DRN-5006961

The complaint

Mr C complains that HSBC UK Bank Plc won't refund money he lost when he was the victim of two investment scams.

Mr C is represented by a firm that I'll refer to as 'R'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

R complained to HSBC, on Mr C's behalf, on 14 June 2023 saying Mr C had fallen victim to an investment scam. In short, they said:

- Mr C was added to a group chat on an instant messenger app related to crypto trading – which had hundreds of people, all of which were investing successfully and showing their withdrawals.
- Before investing with the scam firm, Mr C watched and reviewed all the information within the group chat. But he wasn't able to carry out an internet search or review the company website as he was told it was being built. He was therefore under the belief it was a new and upcoming company which he was fortunate to be involved in at an early stage.
- Mr C had no prior knowledge of investing in crypto at the time – but he had purchased about £100 of crypto about a year earlier.
- Mr C was told he could receive returns of 1000% per month – which he thought reasonable based on articles he'd seen and media reports saying how much could be earned from investing in crypto.
- Mr C had no prior knowledge of how these scams worked.
- Mr C made the following payments to two legitimate crypto exchanges (which I'll refer to as 'B' and 'C'), before forwarding the funds to the scammer:

Date (statement)	Type	Payee	Amount
2 March 2023	Fund transfer	B	£200
5 March 2023	Fund transfer	B	£4,000
7 March 2023	Fund transfer	B	£3,000
8 March 2023	Fund transfer	C	£2,850
13 March 2023	Debit card	C	£2,549.14
14 March 2023	Debit card	C	£4,634.55
17 March 2023	Debit card	C	£514.95
27 March 2023	Debit card	C	£9,269.10
28 March 2023	Debit card	C	£8,752.20
4 April 2023	Fund transfer	C	£5
4 April 2023	Fund transfer	C	£6
		Total	£35,780.94

- Mr C saw good returns on his initial investment. But he realised he'd been scammed after paying withdrawal fees but not receiving the funds.
- HSBC failed to identify out of character payments that were indicative of fraud. And had HSBC intervened appropriately, the fraud would've been prevented. As such, Mr C suffered a preventable financial loss which should be reimbursed.
- HSBC should refund Mr C and pay 8% simple interest.

HSBC didn't uphold the complaint. They explained the funds were sent to Mr C's own account with different financial service providers (B and C) before they were transferred on to the scammer. And so, they wouldn't provide a refund. They also couldn't attempt a chargeback on the debit card transactions as the service was provided.

The complaint was referred to the Financial Ombudsman. Our Investigator found that Mr C had made a £10,000 debit card payment to another firm that provides crypto services – which I'll refer to as 'P' - on 13 December 2022 (thereby preceding the above payments). She queried with R as to whether this payment was also part of the scam. R confirmed it was used to purchase crypto as part of the same scam, and that it was part of Mr C's complaint against HSBC.

As this payment hadn't been included as part of the complaint submitted on 14 June 2023, HSBC were given an opportunity to respond to it. HSBC's position however remained the same – that being they wouldn't provide a refund as the payment was made to an external account held in Mr C's own name with P, and there being no chargeback rights.

Our Investigator considered the complaint and, in short, she said:

- She didn't think there was sufficient evidence to show Mr C had fallen victim to a scam(s). As she noted Mr C hadn't provided statements from B, C or P showing what had happened to the funds. And there wasn't anything to corroborate the first payment to P being connected to the subsequent payments to B and C.
- There were inconsistencies in the information provided by Mr C. This includes:
    - Despite it being the highest value transaction, the £10,000 payment to P wasn't included in the initial complaint to HSBC – which she considered unusual. She would've expected it to have been raised at the same time considering it is largest single loss. And when asked about the payment, Mr C was unsure as to why there was a gap between it and those in March/April 2023.
    - Although R had told the Financial Ombudsman the £10,000 transaction was part of the same scam, R's submission to HSBC suggests otherwise.
    - There hasn't been any evidence of communication with a scammer showing the scam started as early as December 2022. Nor have details of the firm that scammed Mr C in relation to the £10,000 payment been provided. This is despite R's submission to HSBC saying it was a different firm, albeit one Mr C thinks might have been associated to the same group that scammed him in 2023.
    - In the initial complaint submission, Mr C said he had only purchased £100 of crypto before but hadn't invested in crypto previously. This is despite Mr C making the £10,000 transaction to P a few months earlier.
    - During telephone calls with HSBC, Mr C told them he'd used his crypto wallet for a while and had made lots of payments to it from another bank. This is despite telling the Financial Ombudsman he didn't have previous crypto experience. Similarly, despite Mr C saying the scammer told him to open the

crypto wallets and provided information on how to set them up, he told HSBC otherwise.

- Even if there was sufficient evidence to show Mr C had been scammed, our Investigator wasn't persuaded HSBC could've prevented his loss. This was because, having listened to three calls between Mr C and HSBC, she considered he'd provided HSBC with incorrect or misleading information when answering their questions. This included:
    - Mr C saying he found the investment opportunity through friends and family – even though he's since said he received an unsolicited message on an instant messenger app.
    - When asked if he had received any texts or messages from a third party about making a payment to the investment, he confirmed he hadn't.
    - Mr C said he had done a lot of online research, but in Mr C's complaint letter he says he was unable to review the company website or look up reviews as it was new.

  This hindered HSBC's ability to spot what was happening.
- HSBC gave appropriate warnings relevant to the scam and they assessed the risk based on the answers Mr C gave. If Mr C had told HSBC he'd been contacted on the instant messenger app or there wasn't any information online for him to check the company, HSBC could've been able to identify the scam. Mr C's answers however meant HSBC weren't given critical insight into what was really happening – preventing them from unveiling the scam.
- Although HSBC could've probed Mr C further, she didn't think this was warranted as the answers he provided didn't highlight any concerns. Mr C didn't tell HSBC there was any third-party involvement and, based on how he said he had come across the opportunity, the amount of research he said he'd undertaken, along with telling HSBC that he was experienced in crypto and had made withdrawals from the investment, it would've assured HSBC he wasn't likely at risk. So, she didn't think HSBC ought to have done anything more in the circumstances.
- There wasn't anything more HSBC could've done to recover the funds.

R didn't agree. In short, they said:

- The intervention wasn't sufficient, and HSBC missed multiple opportunities to uncover the scam.
    - They maintain Mr C was honest and collaborative in the calls – shown by his grateful attitude when he said, *"thank you for being so cautious".* This illustrates he wasn't prejudiced against the bank.
    - Mr C clearly expressed concern about the investment opportunity when he said, *"I've got a lot of money there* [joint account]*, so if anything did go wrong, then I'd hate for that account to get attacked. I've got less money in my HSBC so it's less of a risk, trying to be as safe as possible*". HSBC didn't however question why Mr C was concerned about anyone attacking his bank account and proceeded to release the payment.
    - When asked if he would be making any more payments, Mr C said, *"hopefully I will be withdrawing from there. So no, I won't be putting more in"*. From this statement, it is abundantly clear that Mr C might be sending money as withdrawal fees, which is particularly common in crypto scams. This was a prominent red flag, but HSBC didn't question Mr C any further.
    - The only time Mr C was questioned about the investment returns, a closed-ended and leading question was used. With the bank asking, *"It's not a scheme that is offering you incredibly high returns, it's just a crypto investment, is it?"* HSBC clearly didn't sufficiently question Mr C's

understanding of crypto or attempt to find out about the end destination of the payments.

Had HSBC intervened properly, the scam would've easily been uncovered.

- All payments were preventable as P had a warning registered with the International Organization of Securities Commissions (IOSCO) before the transactions took place. They've seen cases whereby the Financial Ombudsman has said such a warning should've automatically triggered on a firm's systems, prompting the firm to enquire and provide a scam warning.
- Hence, P is clearly a fraudulent company, and HSBC must have known that. The payment shouldn't have been allowed to go through. Had the bank intervened sufficiently with regards the payment to P, the scam could've been uncovered, and Mr C wouldn't have sent any further payments towards crypto investment scams.
- Mr C provided his crypto wallet statements from C – as well as emails showing his crypto activity.
- They addressed some of the inconsistencies highlighted by our Investigator which they said was due to miscommunication and not a change in testimony:
    - In, or just before, December 2022 Mr C received a message offering him an investment opportunity. This led to the £10,000 payment made to P. And as soon as it was made, all access Mr C had to the platform and service was lost and the scammers cut contact.
    - Mr C went on holiday between December 2022 and February 2023. He was pushed in the pool and the message threads regarding P were lost due to water damage.
    - When Mr C contacted R about the scams, he said he thought his details must have been passed from the initial scam with P to the second scam – and he is now being repeatedly targeted in a manner consistent with his details being shared. They believe the £10,000 payment is intrinsically linked to the events and decision-making being assessed in the secondary scam.
    - Any inconsistencies with Mr C's testimony in respect of crypto is due to his own fundamental misunderstanding of what crypto is, and how it works. As an example, when R asked Mr C if he'd invested in a crypto coin before he said he hadn't, but when asked if he had bought a crypto coin, Mr C confirmed he had. Mr C was unaware this crypto coin was crypto. And he explained he was unaware B and C were crypto exchanges, but rather, he thought he was investing in gold/commodities/oil.
    - Due to Mr C's lack of knowledge surrounding crypto, he was unknowingly transferring the funds into a wallet he had no control over. He wouldn't have done this had he known otherwise and that there wasn't any way the funds could be recovered if something went wrong.
    - They confirmed that, prior to the £10,000 transaction, Mr C had only ever purchased a very small amount of crypto – about £50-£100.
    - Had HSBC questioned Mr C effectively about the payments, such as what crypto he was purchasing, it would've been immediately clear that he wasn't able to invest independently in the matter he appeared to be doing so.
- They don't think Mr C should be punished for not keeping meticulous records and evidence of the scam – as he didn't know he was being scammed at the time. They believe Mr C's testimony is clear and they've not seen HSBC provide anything to contradict this. And, while not complete, the provided correspondence shows Mr C did communicate with scammers – it therefore shouldn't be disputed whether he fell victim to a scam.
- Since the scam, Mr C has experienced some significant and difficult personal circumstances in his life. This includes losing his job, home and family. And as a result, Mr C suffers from mental health difficulties that affect him on daily basis.

Our Investigator considered the additional points put forward by R, but her overall view remained the same. In short, she added:

- The IOSCO warning available at the time the £10,000 payment was made explained that P wasn't regulated in that particular country to provide investment advice. It didn't say P was a scam. P is a crypto platform regulated in a different country which is still running today.
- Mr C hasn't provided any evidence to suggest the payment to P was made in relation to a scam – or that he lost any funds.
- Mr C has said he hasn't been able to provide evidence of the scam due to water damage from being pushed in the pool while on holiday. But messages on the instant messenger app should be recoverable (with our Investigator providing instructions on how to do this).
- Mr C has only provided his communication with the scammer between 24 and 30 March 2023. It therefore doesn't cover the payments before or after this period. Nor has there been any explanation as to why Mr C hasn't been able to provide the full chat conversation – only the middle bit.
- From the crypto wallet statements provided (C), she could link some of the payments Mr C had made to the chat conversation – so there was evidence Mr C had fallen victim to a scam. Although she still hadn't seen anything to suggest that the £10,000 transaction to P was a scam or connected to the subsequent payments.
- Although she was able to evidence that Mr C appears to have sent payments to a scam, she didn't think HSBC were responsible for his loss. This is because their interventions were proportionate for the payment(s) he was making, and Mr C provided incorrect information to them which inhibited their ability to understand the true risk associated with them.

The matter has been passed to me to decide.

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 appreciate Mr C has suffered a significant loss and that, from this, I understand he's had to deal with some difficult personal circumstances. I'd like to reassure Mr C that I've taken everything R, on his behalf, have said into careful consideration. But while I'm extremely sympathetic to Mr C's situation, I must consider whether HSBC is responsible for the loss Mr C is claiming for. Having done so, and while I know this won't be the outcome Mr C is hoping for, for similar reasons as our Investigator I don't think they are. I'll explain why.

At which point, I'd like to acknowledge that R has provided substantive submissions in support of Mr C's complaint – and why they consider HSBC responsible for his loss. But if there's a submission or point that I've not addressed, it isn't because I've ignored it. Instead, it's simply because I've focussed on what I consider to be the central issues in this complaint – that being whether Mr C was the victim of investment scams and if HSBC are responsible for the loss he claims to have suffered.

Where the evidence is incomplete, inconclusive, or contradictory, I must make my decision on the balance of probabilities – that is, what I consider is more likely than not to have happened in the light of the available evidence and the wider surrounding circumstances.

In line with the Payment Services Regulations 2017, consumers are generally liable for

payments they authorise. HSBC is expected to process authorised payment instructions without undue delay. But as a bank, they also have long-standing obligations to help protect customers from financial harm from fraud and scams. Those obligations are however predicated on there having been a fraud or scam. And so, it would only be reasonable for me to consider whether HSBC is responsible for the loss Mr C claims to have suffered if, indeed, he has been scammed. I've therefore considered whether Mr C was a victim of a scam.

I've firstly considered the £10,000 payment Mr C made to P on 13 December 2022. Mr C has explained this payment was made for investment purposes and that it was separate to the subsequent March/April 2023 payments – albeit he believes he may have been targeted by the same group of scammers. But other than Mr C's testimony, there hasn't been anything to evidence what this payment was for. Or that it was linked in any way to the March/April 2023 payments.

R has argued that P is clearly a fraudulent company as it had a warning registered with IOSCO before the transaction took place. So, the £10,000 payment shouldn't have been allowed to be processed by HSBC. And had HSBC stopped the payment, and provided Mr C with a scam warning, he wouldn't have made the subsequent crypto transactions either.

While I've considered R's point here, I'm not persuaded that this warning – or those that have subsequently been added - sufficiently demonstrates P is a fraudulent company. This is because, having considered the wording, the IOSCO warning signposts to a foreign jurisdiction that warned P wasn't authorised to provide certain financial services in their territory. Most crypto-related activities are however unregulated in the UK. And beyond this warning, I haven't seen anything to show that P isn't providing legitimate investment services. It follows that I don't think it would be fair to expect HSBC to treat every payment to P as suspicious or high risk. And so, I don't think HSBC needed to provide a warning to Mr C about P at the time because of the IOSCO warning alone.

As I've said, there hasn't been any evidence provided to show what this payment was for. I appreciate Mr C has said this is because his phone suffered water damage whilst on holiday. But chat conversations on the instant messenger app should be recoverable – and our Investigator has explained how to do this. Nor have I been provided any statements from P. In the absence of this, I can't know what happened to the funds upon them being received by P – including whether Mr C has indeed suffered a loss. P offers a range of financial services, including crypto, and I haven't seen anything to indicate they were involved in a scam.

As I've said, HSBC has obligations to protect their customers from financial harm from fraud and scams. As I've concluded there wasn't a scam to prevent in relation to the £10,000 transaction, there was no reason for HSBC to intervene in the payment instruction Mr C provided (or done more prior to following the instruction).

This brings me to the March/April 2023 transactions. And here, while limited, there is some documentary evidence to support Mr C's claim that he fell victim to an investment scam. That being Mr C's conversation with the scammer on the instant messenger app between 24 and 30 March 2023. It's unclear why the full conversation hasn't been provided – as, from Mr C's testimony, the transactions happened after his previous phone suffered water damage. Mr C's complaint submission also says he received professional documentation from the scammers and that he signed a contract for one-to-one trading, but this hasn't been submitted to the Financial Ombudsman either.

Mr C has however supplied his statements for his crypto wallet with C. And some of the transactions appear to correlate with the chat conversation Mr C has supplied. Considering this, and on balance, I think it's more likely than not that Mr C did fall victim to a crypto scam

in relation to the March and April 2023 payments.

I've therefore considered whether it would be fair and reasonable to hold HSBC responsible for this loss. As I've explained, HSBC has long-standing obligations to help protect customers from financial harm from fraud and scams. Looking at the payments Mr C made to B and C, and considering they were to a payee/merchant identifiable as providing crypto services (which carries a known fraud risk), I think it would've been reasonable for HSBC to have had concerns Mr C could be at risk of financial harm from fraud.

HSBC spoke to Mr C on three occasions, including in respect of the £4,000 payment he made on 5 March 2023. I've therefore considered whether HSBC took reasonable and proportionate steps to protect Mr C from the scam.

Within this call, Mr C explained the £4,000 payment was for crypto investment purposes. And following further questioning from HSBC, Mr C told them: he came across the opportunity through his friends and family, he'd invested in crypto previously having had several wallets in the past and was well aware of how it all worked, he'd set up the wallet and had full control of it, he'd been communicating with the firm online and had carried out checks on the internet (with the firm being well-established and that he'd used them before), and that he'd tested the wallet with a previous payment and withdrawal with both of them being successful.

This however is at odds with what Mr C has told the Financial Ombudsman – with him since saying that he was contacted about the investment opportunity from an unsolicited message on an instant messaging app, he didn't have any previous crypto experience (other than purchasing about £50-£100 of crypto about a year prior), and that he didn't carry out checks on the scam firm online as their website was still being built.

I also find it odd that, within this call, Mr C professed to be experienced in crypto investing having had several wallets before. And that despite HSBC explaining to him that they'd seen a rise in investment scams – such as the opening of fake crypto wallets and providing of fake screenshots of accounts – Mr C failed to mention that he'd fallen victim to what he's claimed was a crypto investment scam only a few months earlier. While this scam hasn't been evidenced to the Financial Ombudsman, considering Mr C says he lost £10,000 to it and all contact was immediately cut after the payment was made, I would've reasonably expected HSBC's warning to have resonated with Mr C and for him to have mentioned it to HSBC at the time.

The absence of sharing this with HSBC and providing them with the above inaccurate information, along with not disclosing that a third-party firm (other than the crypto exchange) was involved, leads me to conclude that Mr C wasn't entirely honest or open about the true purpose of the payment(s) or the circumstances around it. It's unclear why this was, possibly through Mr C being coached by the scammer - although I haven't seen evidence of this, nor has Mr C said this happened. Nevertheless, I don't think the answers Mr C provided HSBC – or what he disclosed to them – would've given them sufficient reason to suspect he wasn't telling the true circumstances surrounding the payment. Instead, I think HSBC would've been reassured that Mr C was investing in crypto legitimately, he was experienced in doing so, and that he wasn't being pressured or guided by a third party.

At which point, I understand R has referred to aspects of the conversations between HSBC and Mr C in which they consider HSBC ought to had reason for concern, thereby prompting further questioning/probing. This includes Mr C explaining that he was using his HSBC account, rather than funding the investment directly from a joint account with another provider, for safety reasons – as he had more money in the joint account and would *"hate"* for it to be *"attacked"*. While I acknowledge R's point that HSBC could've questioned why Mr

C had concerns his bank account might be attacked, I don't think concerns in respect of the security of an account necessarily relate to any concerns in respect of the legitimacy of an investment opportunity. And using an account of a low balance value, opposed to one where high value savings is held, is a sensible and commonly used method to minimise the risk of it becoming exposed (as those account details haven't been used or shared). So, I don't think this security concern would've given HSBC reason to think Mr C suspected the investment wasn't legitimate or posed such a risk.

R also believes HSBC should've identified Mr C might be sending money for withdrawal fees (which is common in crypto scams), as he said *"hopefully I will be withdrawing from there. So no, I won't be putting more in"*. And that they consider the only time Mr C was questioned about the investment returns, a closed-ending and leading question was used.

I've considered R's points here, but I disagree that HSBC should've been on notice that Mr C might be sending money for withdrawal fees. This is because, from what he said, I'm satisfied Mr C was simply explaining – at that time – he didn't intend on investing further but, instead, he hoped to receive returns from this investment. And I think it's quite normal for an investor to expect returns from their investment. Furthermore, and quite importantly here, Mr C had told HSBC he was making the payment for investment purposes, and he didn't make any reference or suggestion that he was sending the funds to pay for any type of fee.

I do accept that HSBC could've used more open questions at times with Mr C. But while that might be the case, I don't think this is the reason the scam wasn't uncovered. As I've explained, I don't think Mr C was entirely open or honest when questioned by HSBC. And even when HSBC queried if it was *"a scheme that is offering...incredibly high returns"* or questioned Mr C whether he'd *"received any calls, texts or emails from third parties"* asking him to make this payment, he failed to disclose the investment firm or that he'd been told he could expect to receive returns of 1000% per month. Although I note R's point that Mr C considered this return reasonable based on articles and media reports on crypto investing, I don't think it can be reasonably argued that this level of return isn't 'incredibly high'. So, despite the method of questioning HSBC used, I think this ought to have resonated with Mr C. I therefore consider it would've been reasonable to have expected Mr C to have disclosed it to HSBC at the time.

For these reasons, I'm not persuaded HSBC had sufficient reason to question Mr C about the payments more than they did. I think it was reasonable for them to accept the information Mr C provided in good faith which, unfortunately, prevented them from identifying Mr C was falling victim to a scam due to the information he withheld. It follows that I don't think HSBC would've had reason to think Mr C was at significant risk of falling victim to financial harm from fraud.

I'm aware that after the telephone conversations between Mr C and HSBC, higher value transactions to C were made – such as the payments on 27 and 28 March 2023 of about £18,000 combined. By this point however, Mr C had been making payments for crypto purposes for some time – nearly four months since the payment to P. Because of this, these payments would've appeared to HSBC as normal account activity – and thereby wouldn't have been seen as unusual or out of character for Mr C. Furthermore, HSBC had previously spoken with Mr C and been reassured – for the reasons I've explained – that he wasn't at risk of financial harm from fraud. I therefore wouldn't have expected HSBC to have carried out additional checks before processing these payments.

For the sake of completeness, I've thought about what would've happened if HSBC had carried out additional checks before processing these subsequent payments. But even if they had, I don't think it would've made a difference. This is because I'm not persuaded that, upon further questioning, Mr C would've answered any differently about the true purpose of

the payments - including how he came across the investment opportunity, his level of crypto experience or disclosing he was being directed by a third party to make the payment(s). I say this as his responses to HSBC's questions across the three conversations remained consistent. And so, I think it's more likely than not Mr C's position would've remained the same on any checks carried out on any of the subsequent payments. I therefore think Mr C would've likely concealed the truth about the payments from HSBC as he had already done.

It follows that I think HSBC took reasonable steps to protect Mr C from the scam. And even if they'd gone further than they did by carrying out further checks on later payments, I don't think it would've made a difference.

I've considered whether, on being alerted to the scam, HSBC could reasonably have done anything to recover Mr C's losses, but I don't think they could. For the payments made by fund transfer, the only option of recovery would've been for HSBC to have contacted the beneficiary banks – that being the banks used by the crypto exchanges. But these funds were moved from Mr C's crypto wallets and so, there wouldn't have been any funds remaining for HSBC to recover. But even if there were funds left, Mr C would've had access to the funds and could've removed them himself at the time – and quicker than any recovery attempt by HSBC. In respect of the debit cards payments, the only possible option for recovery would've been for HSBC to have attempted a chargeback against the payee - that being the crypto exchange (C). But I don't there would've been any prospect of success given there's no dispute that the crypto exchange provided crypto to Mr C, which he – unfortunately - subsequently lost to the scam.

I have a great deal of sympathy for Mr C and the loss he's suffered. But it would only be fair for me to direct HSBC to refund his loss if I thought they were responsible – and I'm not persuaded this was the case.

My final decision

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 C to accept or reject my decision before 2 January 2025.

Daniel O'Dell
Ombudsman