DRN-4875166

The complaint

Mr G complains HSBC UK Bank Plc (HSBC) won't refund the money he lost to a scam

What happened

Mr G came across an advert on social media for a merchant promoting a new cryptocurrency coin. He followed up with the merchant, who added him to their group on the social media platform. He also spoke to them on the platform's messaging service – and they showed him their website. Unfortunately, it appears the merchant was actually a scammer.

I understand Mr G was told he had an opportunity to invest in a new cryptocurrency, and had the opportunity to double his money once the coin went live for public investment/purchase. In May 2023, he sent £3,000 from his HSBC account to a – genuine – cryptocurrency wallet he held, then sent the funds on to the scammers. He thought this was to purchase the new coin. But when the merchant stopped replying to his messages, he realised he had been scammed.

Mr G complained to HSBC that it should have warned him about the scam risk when he made the payment. HSBC denied it was liable, as the funds were sent to his own wallet. The fraudulent loss didn't occur until he sent the funds on from there. Unhappy with this response, Mr G referred the matter to our service.

Our investigator upheld the complaint. They said HSBC should have issued a tailored warning about the risks of cryptocurrency scams when Mr G made the payment. They thought that would have made him realise it was a scam, so thought HSBC was liable for his loss. They didn't think Mr G was to blame for what happened.

HSBC has appealed the investigator's outcome. It says it didn't have cause to intervene as the funds were being sent to a legitimate merchant, and the payment was for a modest amount and didn't look unusual for Mr G. It also said it wouldn't have been able to issue a tailored warning in the way the investigator suggested.

As part of our two-stage process, the case was then passed to me to decide. I asked Mr G for records of his interactions with the scammers – and sent him instructions on how to recover messages from deleted accounts. He says he has tried but can't recover anything. He has been able to provide details of the website the scammers were using.

In May 2024, I then issued my provisional decision on this complaint explaining why I wasn't minded to uphold it. Briefly, that was because I thought HSBC ought to have issued a written warning tailored to the risks of cryptocurrency scams. But I didn't think it was likely this would have dissuaded Mr G from proceeding.

I asked both parties to provide any further comments or evidence before I made my final decision. HSBC didn't respond by the deadline I set. Mr G replied to say that if HSBC had completed further security checks, he would have considered his position further.

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, I've decided to uphold it. This is largely for the reasons given in my provisional decision, so most of the reasoning set out below matches that given in my provisional findings. But I've also responded to Mr G's specific comment in response.

Mr G made this payment due to being tricked by the scammers. Banks have a contractual duty to make payments in compliance with customers' instructions. But I think HSBC should fairly and reasonably have been on the look-out for the possibility of fraud or scams and have taken additional steps, or made additional checks, before processing payments in some circumstances – as in practice all banks, including HSBC, do.

There might be grounds to suspect a fraud risk when a payment is significantly unusual or uncharacteristic compared to the normal use of the account. And/or if the account activity fits a known pattern of fraud.

I've considered HSBC's points around why it doesn't think the payment presented a heightened risk. It is true that he had made similar sized payments before, and that he had also paid cryptocurrency merchants before – albeit for smaller amounts.

However, by May 2023, HSBC ought to have been aware of the risks of multi-stage scams involving cryptocurrency for some time. Many banks had taken steps to limit cryptocurrency transactions, or increase fiction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions.

Given this was a sizeable payment to a cryptocurrency merchant, I think HSBC therefore should have realised the payment presented a heightened risk. And I consider a proportionate response to the level of risk would have been to display a warning tailored to the risks of cryptocurrency scams.

It would be difficult for such a warning to cover off every permutation of cryptocurrency scams without significantly losing impact. But I think it should have addressed the key risks and features of the most common scams of this type. Such as the use of social media adverts; promotion by a celebrity; the use of remote access software; and there being a broker/trader acting on your behalf.

I acknowledge HSBC's comments about the logistics of providing such a warning. It seems to think this would have to be contained within a 'One Time Passcode' (OTP) message. That's not the case. We see firms providing warnings in different ways. Such as sending an email warning, or directing the consumer to the app to display a warning.

HSBC has confirmed it didn't issue a warning when Mr G made this payment. But this alone doesn't mean it would be fair to expect HSBC to refund Mr G's loss. I need to consider whether HSBC's failure likely affected his loss.

I've considered this point carefully. There were some features of this scam – such as the use of social media to promote it, and arguably the level of returns being offered – that might reasonably have been encompassed by a tailored warning. But overall, I'm not persuaded it's likely a tailored warning would have made Mr G realise he was being scammed and therefore prevented him from proceeding.

This is because the scam didn't meet some of the more common hallmarks. Rather than there being a broker investing on Mr G's behalf, he understood he was purchasing a new coin before it was more widely released. He has confirmed remote access software wasn't used, and there is no mention of celebrity promotion either.

I do also consider it relevant that I haven't seen records of the scammer's contact. While I understand why Mr G hasn't been able to provide this, the absence of this evidence makes it harder to understand whether/why a short, tailored warning about the common features of cryptocurrency scams would have struck him as relevant to what he was doing. I can't see what exactly he was told by the scammers or what the nature of their contact was like.

As Mr G has explained, there was a website at the time to support that a new coin was being sold. I've also found a similarly-named coin was released shortly after this occurred. I don't have enough information to confirm, but I think it's possible it was the launch of this genuine coin which the scammers were impersonating. Which may have made it harder for Mr G to identify whether this was a scam – as he may have found information online which appeared to support the scammer's claims.

I appreciate this will be disappointing to Mr G. But I'm not convinced a tailored written warning would have made him realise he was being scammed at the time. The scam didn't match some of the more common hallmarks. And I have very little by way of records to judge why a warning would have struck Mr G as relevant to what he was doing.

I'm conscious Mr G has said, in response to my provisional findings, that additional security measures would have made him consider his position further. It's unclear if he means additional security measures beyond those I have said should have been implemented (i.e. a tailored written warning) – or that he thinks such a warning *would* have successfully dissuaded him.

In any event, I'm satisfied a tailored written warning would have been a proportionate response, for the reasons I have set out above. It wasn't so unusual in amongst Mr G's general account use – including that he had made cryptocurrency-related transactions prior – that I think further intervention was warranted.

I've also set out above why I'm not persuaded such a warning would have successfully dissuaded Mr G. And his response to my provisional decision doesn't shed much further light on *why* he thinks it would have done. Given the particular features of the scam, and the lack of evidence to show what the scammers told Mr G at the time, I'm not satisfied it's *more likely than not* a tailored warning would have succeeded in uncovering the scam.

As the funds were lost to the scam after being transferred on from Mr G's own cryptocurrency wallet, HSBC couldn't have taken action to recover his funds after he reported the scam. Overall, I'm therefore not persuaded HSBC's failure caused or contributed to his loss. So I'm not persuaded it would be fair to direct HSBC to refund him.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 26 July 2024.

Rachel Loughlin
Ombudsman