mr H had not made such large payments in and out of the account. But I need to balance this against the fact that to the bank, the payments in were from Mr H's own account elsewhere and the transfers out appeared genuinely authorised payments and to an existing payee. On the face of it, it seems to me that that there was no reason why the first payment wouldn't have seemed genuine, even with the proceeding £10,000 payments in. But by the second transfer of £5,000 out of his account, I think a pattern had emerged and by that point the overall activity ought reasonably to have been a concern.

HSBC should fairly and reasonably also 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). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or made 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. For the reasons already explained, I think it ought reasonably to have intervened on the second £5,000 transaction to C. Had it done so; I think the scam would have been uncovered.

Overall, as both parties ought to have done more here, I consider the fair outcome in this case would be for HSBC to reimburse 50% of the second payment. I am not asking HSBC to refund part of the first payment because I don't think it needed to do anymore under the CRM Code at this point.

I realise my decision will be a significant disappointment to Mr H as I am not upholding it in full. I sympathise with his circumstances and I am sorry he has fallen victim to a scam. But having considered all the evidence and arguments, I think this is the fair and reasonable outcome here.

Putting things right

For the reasons outlined above and within my provisional decision, I require HSBC UK Bank Ltd to:

- Refund 50% of the second £5,000 payment Mr H made from his HSBC account – a total of £2,500.

- Add interest on the above refund at the originating account rate from the date the payments left Mr H's account to the date of settlement. If the originating account was not interest-bearing then no interest should be paid. [1].

[1] If HSBC is legally required to deduct tax from the interest should send Mr H a tax deduction certificate so he can claim it back from HMRC if appropriate.

With the above in mind, it seems the £5,000 originated from Mr H's current account with another bank but may have been transferred into that account from a savings account. I think it's more likely than not that, if Mr H hadn't fallen victim to this scam, he would've left that money in the account it originated from.

My final decision

For the reasons above, I uphold this complaint in part and require HSBC UK Bank Plc to put things right for Mr H as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 23 March 2023.

Kathryn Milne
Ombudsman