DRN-4555044

The complaint

Mrs Z complains that HSBC UK Bank Plc (HSBC) won't refund the money she lost when she 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 sent money from her sole HSBC account to cryptocurrency wallets she had set up, to purchase cryptocurrency to send on to the platform. She also purchased cryptocurrency from a peer-to-peer market. She sent payments to individual sellers who then loaded the cryptocurrency she had purchased to her wallet – then she sent it on to the platform.

The investigator who looked into this complaint has shared a list of the relevant transactions with both parties, and Mrs Z's representative has confirmed this to be correct. Accounting for some credits/bounced payments, her loss arising from the disputed payments made from this account is in the region of £1,160,000.

Unfortunately, although the investment firm was real, it seems the individual who claimed to be their vice president was a fraudster. 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, Mrs Z complained to HSBC. She said it should have done more to protect her – and if it had, the scam would have been uncovered. HSBC denied it had made an error and so didn't agree to refund Mrs Z. She then referred her complaint to our service (via the professional representative).

Our investigator didn't uphold the complaint. He noted HSBC had questioned Mrs Z on a number of occasions and she had given false explanations for the payments, making it harder for HSBC to understand the risk and warn Mrs Z appropriately. And he wasn't persuaded Mrs Z would have realised the platform was a scam if she had been prompted/warned to look into them further.

Mrs Z appealed the view. In summary, she said:

- The cover stories she gave were absurd and poorly thought out. She said she was buying goods such as kitchenware and furniture – then ultimately admitted she wasn't, but said the payments were linked to an investment by her husband.
- Effective intervention would have uncovered the scam. HSBC should have invoked Banking Protocol, put controls in the account, or at least given her robust education about cryptocurrency scams. If it had, she would have spoken to her son – who would have advised he thought it was a scam, as he did when she spoke to him about the investment. She would have tried to make a withdrawal and would have realised she was being scammed when this didn't succeed.
- There was 'alarming' information online about the alleged trading platform.

I issued my provisional decision in December 2023, explaining why I was minded to agree with the overall conclusions of the investigator. I invited both parties to submit any further comments or evidence in response, but neither provided any additional submissions by the deadline I set (although Ms Z replied to confirm she had received my provisional findings). So, I'm now proceeding to finalise my 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.

As I haven't received anything further in response to my provisional decision, I see no reason to depart from it. I've decided not to uphold this complaint. I've explained why below.

Although tricked by a scam, it's agreed Mrs Z authorised the payments she is disputing. 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 Mrs Z is liable for these payments as she 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 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 Mrs Z's account activity and her 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 her loss.

While Mrs Z did use the account for high-value payments, I do think there was a notable change in the operation of the account due to the scam. This is based on the pace, value and number of transactions Mrs Z started to make.

For example – at the beginning of the scam, Mrs Z mainly transferred funds to her account with a cryptocurrency exchange (C). The payments were generally £5,000 or more, and they became very regular – with multiple payments made within a day and/or on consecutive days.

It seems Mrs Z was asked about the first payment she made to C (£5,200 in March 2021). HSBC has a record of speaking to her in branch about this payment. Its notes show it was aware the payment was going to a cryptocurrency company. Mrs Z confirmed she was happy to proceed; was sure it wasn't a scam; and hadn't been convinced to make the payment.

I think that appears to have been a broadly proportionate response to the risk identified. I can see why HSBC didn't have stronger concerns at that point based on that payment alone. However, I don't think it was reasonable, based on that intervention, to allow the payments to continue unchecked for a further two months, bearing in mind the escalation that occurred after this first payment. During that time, over £250,000 was sent to the same account.

The next record I have of HSBC completing further checks relates to a £10,000 sent to C in June 2021. HSBC called Mrs Z and explained the payment had been flagged for a fraud check. It asked what it was for. Mrs Z said she was buying some items. She said she knew the company was okay as she had been dealing with them for a while. She confirmed no one was forcing her to make the payment.

Mrs Z wasn't being honest with HSBC about the reason for the payment – making it harder for HSBC to protect her. Regardless, I'm not persuaded HSBC did enough. The earlier payment had been linked to cryptocurrency, so I can't see why this one wasn't – especially as Mrs Z mentioned C's name. The response she gave that she was buying 'items' was also vague. Without understanding more about what she was doing, I don't think HSBC should have been satisfied she wasn't at risk from fraud. Yet it allowed her to continue making frequent, high value transfers to C throughout June 2021 without questioning her further.

I've therefore considered whether appropriate intervention by HSBC was likely to have uncovered the scam at this point. Having weighed this up carefully, I'm not persuaded it would have done.

I do consider it relevant that, when questioned, Mrs Z gave a cover story rather than disclosing what she was actually doing. Her exchanges with the scammer show they gave her advice on what to say. If probed further, I think she would likely have sought more advice from them on what to tell HSBC. And I think the scammers would have been able to guide her on what to say to avoid or minimise suspicion – such as insisting there was no third-party involvement and that she was acting alone. So I think it's unlikely that further probing would have made it obvious to HSBC that Mrs Z was falling victim to a scam.

I think Mrs Z's relationship with HSBC is relevant to this. It has explained she holds a substantial investor portfolio as well as an account specifically tailored for high-net-worth individuals. So if HSBC had discussed things further with Mrs Z, I don't think it would have seemed uncharacteristic or suspicious that she was investing such large amounts.

However, if a cryptocurrency link was established (which, as explained above, I'm minded to think should have been), then I think it would have been prudent for HSBC to have issued a tailored warning to Mrs Z about the common features of cryptocurrency scams. But I'm not persuaded doing so would have unveiled the scam.

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.

Mrs Z (via her representative) has provided links to a website identifying concerns with some of the platform names used by the scammers. She has suggested that, if she had been prompted to do further research, she would have come across these sites and would therefore have realised she was being scammed. But I'm not persuaded a warning to research who she was investing with would have prompted her to do further research – bearing in mind the research she had already done and the trust she had built with the scammers. Regardless, my research suggests these websites weren't easily findable when searching for the companies at the time.

Mrs Z says that, if concerns had been raised, she would have tried to make a withdrawal – and this would have uncovered the scam. But she 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.

While 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 Mrs Z, or HSBC, concern.

For these reasons, I'm not persuaded HSBC is at fault for not uncovering the scam at this point. But given the significant amounts Mrs Z continued to send, I've gone on to consider whether there were later opportunities to uncover things.

After June 2021, the scam payments stopped for a while. I've not been told why, although I appreciate it could simply be that Mrs Z (thought she) was trading using the money she had already sent. Then in mid-October 2021, she started to make a high volume of card payments to a different cryptocurrency merchant (B).

I don't think these looked particularly unusual compared to the previous spending a few months prior. But even if HSBC had intervened in response to the pace and value of the payments, I'm not persuaded it would have been any more likely to uncover the scam at this point – bearing in mind why I don't think it would have succeeded prior. As time went on, the scammers will have built up more trust with Mrs Z.

HSBC then spoke to Mrs Z about a bank transfer to a new recipient. While I understand this was a cryptocurrency purchase, that wouldn't have been apparent to HSBC, and Mrs Z didn't disclose this when it spoke to her. I think HSBC responded broadly proportionately here. The payment was for a lower amount than most other payments. And HSBC issued relevant warnings based on what it knew/was told about the payment.

The next intervention occurred in November 2021. HSBC spoke to Mrs Z twice about bank transfers to a particular individual. She has explained to us this individual wasn't a scammer; she was genuinely purchasing cryptocurrency from then through a peer-to-peer market. But the payments are connected in the sense she sent the cryptocurrency she bought (which was loaded to her cryptocurrency wallet) on to the scam platform.

Mrs Z told HSBC she was buying furniture/kitchen items from her friend. She confirmed she had already received these items; knew the friend well; had got the payment details from them directly; and the friend had received the previous payments she had made.

I'm conscious of the substantial amount Mrs Z sent this recipient. But based on what she told HSBC, I don't think it had reason to suspect these payments might be linked to a cryptocurrency scam. So I'm not persuaded this was a missed opportunity to uncover the scam.

There was then another gap between November 2021 and February 2022 where no further scam payments were made. Mrs Z then resumed making card payments to B. She also started making transfers to an account she set up with an authorised Electronic Money Institute (EMI). This account was linked to Mrs Z's account with B.

Again, by this stage, Mrs Z had an established history of making lots of high-value payments (including payments identifiably linked to cryptocurrency) from the account. So I don't think the payments looked uncharacteristic. However, HSBC did block the first substantial payment to the EMI account (£24,000) and directed Mrs Z to attend branch to discuss it.

From branch, Mrs Z spoke to HSBC's fraud team over the phone. She said the payment was for refurbishments and confirmed she wanted to proceed. This came very shortly after Mrs Z received significant proceeds from a house sale. I think that context added weight to the plausibility of her explanation.

Given the steps HSBC took to require Mrs Z to go to branch, it could have probed further here. But I'm not persuaded it had cause to refuse the payment or invoke Banking Protocol. I don't think further warnings or probing were likely to unveil the scam at that point, as I don't think the explanation gave seemed particularly worrying or implausible.

HSBC continued to speak to Mrs Z, including in branch (seemingly due to concerns over the language barrier when speaking to her on the phone), about the payments she continued to make to the EMI account. She continued to maintain she was refurbishing and buying furniture as part of an ongoing project.

HSBC did go as far as to question why she was sending the funds via an EMI which is used for currency exchange. But Mrs Z said this was because the company she was purchasing from was based abroad. HSBC pointed out she had sent a lot of payments to the account by this point and asked whether she had a "final bill". There was also discussion around what exactly she was buying. It came across that HSBC had concerns and didn't understand what Mrs Z was doing. She repeatedly maintained everything was fine and there were "no problems", although said she had difficulty understanding some of the questions due to the language barrier.

It seems this prompted HSBC to direct Mrs Z to go to branch again to discuss what she was doing. At that point, Mrs Z changed her story. She said she thought the payments were for antique furniture. But after speaking to her husband, she had found out they were actually for an investment. She said her husband had traded for many years and knew what he was doing.

HSBC asked Mrs Z if the money she had sent previously had arrived in her investment account. She confirmed it had. HSBC also asked Mrs Z whether anyone had told her to mislead the bank in any way, or had guided her on how to answer its questions. She confirmed that hadn't happened.

I do think this change in explanation for the payments looked suspicious, so arguably ought to have warranted more caution and questioning from HSBC. But, overall, I'm not persuaded it would be fair to conclude it ought to have uncovered the scam and prevented Mrs Z's further loss at this point. This is because:

- Mrs Z likely got advice from the scammers on what to tell HSBC. She was still not answering its questions honestly (such as about the nature of the investment and whether she had been told to give a false explanation). So I'm not persuaded HSBC would have able to get a full and honest explanation from Mrs Z about what she was doing, in order to accurately warn her of the risks.
- While Mrs Z says she didn't have much investment experience, I can't overlook the nature of her customer relationship she (and her husband, who she told HSBC was behind the investment) had with HSBC. She held substantial investments with HSBC, was a high-net-worth customer, and was in the UK on the basis of a visa requiring her to make substantial investments. In that context, I would consider it reasonable for HSBC to rely on Mrs Z's insistence she and her husband were satisfied with the investment.
- Mrs Z was very persistent in making these payments. She (and her husband) had sold a property in order to fund it. This shows the strength of her belief that the investment was real. And by the point of this intervention, the investment had been ongoing for almost a year. In that context, I find it difficult to conclude there is more HSBC ought to have done which would have prevented Mrs Z from proceeding – bearing in mind its primary duty to act on her authorised payment instructions.
- This is further supported by the conversations HSBC had with Mrs Z around this time about scam payments made from her joint account. Our service is looking into a separate complaint about this. But it is of relevance when assessing whether further intervention regarding payments made from her sole account would have succeeded.
- Mrs Z said the payments (which weren't clearly cryptocurrency-related) were for an investment. She said the individual the payments were being sent to was someone her husband had been introduced to via a friend; had spoken to on video chat; and who he had known for months. In reality, the payments were being sent to a peer-to-peer cryptocurrency seller who (so far as I'm aware) they didn't have prior links to.

- HSBC warned Mrs Z about fraudsters gaining trust via social media, and of the need to do research to ensure the legitimacy of the investment company. It also warned about how fraudsters can spoof genuine websites and firms – and may ask consumers not to disclose information to the bank, which is an attempt to prevent the bank from stopping the scam. In response to these warnings, Mrs Z maintained she wanted to proceed.
- I appreciated Mrs Z's representative has pointed out that, when she showed her son the trading platform, he had doubts. However, I can't see HSBC had the same opportunity to assess the true risk – as Mrs Z wasn't upfront about who she was dealing with or what she was doing. Her insistence to proceed without divulging the true nature of the investment gives me significant doubt that HSBC would have been able to get a full and honest explanation from Mrs Z.

In the face of Mrs Z's persistence in making these payments; the explanations she gave; the particular nature of her customer relationship with HSBC; and the sophisticated nature of the scam – I'm not convinced HSBC can be held at fault for failing to dissuade Mrs Z from proceeding at this point.

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

Nor are the payments covered by the Lending Standards Board's Contingent Reimbursement Model (CRM) code. That's because the CRM code only covers scam payments made to another person between UK accounts held in pounds sterling. Whereas all the money lost to the scam was sent via Mrs Z's own cryptocurrency accounts. And the cryptocurrency purchases weren't scam payments as defined by the code as the sellers were genuine.

I appreciate how disappointing this will be for Mrs Z, who has clearly lost out substantially to a sophisticated scam. But in all the circumstances, I'm not persuaded it would be fair to expect HSBC to reimburse her for this.

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 Mrs Z to accept or reject my decision before 9 February 2024.

Rachel Loughlin
Ombudsman