DRN-5608336

The complaint

Mr K complains that HSBC UK Bank Plc, won't refund the money he lost to an investment scam. Mr K is represented in this complaint, but I'll refer to him as it's his complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In or around August 2024, Mr K was contacted by X (the scammer), on a social networking service, about an investment.

He started to speak to X, who said she was a financial analyst and a business mentor, on a messaging app. X introduced Mr K to a broker called Company Z and Investment Platform P. Mr K could see realistic investment graphs and he thought they were official and legitimate. Also, he could see people making money from bitcoin.

Mr K says he researched cryptocurrency, Company Z and the investment platform and then started to invest. He explains that the P Platform showed him he was making a profit on a daily basis, which gave him further reassurance that the investment was legitimate. Also, each day he would speak to X and Company Z. Mr K started to build a relationship and trust with X, who said she was religious, and he was convinced she was genuine and helping him.

Mr K had accounts with HSBC, Bank B, Bank N and Firm R and he transferred funds from these accounts to his accounts with crypto exchanges and then onto the scammers' crypto account.

The scammers' tactics were:

- To show Mr K that he was making significant profits and that to make higher profits, he needed to pay them fees.
- For X to encourage him to invest and, when he doubted the investment and got frustrated and annoyed, to persuade him that it was legitimate and to pay more and more fees until he had given them all his money. Also, to persuade Mr K, X would explain the fees, withdrawal issues and how successful his investment had become. Also, when he struggled to pay the fees, she agreed to make fake contributions.

Mr K highlights that, under the spell of the scammers, he made the following payments between 13 August 2024 and 24 October 2024:

- £12,500 from Bank R – 13 to 23 August 2024
- £17,804 from HSBC – 16 August 2024 to 24 September 2024
- £18,550 from Bank N – 9 to 11 September 2024
- £36,400 from Bank B – 13 September 2024 to 24 October 2024

The following table illustrates the payments Mr K said he made from his HSBC account to crypto exchange Companies M, CB and CR and then onto the scammers:

Payment Number	Date	Payment Method	Beneficiary	Amount (£)
1	16/8/24	Faster payment	Mr K's account with Bank B	134.83
2	16/8/24	Debit card	Mr K's account with Company M	50.00
3	16/8/24	Debit card	Mr K's account with Company M	500.00
4	16/8/24	Debit card	Mr K's account with Company M	300.00
5	16/8/24	Debit card	Mr K's account with Company M	500.00
6	16/8/24	Debit card	Mr K's account with Company M	500.00
7	16/8/24	Debit card	Mr K's account with Company M	500.00
8	22/8/24	Debit card	Mr K's account with Company M	500.00
9	22/8/24	Debit card	Mr K's account with Company M	500.00
10	24/8/24	Debit card	Mr K's account with Company CB	1,000.00
11	24/8/24	Debit card	Mr K's account with Company CB	1,000.00
12	29/8/24	Debit card	Mr K's account with Company CB	1,000.00
13	29/8/24	Debit card	Mr K's account with Company CB	1,000.00
14	31/8/24	Debit card	Mr K's account with Company CB	(1,000.00)
15	16/9/24	Debit card	Mr K's account with Company CR	1,338.87
16	23/9/24	Debit card	Mr K's account with Company CR	308.97
17	24/9/24	Debit card	Mr K's account with Company CR	2,497.51
18	24/9/24	Debit card	Mr K's account with Company CR	2,482.06
19	24/9/24	Debit card	Mr K's account with Company CR	2,471.76
Total				17,084.00

Mr K realised he'd been scammed at the point he thought his investment was worth £785,000. He wanted to withdraw £100,000 but couldn't afford fees which had a deadline.

Mr K complained to all four banks.

In his complaint to HSBC, in which Mr K asked for a refund of his £17,084 loss and interest, he said:

- *'The payments were completely unusual and out of character, and had the relevant interventions been conducted, the scam would have been stopped and the loss prevented'.*
- *'HSBC did contact me within the app, but it was simply to state it was me making the payment. They also rang me – I was open and honest and held nothing back'.*

HSBC rejected Mr K's claim. Their response included the following:

- '*We did ask Mr K on 21 August and 1 and 5 September 2024 for the reason he was transferring his funds. He told us he was paying bills and friends and family when there were options to tell us he was making an investment or paying for cryptocurrency.*

- *Associated fraud and scam advice was provided onscreen before we referred him to our Fraud Centre for further guidance.*
- *Our Payment Detection Team also spoke with Mr K on 24 August 2024. Having listened to the call, I'm satisfied he was fully questioned about the purpose of the transfer and given associated scam advice. Mr K told my colleague he was sending the money to his own wallet that he'd opened himself and he had sole access to'.*

Mr K was dissatisfied with HSBC's response and brought his complaint to our service. However, upon listening to recordings of interventions from HSBC and Bank B our investigator didn't think HSBC should reasonably have been expected to prevent the scam.

As Mr K remains dissatisfied his complaint has been referred to me to look at.

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, although I'm very sorry to hear that Mr K has been the victim of this cruel investment scam and lost a significant amount of money, I'm not upholding this complaint. I'll explain why.

I should first say that:

- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on the balance of probabilities.
- Although HSBC is a signatory of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code which requires firms to reimburse customers who have been the victim of a scam in most circumstances, I'm satisfied this code doesn't apply to payments made by card and to where a customer transfer funds to another account in their name.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty is relevant here.

  PSR

  Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr K made the payments here, so they are considered authorised.

  However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

  So, I consider HSBC should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.

- Have systems in place to look 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 banks are generally more familiar with than the average customer.
- 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.

Consumer Duty

Also, from July 2023 HSBC had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, HSBC was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud

With the above PSR and Consumer Duty in mind I first considered whether:

<u>HSBC should've recognised Mr K was a risk of financial harm from fraud and put in place proportionate interventions?</u>

Mr K started to make payments to Company M, a known crypto exchange, on 16 August 2024. Although each payment was to a legitimate business and for a relatively low value Mr K made six payments to this new payee on one day and considering his payment history (which didn't include crypto payments), the velocity of payments, two transfers to his new account with Firm R totalling £5,500 and HSBC's knowledge of cryptocurrency fraud (involving multi-stage payments) in 2024, I would've expected them to have taken the following action:

A. Provide automated scam and fraud warnings on the initial payments.
B. Step in on the fifth payment to Company M for a fraud and scam agent to question Mr K about the payments and transfers.

As if a bank doesn't question payments that might be at risk then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, considering the circumstances, I believe it ought to have contacted Mr K on this day (16 August 2024) to check he wasn't at risk of falling victim to fraud.

However, I found that HSBC did take both actions A and B soon after. Five days later on 21 August 2024 (before Mr K made a seventh payment to Company M) and again on 1 September and 5 September 2024, they put in place automated scam warnings and gave Mr K information. And on 24 August 2024, after Mr R's seventh payment to Company M and when he started to send money to Company CB (another legitimate crypto exchange) they put in place a human intervention.

So, although later than I would've expected, I'm satisfied they did recognise a risk of financial harm from fraud and did put in place proportionate interventions.

I then considered:

<u>The effectiveness of HSBC's interventions and why they, together with interventions from other banks, didn't prevent Mr K's loss?</u>

Automated interventions

The 21 August 2024 payment went to Firm R (to send to the scammers) and the 1 and 5 September 2024 payments appear to have been sent to Firm M, but HSBC didn't give Mr K

automated warnings relevant to either crypto and / or investments scams. This is because Mr K said they were, respectively, to pay a bill and family / friends.

Nonetheless, the warnings beneath coloured exclamation marks and the words '*Stop and think*' and '*Self defence'* written in bold print did say:

- *'If someone has told you to mislead us about the reason for your payment and choose the wrong payment type, stop. This is a scam.*
- *Fraudsters may pretend to be a genuine business.*
- *Do you really know them. Fraudsters may use social media to build up a relationship with you.*
- *Self defence. Visit our fraud centre for further guidance on how to undertake the required checks before proceeding'.*

Although not as effective as they should've been, these warnings were still relevant to the scam and Mr K was asked to '*continue*' (accepting the risk of not being able to recover his money) or '*stop*'. Although, I was surprised the warnings didn't automatically include a warning about the heightened risk of crypto, I don't think it would be fair or reasonable to say the lack of effectiveness here was an error when Mr K selected an inaccurate reason.

Also, I noted that when Bank B put an automated intervention in place Mr K again said he was paying friends and family.

However, Bank N did put in a strong tailored automated intervention on 9 September 2024, when Mr K paid a crypto exchange. However, despite this being about crypto payments and bitcoin and being directly relevant to the scam Mr K still chose to proceed.

So, even if HSBC included crypto payment warnings, I think Mr K would've still continued to make the payments.

Human interventions

Although there isn't any evidence that coaching took place to reduce payments and counteract interventions and Mr K says he *'had no reason to lie or evade questions from the bank'*, I considered this to be a possibility:

- Due to Mr K's selection choices when HSBC put in place automated interventions.
- I found Mr K wasn't truthful to HSBC when he spoke to one of their fraud and scam agents. Also, the agents of Bank B.
- Mr K was having daily conversations with the scammers.
- I noted that in his dialogue with X, Mr K discussed the banks he was using and after the intervention call with Bank B concluded on 13 September 2024 he said to X:
    - '*What a nightmare. I feel like a criminal all the questions!'*

So, although I don't know if the scammers were coaching Mr K, when listening to HSBC's call recording and others, I considered whether the agent was alive to the risk of coaching.

An intervention shouldn't be an interrogation; it should be suitable questions designed to unearth a potential scam and establish if the customer is at risk of financial harm.

Mr K faced lots of probing questions from the HSBC fraud and scam agent. Although I think she should've asked more open questions and probed some of Mr K's answers, she gave information to educate Mr K on the heightened risk of crypto investments (due to lack of regulation and volatility), different types of scams and the rise in crypto investment scams. The latter included fake platforms and screens, scammers continuously pressurising for extortionate fees to release funds, victims not having any control of the account and unable to make withdrawals. And Mr K listened to this information that directly applied to the scam

and at the time of the call, the messages between him and the scammer show that he was anxious and frustrated at the continuous high fees, pressure and not being able to withdraw.

Despite this I found when the agent asked Mr K questions about the purpose, control, access, fees, gains and loss, he wasn't truthful. He said he was the only one with access and control, he was acting alone after a well-known male friend had given him advice and there were no third parties. Also, there was no pressure, no one asking for fees and he could make withdrawals.

Although in some areas the HSBC call (at week 2 of the 11-week scam period). could've been stronger, when considering it together the three human intervention calls that Bank B put in place on 12,13 and 17 September 2024 (at week 5 and 6 of the 11-week scam period), I found the education and warnings to have been consistently strong.

Mr K was informed:

- Scammers approach people on social media and the scams include fake brokers, fake platforms and trading accounts.
- Scammers show realistic graphics illustrating profits together with group chats or messages from people making profits.
- The profits will be too good to be true. Scammers pressurise victims to pay more and more money in extortionate fees to access high profits.
- Even when victims can't access fake profits, and they think it may be a scam, they often struggle to accept the reality and continue to pay more.
- Scammers tell and coach victims to move funds between accounts and to lie to their banks.
- Banks continue to see a rise of investment scams with crypto and bitcoin being higher than normal risk. These are volatile due to lack of regulation and therefore due diligence and checking with the FCA is important.

Overall, I found that the probing was strong and when Mr K was asked more open questions and probed further he still gave false and misleading answers. For example, when asked the following:

- Why was he investing in bitcoin? How was he introduced to it?
    - He consistently said it was a long-standing male friend who was making money from bitcoin through a crypto exchange company. And when probed further about his friend, how he knew him and how he communicated with him, he gave false answers.
- Was any third party advising or helping him? Did he have an investment company and broker acting on his behalf? Is he paying exorbitant fees? What research had he done?
    - He consistently said no, which also wasn't the case.
    - Also, he'd done his own research following his friend's advice.
- How does he communicate with a third party or investment company? How does he know the investment company? How does he make withdrawals? Is someone saying you can make loads of money? Who is advising you?
    - He again consistently said it was just him acting on his friend's recommendation.

Also, he was repeatedly told that for the bank to protect him they needed him to be honest and asked if anyone was telling him to lie or manipulating him. And that only a scammer would do so. However, he consistently said no to these questions.

Mr K was asked a number of other questions including why he was transferring funds between his accounts and whether he was gaining high returns in a short space of time.

Most, and perhaps all, of the above scam warnings applied to Mr K. He had been approached by social media, he thought he had a broker, he was surprised the profits were so large (commenting to X that '*When it's too good to be true it usually is'*), he was getting annoyed and frustrated with the extortionate fees and being asked to make more and more payments. At a number of stages, he thought he was being scammed but due to the spell X had over him and the amount of money he had invested had he ignored his own misgivings. Also, he appears to have had misgivings over the investment as he tells X *'Lots of people have told me that this company are scammers'.*

Yet when repeatedly asked questions about whether any of the above applied to what he was doing he said it didn't, and he consistently gave false answers saying he was acting alone after a well-known male friend had given him advice. Regarding the warnings about the high risk of losing all his money, Mr K again accepted the risks.

Regarding Mr K's above comments about how he felt about the Bank B call, which lasted thirty minutes and was a very strong call in terms of education, warnings and probing. I think the Bank B agent may have been suspicious that Mr K was being coached as he repeatedly asked him if anyone was asking him to lie and told him about the importance of giving honest answers to his questions. However, on all the calls Mr K was insistent that no one was telling him to lie, maintains this in his complaint, and it isn't illegal for customers to trade in crypto.

Having considered all the above, even if HSBC put in place earlier and further interventions, I think Mr K would've prevented them from uncovering or stopping the scam.

Finally, with regards to recovery, Mr K's funds were paid into a crypto wallet and then sent on to the scammer, so unfortunately there was no realistic opportunity for HSBC to recover the funds. Also, for payments made by card the chargeback rules don't cover scams.

I realise the outcome of this complaint will come as a great disappointment to Mr K and I'm very sorry he has lost a significant amount of money here. But, for the reasons I've explained, I won't be upholding this complaint and asking HSBC to make any refund.

My final decision

For the reasons mentioned above my final decision is that I'm not upholding this complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 20 October 2025.

Paul Douglas
Ombudsman