DRN-5381721

The complaint

Mr M has complained that HSBC UK Bank Plc ("HSBC") failed to protect him from falling victim to an investment scam and hasn't refunded all of the money he lost.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mr M says that around April 2024 he received a call form an individual ("the scammer") who claimed they could help him recover the funds he'd lost in a previous cryptocurrency scam. He's explained that he was told by the scammer he had a recoverable portfolio worth around $1,500,000 and they sent Mr M a link to register for a supposed investment platform in which he could see his alleged assets. The scammer told Mr M they could help him to invest his current assets to help him make a profit, and in turn, recover the loss he'd previously experienced.

Mr M has explained that he was in contact with the scammer daily using a messaging app, which it appears built a level of trust. He says the conversations were focussed on investments, and the scammer also used this method of contact to request Mr M send further payments in order to make additional investments.

Mr M explains that the scammer gave him instructions to open various accounts with electronic money institutions (EMIs), banks and cryptocurrency platforms, and they persuaded him to install remote access software on his computer so they could guide him through the process.

To facilitate the scam Mr M made 21 payments from his HSBC account to his own accounts at other institutions, in order to buy cryptocurrency. From there, he transferred cryptocurrency to wallets directed by the scammer under the belief he was funding his investment. As he could see the payments reflected in his balance at the fraudulent investment platform, this persuaded him that the investments he was making were legitimate.

The payments Mr M made were as follows:

	Date	Amount	Method of payment	Refunded?	Refund Amount
1	17/07/2024	£1,900.00	Card payment	Yes – 75%	£1,425
2	25/07/2024	£2,100.00	Card payment	Yes – 75%	£1,575
3	29/07/2024	£7,000.00	Faster payment	Yes – 75%	£5,250
4	31/07/2024	£10.00	Faster payment	Yes – 75%	£7.50
5	01/08/2024	£11,000.00	Faster payment	Yes – 100%	£11,000
6	01/08/2024	£2,500.00	Faster payment	Yes – 75%	£1,875
7	01/08/2024	£2,495.00	Faster payment	No	-

8	01/08/2024	£2,490.00	Faster payment	No	-
9	01/08/2024	£2,485.00	Faster payment	No	-
10	02/08/2024	£1,000.00	Faster payment	No	-
11	02/08/2024	£4,000.00	Faster payment	Yes – 100%	£4,000
12	05/08/2024	£20.00	Faster payment	Yes – 75%	£15.00
13	05/08/2024	£3,800.00	Faster payment	No	-
14	14/08/2024	£300	Faster payment	Yes – 75%	£300
15	14/08/2024	£20	Faster payment	Yes – 75%	£20
16	09/09/2024	£2,500.00	Faster payment	Yes – 75%	£1,875
17	10/09/2024	£700.00	Faster payment	No	-
18	13/09/2024	£10.00	Faster payment	Yes – 75%	£7.50
19	24/09/2024	£2,500.00	Faster payment	No	-
20	24/09/2024	£1,700.00	Faster payment	Yes – 100%	£1,700
21	25/09/2024	£1,700.00	Faster payment	No	-
	Total	**£50,230**			**£29,050**

When he realised he'd been scammed Mr M made a complaint to HSBC, which it didn't uphold. It said it had shown Mr M warnings and contacted him to highlight its concerns for thirteen of the payments, but Mr M ignored HSBC's advice and chose to proceed with the payments. Mr M disputed HSBC's outcome and it re-reviewed the complaint and partially upheld it. It refunded 75% of ten of the payments, as it didn't intervene before they were made, but it made a deduction for the part Mr M played in allowing the scam to happen.

HSBC didn't refund eight of the payments as it said it intervened before they were made, either by giving Mr M an on-screen warning or speaking to him, and he chose to proceed regardless. HSBC also explained that payments five, eleven and 20 were reversed so they didn't cause a financial loss.

Mr M remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained she thought HSBC had intervened proportionately. She also didn't think it had acted unfairly by reducing Mr M's refund by 25% to reflect the part Mr M played in allowing the scam to take place.

As Mr M didn't accept the investigator's opinion, the case has been passed to me to make a 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 sorry to disappoint Mr M but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr M authorised these payments from leaving his account. It's accepted

by all parties that Mr M gave the instructions to HSBC and HSBC made the payments in line with those instructions, and in line with the terms and conditions of Mr M's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

Should HSBC have recognised that Mr M was at risk of financial harm?

HSBC had a duty to monitor the activity on Mr M's account for signs of fraud, and intervene where appropriate.

Payments one and two were relatively low in value, spread over a week apart, and made via card to another financial institution. These factors meant they didn't raise sufficient red flags to warrant intervention. There was no immediate indication that the payments were unusual or high-risk on their own so I don't think it was wrong for HSBC to allow them to be processed without intervening before doing so.

Payment three was notably different to the first two payments. It was for a higher amount than the previous two payments and was made via bank transfer using Open Banking. Whilst the fact that this was an Open Banking payment – meaning it was destined for Mr M's own account at an Electronic Money Institution (EMI) – could offer HSBC some reassurance, I've also kept in mind the other characteristics of to the payment.

The payment was made just a few days after payment two, and it was the second increase in value, both of which suggest an evolving fraud pattern. And given the heightened risk associated with multi-stage fraud involving EMIs, HSBC should've identified this as a potential indicator of a scam.

Payments four to eleven were all made to an identifiable cryptocurrency platform, and by mid-2024, HSBC ought to have been aware of the elevated fraud risks associated with cryptocurrency transactions.

Payment five was reversed and Mr M was refunded in full, so I haven't considered an applicable intervention.

Payment six, made on 1 August 2024 for £2,500, wasn't an extraordinarily high amount in isolation, so it was reasonable for HSBC to allow it to proceed without intervention. But when Mr M attempted to make a second payment on the same day for £2,495, this should've raised concerns for HSBC. At this point, HSBC ought to have recognised a potential scam risk and stepped in to issue a warning.

Turning to the remaining payments, I also consider that HSBC ought to have intervened when Mr M made payment 13 for £3,800. Given the value of this payment and the fact that it was identifiably going to a cryptocurrency platform, it should have raised a red flag. While there had already been multiple payments to cryptocurrency platforms in this series, I acknowledge that HSBC needed to balance its fraud prevention responsibilities with avoiding undue inconvenience to its customers. But by the time Mr M attempted payment 13, the pattern of transactions, combined with the increased value, tipped the balance in favour of intervention.

What kind of warning should HSBC have given to Mr M?

As these payments took place after the introduction of the Financial Conduct Authority's Consumer Duty, I'd have expected HSBC to go some way to preventing foreseeable harm for Mr M.

For payment three I'd have expected HSBC to ask Mr M a series of targeted questions to better understand the purpose of the payment. This would've allowed it to assess the scam risk more effectively and provide Mr M with a better automated warning - tailored to the specific scam risk – rather than a generic one. I'd have expected HSBC to provide this with a view to providing a more effective intervention, to help Mr M realise he was at risk of fraud.

This intervention shouldn't have been limited to a general scam warning but should have involved asking Mr M a series of targeted questions to establish the purpose of the payment before providing a tailored warning relevant to the specific fraud risk. As Mr M went on to make two further payments that same day, this escalating pattern of transactions should have triggered additional intervention by HSBC.

By the time Mr M attempted to make payment seven, HSBC should have gone beyond an on-screen warning and conducted a human intervention – asking Mr M to speak with a member of its staff. Given the rapid succession of payments to an identifiable cryptocurrency provider, and the cumulative value of payments on the same day, during this intervention HSBC should've asked Mr M probing and specific questions to assess their legitimacy and identify any potential scam indicators, before allowing it to proceed.

Finally, HSBC should've stepped in to question Mr M about the nature and purpose of payment 13, and provided a better automated scam warning, again in an attempt to help him recognise the risks involved before allowing the transaction to proceed. This warning should've taken the form of a tailored on-screen warning, narrowed down to the scam risk identified.

How did HSBC intervene?

HSBC didn't intervene for the first four payments. It accepted liability for those payments and refunded them to Mr M, minus a deduction for his negligence, which I'll consider in the next section.

Before HSBC released payments seven to nine (which all took place on the same day) it blocked then and spoke to Mr M by phone. I've listened to a recoding of that call and although I don't intend to transcribe it in full, I've included a summary of it below.

The call begins with HSBC clarifying that Mr M attempted to make a payment of £11,000, which was subsequently returned. There is further discussion about four additional payments made on the same day, with HSBC explaining that these transactions require further checks before they can be processed. HSBC highlights that the payments exhibit characteristics commonly associated with fraud and scams.

Mr M quickly tells HSBC that the funds are being transferred to his own account with a cryptocurrency platform and confidently explains that he has been doing "rather well" with his investments, so he is simply funding further purchases. HSBC then checks whether Mr M has been asked to transfer funds to a so-called "safe account," which Mr M denies. But HSBC continues to probe, asking why Mr M is transferring money to a cryptocurrency platform and where the funds will be sent from there.

As the conversation progresses, HSBC issues several warnings about the risks of cryptocurrency investments, explaining that it's unregulated and that many investment platforms aren't legitimate companies but rather exist "on paper" only. Despite this, Mr M

interjects multiple times, asserting, “I understand the risks involved,” and reassures HSBC that he is being cautious by not investing all his money into crypto. When asked whether he is able to speak to the investment platform directly over the phone, Mr M insists that he can communicate with them through the app.

Throughout the call, HSBC consistently raises concerns and provides multiple warnings about the risks associated with cryptocurrency investments. But Mr M maintains a confident and self-assured demeanour, giving the impression that he’s knowledgeable and in control of his decisions. Given the content of this call, I am satisfied that HSBC’s intervention was appropriate and sufficiently robust. Mr M either didn’t believe the warnings because he was under the influence of a scammer, or because he’d been instructed to mislead HSBC to ensure the payments were processed.

Either way, I think it was reasonable for HSBC to have been satisfied it had warned Mr M of the risks associated with the payments and I don’t hold it responsible for Mr M’s decision to proceed.

I’ve also listened to the call that took place on 5 August 2024, before payment thirteen was released. I’ve again provided a summary below.

The call begins with Mr M explaining that a payment he had made to pay his credit card balance had been stopped and that he had received a message instructing him to contact HSBC.

HSBC responds by explaining that, due to evolving fraud trends, some payments may be stopped while others are not. The representative clarifies that she needs to ask Mr M some questions about the payment. HSBC then provides a detailed explanation of how scammers often impersonate banks or the police, highlighting the sophistication of these scams, before asking Mr M whether he’s received such a call. Mr M confirms that he hasn’t and takes the opportunity to state that he’s fully aware of fraud processes, as he’s encountered them many times before.

HSBC checks whether this is the first payment to the recipient, which Mr M refers to as his digital bank account. HSBC then asks why Mr M initially sent a smaller payment of £20. Mr M explains that he opened this new account because he was dissatisfied with another provider, though he doesn’t directly answer why he made the £20 transaction. He adds that he plans to use the new account for household payments and direct debits.

HSBC proceeds to issue a warning about “safe account” scams, which Mr M confirms isn’t relevant to his situation. HSBC then asks whether he saw a fraud warning when making the payment, which Mr M confirms he did. He states that he makes so many payments that he is accustomed to these warnings. HSBC stresses the high level of fraud risk and advises him to be cautious. Mr M reiterates that the payment is to his own account and will later be forwarded to pay his credit card. When asked whether he has been instructed to make this payment, Mr M firmly responds, “Not at all, it’s me.” HSBC also queries why he chose this particular provider, and he explains that he wanted a digital account for when he travels.

HSBC then warns Mr M about scammers impersonating genuine websites, but he talks over the representative to mention that one of his other accounts has been closed. HSBC suggests that he contact the company he is paying to verify its authenticity, particularly given the large amount involved. The representative recommends that Mr M call the company immediately and offers to call him back in six minutes. However, Mr M insists that he has no concerns. He explains that, as it is a digital account, he cannot call them directly. HSBC reiterates the importance of verification, but also acknowledges that if Mr M insists, the payment will be processed. Mr M states that he can chat with his account provider, but

HSBC advises against using online chat, as scammers can create fake websites, and instead recommends a phone call. After further discussion, Mr M convinces HSBC that he's confident enough to proceed without verifying the recipient, and the payment is ultimately released.

Did HSBC do enough to protect Mr M from harm?

Having considered everything, in particular the calls I've outlined above, I've concluded that HSBC intervened proportionately at the points I would have expected it to, and in fact, it did so more frequently and more robustly than I'd have expected.

HSBC asked relevant questions and provided multiple tailored warnings about the risks of fraud and scams related to cryptocurrency, but Mr M actively chose to deceive HSBC by providing misleading reasons for his payments – for example by telling it he'd had a lot of success in trading cryptocurrency, and that he was simply transferring funds to pay off his credit card.

Mr M also dismissed the warnings HSBC gave him, maintaining a confident and reassuring attitude throughout both intervention calls. Given his responses and insistence on proceeding, it was reasonable for HSBC to allow the payments to be made after its thorough interventions.

Is Mr M responsible for any of his losses?

In considering whether HSBC acted appropriately, it's also fair for me to consider whether Mr M's actions – or inactions – contributed to his losses.

Having thought carefully about this, I've concluded that whilst I appreciate that Mr M was a victim of a sophisticated scam, there were several points where he could have taken more care to protect himself.

Mr M accepted a cold call inviting him to invest, which is a common feature of scams. Given that he'd previously been scammed, I believe he should've been more alert to the warning signs, particularly those associated with multi-stage cryptocurrency scams. I'm also not convinced that he carried out thorough research before making the payments to the alleged investment.

Most importantly, Mr M wasn't truthful with HSBC about the reasons for his payments, which prevented the HSBC from being able to step in effectively.

I've taken into account Mr M's personal circumstances, including his financial worries caused by the previous scam, and his difficult family situation, which may have made him more susceptible to the scam. Although I'm not aware that HSBC knew about these factors at the time, I think it was reasonable for HSBC to reduce the refund by 25%, rather than splitting responsibility equally, after it was made aware of Mr M's circumstances.

Recovery of the funds

As the first two payments were made using Mr M's debit card, the chargeback process is relevant here.

In simple terms a chargeback is a mechanism for a consumer, via their card provider, to reclaim money from a retailer's bank when something has gone wrong, provided the transaction meets the eligibility criteria. It's for the card provider to decide whether to raise a chargeback, and it only needs to do so if it has a reasonable prospect of success.

It's also relevant to note that raising a chargeback isn't a legal right, and it's for the debit or credit card provider to decide whether to make a chargeback request to the retailer's bank. The process for managing these claims is determined by a set of rules by the card payment networks and there are no guarantees the card provider will be able to recover the money through the chargeback process.

In order for HSBC to raise a successful chargeback it'd need to provide evidence that the merchant didn't provide the goods or services that Mr M paid for. So although I understand Mr M used his debit card to fund his cryptocurrency account and ultimately purchase cryptocurrency, which he sent on to the scammer, there's no evidence the merchant didn't fulfil its obligation to provide the cryptocurrency that Mr M paid for. So the dispute doesn't lie between Mr M and the merchant, but instead Mr M and the scammer. As there wasn't a reasonable prospect of a chargeback claim being successful, I don't think that was a route that HSBC ought to have pursued.

HSBC attempted recovery of the funds for the remaining payments as soon as Mr M made it aware of the scam.

I've seen evidence that it was advised by all of the recipient banks that the funds had been withdrawn and it was therefore unable to recover them. Whilst this is disappointing, I'm satisfied that HSBC contacted the recipient banks promptly once it was aware of the scam, so there's nothing more I'd have expected it to do.

I'm very sorry that Mr M has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't require HSBC to pay him any more money as it has already refunded more than I would've suggested.

My final decision

I don't uphold Mr M's complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 12 May 2025.

Sam Wade
Ombudsman