

## **The complaint**

Mr D and Mrs Z complains that HSBC UK Bank Plc (HSBC) won't refund the money they lost when they fell victim to an investment scam.

## **What happened**

The details of this complaint are well known to both parties, so I won't repeat them all again here. Instead, I'll summarise the key points, and focus on giving reasons for my decision.

In early 2021, Mrs Z was looking to invest. She spoke to an individual on a chat room app who she believed to be the vice-president of a big investment firm based abroad. As the app is audio-based, she says she checked his voice against his other social media profiles and found that it matched.

The individual guided Mrs Z to start investing in cryptocurrency through a particular platform. The name and website changed several times, which Mrs Z was told was due to improvements and updates as the customer base increased. She started with smaller investments and, when these performed well, invested more to get better returns.

Mrs Z started sending money to the scam platform via her sole account with HSBC. We are considering a complaint about the payments made from that account separately. After a few months, she also started sending payments via the joint account she and Mr D held with HSBC.

In June 2021 and November 2021, she sent funds from the joint account to a cryptocurrency wallet she had set up – in order to purchase cryptocurrency to send on to the scam platform. Then in February 2022, she purchased cryptocurrency from a peer-to-peer market. She sent payments from the joint account to an individual seller, who then loaded the cryptocurrency she had purchased to her wallet. From there, she sent the funds on to the platform. In total, she sent around £320,000 from the joint account.

Unfortunately, although the investment firm was real, it seems the individual who claimed to be their vice president was a fraudster. Mr D and Mrs Z's funds weren't actually being invested. She had been able to make some withdrawals initially. But when she showed the investment platform to her son, he expressed concerns. That prompted her to attempt a significant withdrawal (for £250,000). She was asked for a 20% withdrawal fee and her account was frozen. This made her realise it was a scam.

Supported by a professional representative, Mr D and Mrs Z complained to HSBC. They said it should have done more to protect them – and if it had, the scam would have been uncovered. HSBC denied it had made an error and so didn't agree to refund Mr D and Mrs Z. They then referred their complaint to our service (via the professional representative).

Our investigator didn't uphold the complaint. He found HSBC had questioned Mr D and Mrs Z about the payments towards the end of the scam, and they gave false explanations about what they were for. And the sophisticated nature of the scam meant he wasn't persuaded they would have realised it was fraudulent if they had looked into the company

further – noting they also had significant investment experience. Overall, while he thought HSBC could have done more to protect Mr D and Mrs Z, he wasn't persuaded this was likely to have succeeded in uncovering the scam.

Mr D and Mrs Z has appealed the investigator's outcome. In summary, they say:

- The cover stories they gave were absurd and poorly thought out.
- Effective intervention would have uncovered the scam. HSBC should have invoked Banking Protocol, put controls in the account, or at least given them robust education about cryptocurrency scams. If it had, they would have spoken to their son – who would have advised he thought it was a scam, as he did when they spoke to him about the investment later on. They would have tried to make a withdrawal and would have realised they were being scammed when this didn't succeed.
- There was 'alarming' information online about the alleged trading platform.
- They wanted the ombudsman to consider the intervention calls from HSBC, as these show there were red flags that were missed.

### **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 not to uphold it. I'll explain why.

Although tricked by a scam, it's agreed Mr D and Mrs Z authorised the disputed payments. In line with the Payment Services Regulations 2017, HSBC has a duty to act on authorised payment instructions without undue delay. The starting position is that Mr D and Mrs Z are liable for these payments as they authorised them.

However, our service does expect banks to have systems in place to monitor for uncharacteristic transactions or other signs its customers are at risk from fraud (amongst other things). In some circumstances, when an identifiable fraud risk is present, it may be appropriate to take additional steps before processing a payment.

Our service's approach to this is well-established, as both HSBC and Mr D and Mrs Z's representative will be aware. And it has been formed by a range of factors, including:

- Firms' obligations regarding fraud risks as set out in Banking Conduct of Business Sourcebook (BCOBS). Such as BCOBS Rule 5.1.10A requiring firms allowing electronic payments (such as HSBC) to:

*“...consider the risk of fraud and put in place appropriate procedures and technical safeguards to ensure that such payments can be carried out in a safe and secure manner.”*

- And BCOBS Guidance 5.10.B, which goes on to explain:

*“Such procedures should include authentication procedures for the verification of the identity of the banking customer or the validity of the use of a particular payment instrument, proportionate to the risks involved”.*

- The recommendations from the Banking Standards Institution (BSI) code about how firms can recognise when its customers might be at risk from fraud, and how to protect them.
- The Banking Protocol, which is an initiative between banks and the police, to help banks identify common authorised push payment scams – specifically when its customer is making such a payment in branch. In some circumstances when the bank thinks its customer is falling victim to a scam, they can call the police.

Please note this isn't an exhaustive list of the factors which have helped form our approach. But the examples I've given are intended to offer some insight into when we think banks should have fraud concerns, and what it might be proportionate to do in response.

In line with our approach, I've considered Mr D and Mrs Z's account activity and their contact with HSBC during the scam – to see if HSBC did (or ought to have had) concerns. And, if so, whether it responded proportionately. If I find it failed in this regard, I'll go on to consider whether this had a material impact on Mr D and Mrs Z's loss.

In the run up to the scam payments, Mr D and Mrs Z were using their account to make high-value payments. But I do think there was a notable change in the operation of the account due to the scam. They sent funds to Mrs Z's cryptocurrency wallet, for sums ranging from £10,000 to £25,000, on consecutive days. That level of spending looked unusual for them. Yet they weren't questioned about any of these payments – or about the two further payments they made to the cryptocurrency wallet in November 2021.

Given the change in account activity, I do think HSBC should have completed further checks on some of these payments – such as speaking to Mr D or Mrs Z to find out more about the circumstances in which they were being made. However, I'm not persuaded appropriate intervention was likely to have uncovered the scam.

That's because of what we know about how Mr D and Mrs Z responded when asked later about the scam payments made from this account in February 2022 – as well as how Mrs Z responded when questioned in relation to payments made from her sole account.

In February 2022, having not made any more scam payments since November 2021, Mr D and Mrs Z started making payments to an individual. They have explained they were buying cryptocurrency from him via a peer-to-peer market. The cryptocurrency they bought was loaded to Mrs Z's wallet then sent on to the scam.

Some of these payments were blocked for fraud checks. I've listened to the calls between Mr D and Mrs Z and the bank about these payments. One was made from branch – seemingly due to concerns over the language barrier when speaking to HSBC on the phone.

When Mr D and Mrs Z were asked what the payments were for, they said they were for an investment by Mr D. They said no one had told them how to answer the bank's questions, or to mislead it. HSBC explained if they had, that would be a strong indication they were being scammed.

Mrs Z also told HSBC they had known the individual they were saying for a few months and had been doing business with him for some time, having been introduced to him by a friend. When asked about the level of returns the individual was offering, Mrs Z said the returns were reasonable and weren't too high. HSBC advised them on how to check the investment, such as checking reviews and getting advice. Mrs Z said she had done that and was satisfied.

I think the nature of Mr D and Mrs Z's customer relationship is relevant here. They held substantial investments with HSBC, were high-net-worth customers, and were in the UK on the basis of a visa requiring them to make substantial investments. In that context, I would consider it reasonable for HSBC to rely on their insistence they were satisfied with the investment. I don't think it had cause to refuse the payments or invoke Banking Protocol.

It's also clear there are aspects of what Mr D and Mrs Z told HSBC that weren't true. There is no record of them dealing with the individual prior to February 2022, despite their assertion they had known him a few months and had been introduced by a friend. We've also seen contact records between Mrs Z and the scammers showing they coached her on what to tell the bank about the payments – as HSBC warned her was a likely scam indicator. Yet they persisted in giving cover stories for the payments.

Mr D and Mrs Z also didn't make it clear the investment related to cryptocurrency, instead referring to stock market investments. Nor would the link have been apparent to the bank at the time, given the payments were going to an individual account. Please note the payments are not covered by the Lending Standards Board's Contingent Reimbursement Model (CRM) code, as they were genuine purchases; the fraudulent loss only occurred when the funds were sent on from Mrs Z's cryptocurrency wallet. The earlier payments also aren't covered as the code doesn't cover me-to-me payments.

When questioned in relation to scam payments from her sole account (which is being considered as a separate case but has relevance to my judgment here over whether better/earlier intervention would have succeeded), Mrs Z also gave various cover stories about what the payments were for. Such as claiming payments were for furniture.

Overall, I'm not persuaded HSBC can fairly be held at fault for not preventing the scam. It seems Mr D and Mrs Z were adamant about making these payment – and were unwilling to disclose the true nature of what they were doing. So I'm not persuaded they would have responded in a way that made it obvious they were falling victim to a scam in response to earlier, or more thorough, questioning.

I appreciate that, had HSBC intervened earlier, it may have been more obvious that the payments Mr D and Mrs Z were making were linked to cryptocurrency. However, I still don't think it's likely they would have revealed the full extent of what they were doing such that it would have been obvious they were being scammed. And I don't think it's likely they would have been dissuaded from proceeding in response to warnings about the nature of cryptocurrency scams.

The scam didn't meet some of the more common features, such as use of remote access software. While Mrs Z came across the opportunity via social media, she has told us she took further steps to corroborate the individual – such as comparing with other social media profiles dating back over eight years. So I don't think she would have been concerned by a warning about scammers using social media to contact victims – bearing in mind the lengths she had gone to in order to verify who she was dealing with.

Mr D and Mrs Z's representative has provided links to a website identifying concerns with some of the platform names used by the scammers. It suggests they would have found these if prompted to do further research into the company. But Mrs Z was advised over the phone about how to look into the company and she confirmed she was happy they were legitimate. In any event, my research suggests these websites weren't easily findable when searching for the platform name(s) at the time.

There has also been a suggestion that, if concerns had been raised, Mr D and Mrs Z would have tried to make a withdrawal – and this would have uncovered the scam. But Mrs Z has also told us she was able to make some direct withdrawals from the scam platform(s). Her cryptocurrency wallet activity suggests the withdrawals came to a significant amount. So I'm not persuaded by this argument – as it appears she was able to make withdrawals initially.

Furthermore, this suggestion appears to be based on the large withdrawal Mrs Z tried to make after her son raised concerns, which set her on the path to discovering the scam. But the key difference here is that Mrs Z and Mr D showed their son the trading platform they were using. Whereas they weren't being upfront with HSBC about what they were doing – meaning HSBC wasn't able to properly assess, and warn them of, the risks.

While Mr D and Mrs Z's representative has pointed out the trading platforms weren't regulated, as it will know, that isn't a requirement for cryptocurrency. So that in itself was unlikely to have caused them, or HSBC, concern.

The funds paid were sent on to the scam via Mrs Z's cryptocurrency wallet(s). Given the payment steps involved, HSBC couldn't have recovered the funds once the scam was reported as they had already been moved on.

Overall, I'm mindful Mr D and Mrs Z have lost significant amounts to a very sophisticated scam. But in all the circumstances, I'm not persuaded it's fair to hold HSBC liable for their loss. Mr D and Mrs Z's determination to make the payments, investment experience and the explanations they gave for the payments mean I'm not convinced HSBC ought to have been able to uncover the scam and prevent their fraudulent losses.

### **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 D and Mrs Z to accept or reject my decision before 11 January 2024.

Rachel Loughlin  
**Ombudsman**