DRN-5200332

The complaint

Mr A has complained about HSBC UK Bank Plc not refunding several payments he says he made and lost to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. In summary, Mr A fell victim to an investment scam after receiving an unsolicited telephone call. Mr A was asked to download screensharing software and between April and June 2021 he sent funds from his HSBC account to cryptocurrency exchanges (which I will refer to as "G", "B", "S" and "M"). From there Mr A sent funds to what he believed was a credible investment firm (that I will call "F"). However, Mr A was actually sending his funds to fraudsters. Most of the funds sent to F came from a consolidation loan Mr A was persuaded to take. Mr A subsequently uncovered the investment was a scam when the fraudsters wouldn't allow him to withdraw the funds without paying further monies.

The relevant transaction history from his HSBC account statements are as follows:

Transaction	Date	Type of Transaction	Amount
1	29 April 2021	Debit card payment to G	£250
2	4 May 2021	Debit card payment to B	£15 (not sent to the fraudsters)
	6 May 2021	Faster payment from B	£34.50
	10 May 2021	Faster payment from S	£245.25
3	11 May 2021	Debit card payment to S	£252.20
4	12 May 2021	Debit card payment to M	£110.04
5	14 May 2021	Faster payment to B	£7,500
6	20 May 2021	Debit card payment to B	£100 (not sent to the fraudsters)
7	2 June 2021	Debit card payment to B	£750

HSBC didn't reimburse Mr A's lost funds and so he referred his complaint to us. Our Investigator looked into things but didn't recommend the complaint be upheld. They weren't persuaded, on balance, that HSBC could have prevented Mr A from falling victim to the scam. As our Investigator couldn't resolve the matter informally, the case has been 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.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focused on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

I don't doubt Mr A has been the victim of a scam here – he has lost a large sum of money and has my sympathy for this. However, just because a scam has occurred, it does not mean Mr A is automatically entitled to recompense by HSBC. It would only be fair for me to tell HSBC to reimburse Mr A for his loss (or a proportion of it) if: I thought HSBC reasonably ought to have prevented all (or some of) the payments Mr A made, or HSBC hindered the recovery of the payments Mr A made – whilst ultimately being satisfied that such an outcome was fair and reasonable for me to reach.

I've thought carefully about whether HSBC treated Mr A fairly and reasonably in its dealings with him, when he made the payments and when he reported the scam, or whether it should have done more than it did. Having done so, I've decided to not uphold Mr A's complaint. I know this will come as a disappointment to Mr A and so I will explain below why I've reached the decision I have.

I have kept in mind that Mr A made the payments himself and the starting position is that HSBC should follow its customer's instructions. So, under the Payment Services Regulations 2017 (PSR 2017) he is presumed liable for the loss in the first instance. I appreciate that Mr A did not intend for his money to ultimately go to fraudsters – but he did authorise these payments to take place. However, there are some situations when a bank should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made.

Considering the 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 - HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- 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). This is particularly so given the increase in sophisticated fraud and scams in recent years, which payment service providers are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So, I've thought about whether the transactions should have highlighted to HSBC that Mr A might be at a heightened risk of financial harm due to fraud or a scam.

I have kept in mind the payments were to cryptocurrency providers, but that doesn't mean they should automatically be treated as suspicious, particularly when there are no other concerning factors about the payments. It's also important to note all of Mr A's payments were sent in 2021. Whilst cryptocurrency scams were on the rise at that time, HSBC didn't have as much awareness around cryptocurrency payments as now.

I do not think the values of payments 1 to 4 were remarkable enough to have caused HSBC any concern. Nor do I consider enough of a pattern formed here to suggest Mr A might be at a heightened risk of financial harm due to fraud or a scam. The payments were not made in quick succession and were spread out across a number of days. Mr A was also making payments to various platforms, meaning it wouldn't have appeared immediately obvious to HSBC that the payments were connected. So, I'm not persuaded HSBC reasonably ought to have been concerned about these payments.

Payment 5 was of a value far more significant than Mr A's normal account usage. Therefore, although HSBC's level of awareness towards payments to cryptocurrency exchanges was not the same as now, a scam warning should have been shown to Mr A. However, the scam warning given here would have been dependent upon the accuracy of the selected transfer reason.

As Mr A did not provide the accurate reason for the purpose of the payment, it denied HSBC the opportunity to display a more applicable warning. Had Mr A selected 'Making investments', rather than 'Buying Goods and Services', he would have been shown an investment scam warning. This warning would have stated fraudsters will offer what appears to be genuine investment opportunities with high returns. As Mr A was led to believe his investment would yield a 40% monthly return; this warning would also have highlighted some similarities to his own circumstances. The warning also recommended speaking with a trusted party not connected with the investment and conducting independent research as the funds may not be recoverable in the event of a scam. Considering the level of awareness HSBC would have had about cryptocurrency exchange payments in 2021, a warning such as this, which broadly covered the risks of an investment scam, would have been reasonable.

I've also considered whether the origin of the payment five funds, a loan Mr A was persuaded to take by the fraudsters, with the reason given of home improvements, should have caused HSBC additional concern. However, it is not unusual that a home improvement loan may shortly leave an account after being received. I'm also not persuaded that the selection reason of 'Buying goods and services', when transferring funds from a home improvement loan, should have indicated a heightened risk of financial harm. But for the fact Mr A had no intention of using the loan for home improvements, such a selection reason for such a loan would have seemed reasonable.

Similarly to the first four payments, I do not think payments 6 to 7 were remarkable enough to have caused HSBC any concern.

I've also checked the official organisations that publish warnings about merchants that operate in the UK and abroad, to check if there were any warnings about who Mr A paid that ought to have triggered HSBC's fraud prevention systems. I've searched the Investor Alerts Portal of the International Organization of Securities Commissions ("IOSCO"), the international body that brings together the world's securities regulators. And the FCA (as the UK regulator) also has its own warning list, which is in place to share alerts and insight about merchants that have been identified as potentially being fraudulent or at risk of scamming individuals. There were no such warnings about the merchants Mr A paid. So, this is another reason why I don't think the payments ought to have been automatically stopped or triggered any warnings by HSBC.

I've noted Mr A has referenced decisions that he believes are close to his circumstances. However, we consider each case on its own individual merits and although he believes the circumstances of these other complaints to be similar, there are key differences.

Therefore, due to the reasons I have outlined above, I am not persuaded HSBC ought to have done more and due to this couldn't have prevented Mr A's losses.

Recovery

The only method of recovery HSBC has for payments made by card is to request a chargeback. However, Mr A didn't make the debit card payments to the scammers directly, he paid separate cryptocurrency exchanges. The service provided by the cryptocurrency exchanges would have been to convert or facilitate conversion of Mr A's payments into cryptocurrency. The fact that the cryptocurrency was later transferred elsewhere – to the scammers – doesn't give rise to a valid chargeback claim against the merchants Mr A paid. As the cryptocurrency exchanges provided the requested service to Mr A any chargeback attempt would most likely fail.

In relation to the other payments Mr A made, it's important to note he didn't instruct HSBC to send the money directly to the scammers. Mr A completed transfers directly to his own account within the cryptocurrency exchange. The majority of these funds were then sent on to a wallet address provided by the scammers. HSBC would only ever have been able to attempt to recover the funds from the wallets where they were originally sent, which were still in Mr A's control. If these funds had not already been transferred to the scammers, they would be in Mr A's control to access as and when he chose. Therefore, I won't be asking HSBC to do anything further.

The Contingent Reimbursement Model Code

Although HSBC has signed up to the Contingent Reimbursement Model Code, the transfers Mr A made from his HSBC account aren't covered by the Code because he made the payments from his HSBC account to his other accounts and not to another person. I cannot fairly and reasonably say that HSBC should have to refund payments under the Code when it doesn't apply here.

So, in light of all of the above findings, there's no fair and reasonable basis under which I can ask HSBC UK Bank Plc to reimburse Mr A's loss.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 6 March 2025.

Lawrence Keath
Ombudsman