DRN-5816154

The complaint

Mrs D complains that HSBC UK Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

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.

Mrs D saw an advert on social media for an opportunity to make returns of up to 100% by investing in cryptocurrency. The advert was endorsed by a well-known celebrity. After expressing an interest, Mrs D was contacted by someone I'll refer to as "the scammer" who claimed to work for Company T. She didn't have any investment experience, but she searched for T on google and thought the website seemed professional.

The scammer told Mrs D to download AnyDesk remote access software and to open accounts on T's trading platform, and a cryptocurrency exchange I'll refer to as "B". The broker asked her to first purchase cryptocurrency through B and then load it onto an online wallet. Between 8 August 2023 and 29 August 2023, the scammer used AnyDesk to make seven debit card payments and one transfer from HSBC to B totalling £34,600. Mrs D took out loans for £7,000 and £10,000 to fund the investment, and during the investment period she received credits into the account for £212.04 and £4,000.

After the initial deposits, the scammer told Mrs D she'd need to pay an additional insurance fee of £10,000 and transferred £4,000 to her account to help fund the payment. She was then told her that her cryptocurrency account was frozen, and that she'd have to pay £3,500 to unblock it.

In September 2023, HSBC restricted the account and asked Mrs D to attend the branch to discuss the £4,000 payment into the account. In branch on 18 September 2023, Mrs D explained the money was from an investment payout and that she was being assisted by a broker who worked for T, who she'd found online. During a call on 19 September 2023, she said she wanted to send funds to her cryptocurrency account. And on 20 September 2023, she accepted she was being scammed.

She complained to HSBC with the assistance of a representative who said it should have contacted her sooner and had it done so it would have detected the scam because she found the investment on social media, she was guaranteed high returns, she was using AnyDesk, and she was communicating with a broker using WhatsApp.
But HSBC refused to refund any of the money. It said the transfer was to her own account, and it was unable to dispute the debit card payments because the service had been provided. It explained it blocked the account because it had received an APP scam allegation from the sending back regarding the £4,000 credit.

Mrs D wasn't satisfied and so she complained to this service with the assistance of her representative. They said she had previously invested small amounts through HSBC and the

account was normally used for savings, day to day spending, and paying off her credit card. They said the payments were large and unusual payments to a cryptocurrency exchange and Mrs D was receiving credits into the account before sending funds to a cryptocurrency merchant, which is typical of an investment scam. They said HSBC should have intervened on 17 August 2023 when Mrs D made the £7,000 payment.

Responding to the complaint, HSBC explained the transfers weren't covered under the Contingent Reimbursement Model ("CRM") Code because they were to an account in Mrs D's own name.

Having initially concluded that an earlier intervention wouldn't have made any difference because Mrs D had misled HSBC when it intervened on 28 August 2023, our investigator issued a second view, upholding the complaint. He explained that he thought HSBC should have intervened on 17 August 2023 because the £7,000 payment was unusual, out of character, and significantly higher than any of the previous transactions on account. Additionally, it was an international payment to a high-risk cryptocurrency merchant.

He explained that he thought HSBC would have uncovered the scam if it had questioned Mrs D about the purpose of the payment, whether there was a third party involved, what returns she'd been promised, whether the investment company was registered with the Financial Conduct Authority ("FCA"), whether she'd been given a trading account, whether she'd been asked to take out loans to fund the investment, whether she'd installed AnyDesk, whether she'd made any withdrawals, and whether she'd been coached to lie.

In reaching this conclusion, he noted that Mrs D hadn't yet taken out the loans and therefore there would have been less at stake. He explained that HSBC should have given Mrs D a meaningful scam warning and had it done so, it would've been clear that she was being scammed. So, he thought it should refund the money she'd lost from the third payment onwards.

He further explained that the settlement should be reduced by 50% for contributory negligence because Mrs D responded to an advert on social media, the returns were too good to be true, she used loans to fund the investment, there was no evidence that she'd done any due diligence, and she misled HSBC during the first intervention.

My provisional findings

I issued a provisional decision on 19 August 2025 in which I stated as follows:

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mrs D says she's fallen victim to, in all but a limited number of circumstances. HSBC has said the CRM code doesn't apply in this case because she paid an account in her own name, and I'm satisfied that's fair.

I'm also satisfied Mrs D 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Mrs D is presumed liable for the loss in the first instance. There's no dispute that this was a scam, but although Mrs D didn't intend her money to go to scammers, she did authorise the disputed payments. HSBC is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

I've thought about whether HSBC could have stopped the scam sooner than it did. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, HSBC ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened sooner. If there are unusual or suspicious payments on an account, I'd expect it to intervene with a view to protecting Mrs D from financial harm due to fraud.

I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mrs D normally ran her account, and I think they were. The first two payments were very low value, and so HSBC didn't need to intervene. But I agree with our investigator that it should have intervened on 17 August 2023, because Mrs D was sending £7,000 to a high-risk cryptocurrency merchant and this was unusual for the account.

I think a proportionate response would have been for HSBC to contact Mrs D to ask questions about the payment including why she was making the payments, whether there was a third party involved and if so how she'd met them, whether she'd downloaded remote access software, whether she'd been promised unrealistic returns, whether she'd made any withdrawals, whether she'd been coached to lie, whether she'd done any due diligence and whether she'd been advised to make an onwards payment from the cryptocurrency exchange.

If Mrs D answered these questions truthfully, the scam might have been detected, and I accept that when she attended the branch on 18 September 2023, she did disclose that the money was from an investment payout and that she was being assisted by a broker who worked for T, who she'd found online.

But she gave misleading responses when questioned on 28 August 2023, stating that she was sending the funds to family overseas and she was transferring it to her EMI account so she could transfer it into the correct currency. She also denied having been told to give a different payment purpose.

I accept she hadn't yet taken out the loans on 17 August 2023, and she wouldn't have been able to say she was sending funds to family overseas because she was sending funds to a cryptocurrency exchange. But the messages between Mrs D and the scammer show they were in regular contact, and the scammer told Mrs D what to say to HSBC on 28 August 2023. So, I think the scammer would have done the same if HSBC had contacted her on 17 August 2023.

I don't agree the fact Mrs D hadn't yet taken out loans means it's less likely that she wouldn't have followed the scammer's advice to mislead HSBC, and while she did disclose more information about the scam while she was in the branch, its significant she wouldn't have been able to seek advice from the scammer while she there, and she'd also started to have doubts about the investment at this point.
The account remained blocked and Mrs D contacted HSBC on 19 September 2023 because she still wanted to make payments to the scam, and on 20 September 2023 she called again and said she'd been scammed, yet she continued to send messages to the scammer.

Consequently, while I think HSBC should have intervened on 17 August 2023, I don't think Ms D would have disclosed key facts about the investment which would have enabled it to uncover the scam, and even though I would expect it to have given her a warning which was tailored to cryptocurrency investment scams, I don't think this would have been enough to stop the scam because she clearly trusted the broker to the extent that she followed his

advice to lie to HSBC on 28 August 2023, and she continued to communicate with them after she began to suspect that she was being scammed. So, I don't think HSBC missed an opportunity to prevent her loss.

Mrs D went on to make further payments to the cryptocurrency exchange, including two payments totalling £13,700 on 25 August 2023. Arguably, HSBC could have intervened again because of the value of the payments but, even if it did, I think the outcome would have been the same.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mrs D paid accounts in her own name and moved the funds onwards from there.

I've thought about whether HSBC could have done more to recover Mrs D's payments when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. HSBC) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mrs D).

Mrs D's own testimony supports that she used a cryptocurrency exchange to facilitate the transfers. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mrs D's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that HSBC's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mrs D to part with her funds. I haven't found any errors or delays to HSBC's investigation, so I don't think she is entitled to any compensation.

Developments

Mrs D's representative has made further comments, arguing that the pattern of spending against the backdrop of overdraft usage should have prompted more robust questioning about the source of funds and their ultimate destination.

They've commented that Mrs D was given a cover story on 28 August 2024 because she'd struggled to obtain loans and there were problems with the cryptocurrency exchange, so there was a sense of urgency which didn't exist on 17 August 2024. And the scammer didn't give her a detailed cover story for cryptocurrency-related transactions or advise on how to answer questions beyond a basic payment purpose, so she wouldn't have been able to mislead a trained fraud expert if HSBC had intervened on 17 August 2024.

They've argued that HSBC should have asked Mr D what returns she was expecting, how the investment worked, who the broker/company was, and whether they were regulated and, had it done so, she wouldn't have been able to credibly explain why she was using cryptocurrency. Alternatively, if she said she was investing in cryptocurrency, HSBC ought to

have asked what returns she was expecting, whether she'd made any withdrawals, where was the cryptocurrency going, and whether she'd checked the company was regulated.

The representative has suggested that, even if Mrs D had sought the scammer's advice on how to deal with HSBC's questions, she wouldn't have been able to justify the payment given the low quality of coaching and the inherently suspicious account activity.

In addition, they've stated that phone interventions are effective in identifying cover stories and Mrs D already had doubts on 17 August 2024, having expressed concerns about her ability to access her funds in messages to the scammer on 10 August 2024. So, if HSBC had provided a clear, tailored cryptocurrency warning, highlighting the key features of cryptocurrency investment scams, she would likely have disclosed the true nature of the payments.

They've further stated that Mrs D's willingness to provide an incorrect explanation doesn't mean she trusted the scammer to an extent that would have rendered an earlier intervention ineffective, arguing that providing a brief, basic explanation to a bank, isn't the same as fabricating an elaborate cover story. And that she didn't make any further payments after she realised she'd been scammed, so the fact she continued to communicate with the scammer after she discovered the scam doesn't mean she continued to believe they were legitimate.

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've considered the further comments made Mrs D's behalf, but I'm afraid the findings in my final decision will remain the same as the findings in my provisional decision.

Her representative has argued that there would have been no sense of urgency on 17 August 2024, and so if HSBC had intervened, she wouldn't have sought the scammer's advice. But they were in almost daily contact, with the scammer providing regular guidance and instructions. And I think there was a sense of urgency throughout (see for example messages dated 4 August 2024). So, I think it's likely she would have sought the scammer's advice in the face of questioning by HSBC.

The representative has further argued that if Mrs D had sought the scammer's advice on 17 August 2024, she wouldn't have been able to provide satisfactory responses because she was paying a cryptocurrency exchange. I accept there's no evidence that the scammer had previously provided a cover story in the event of a payment to a cryptocurrency exchange, but this is because HSBC didn't intervene when it should have done. And I've no reason to doubt the scammer would have simply told her not to mention that she was being assisted by a third party or that she'd downloaded AnyDesk (HSBC has confirmed it didn't detect the use of remote access software), and this would have prevented HSBC from detecting the scam.

In addition, the representative has said that the messages between Mrs D and the scammer show she'd had doubts as early as 10 August 2024 and so she'd have acted on a tailored cryptocurrency investment scam warning on 17 August 2024. I've carefully considered the relevant messages, and I note she was showing caution by questioning how she could withdraw her funds in case of an emergency, but I don't consider she was concerned that the investment might be a scam. However, by the time she attended the branch over a month later, her account had been restricted for fraud, and she was very stressed and asking the scammer if she'd been scammed, so she was in a completely different frame of mind.

I accept Mrs D didn't make any further payments to the scam after she realised she'd been scammed but I remain satisfied that she'd have followed the scammer's advice to lie to HSBC and to disregard any warnings it might have given on 17 August 2024.

I'm sorry to hear Mrs D has lost money and the effect this has had on her. But for the reasons I've explained, I don't think HSBC is to blame and so it doesn't need to do anything further to resolve this complaint.

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 Mrs D to accept or reject my decision before 12 October 2025.

Carolyn Bonnell
Ombudsman