DRN-4309849

The complaint

Miss F complains that HSBC UK Bank Plc ("HSBC") has failed to refund over £23,000 she lost to a cryptocurrency investment scam in March 2022 after being contacted on social media by a scammer.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Miss F fell victim to a cryptocurrency investment scam after she was contacted by two individuals on Instagram claiming to be brokers from Perfectmegatrade.com and Todaysstockmarket.net.

Over the space of around two weeks, Miss F transferred over £23,000 to the scammers via crypto wallets she opened as part of the scam. She realised it wasn't a legitimate investment when the scammers kept asking for more money to withdraw her profits, and eventually stopped responding to her altogether. HSBC refused to refund the money Miss F lost as it said she had authorised the payments.

Our investigator upheld the complaint. She thought that HSBC should have intervened in the payment of £9,000 Miss F made on 13 April 2022 and thought that this would have likely prevented any further losses. As a result, the investigator recommended that HSBC refund the money Miss F lost from this payment onwards. HSBC disagreed, so the matter was escalated to me to determine.

I issued my provisional decision on this complaint on 24 July 2023. I said I was minded to uphold it, but on a slightly different basis to the investigator, and set out the following reasons:

> *It doesn't appear to be in dispute that Miss F has fallen victim to a scam here. And having reviewed the evidence she has provided. I'm also not persuaded the merchants had honest intentions, but instead set out to defraud Miss F of her money. It is also common ground that the disputed payments were 'authorised' by Miss F for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. This is because they were made by her using the legitimate security credentials provided by HSBC. But having concluded that this was a scam, it's also necessary to consider whether the disputed payments were unusual or uncharacteristic enough for Miss F's account such that they ought reasonably to have triggered an intervention by HSBC.*
>
> *It isn't in dispute that the £500 payment Miss F made to Moonpay on 4 April 2022 from her HSBC account was unusual given that it did trigger the bank's fraud prevention systems and was automatically blocked pending further enquiry. Accordingly, it's just a question of whether the bank went far enough in all the circumstances with that intervention.*
>
> *When HSBC spoke to Miss F over the phone, it asked her about the nature of the payment she was making, to which she was upfront and told it that she was investing*

in Bitcoin for the first time. But then instead of asking for further details about the investment opportunity and how she came across it, HSBC instead recommended that Miss F verbally confirm the account details with the beneficiary. She later called back and explained how she had obtained the account details, and also gave further information about being able to see her investments on a platform. However, this prompted no further questioning or line of inquiry from HSBC about the context of the investment she was making, and the payment was released.

I understand our investigator considered this level of intervention to be proportionate given the relatively low value of the payment being made. But based on the information Miss F had given HSBC during the calls on 4 April 2022, I think it had a clear opportunity to prevent the scam at that point, which I think it could've likely done if it had simply probed further into the answers Miss F provided. When she said she was investing in cryptocurrency for the first time, for example, this should have instantly prompted the bank to ask further questions about the nature of the investment and how she found it, given the high risks of fraud and scams inherent in this form of trading. However, HSBC didn't ask any such questions and instead mainly focussed on how she had obtained the account details and whether she had checked who she was paying.

If HSBC had instead asked for more of the basic surrounding context, it would have likely established that she had been contacted out of the blue by two people on social media, who were encouraging her to invest in cryptocurrency. It could've also established that they had coached her through opening different crypto wallets to send money to, where she was then being instructed to send Bitcoin on to further wallets – all of which are typical features of these sorts of investment scams. I have no reason to doubt that Miss F wouldn't have been upfront about what she was doing. She hasn't said she was coached by the scammers to deceive the bank, for example, and she readily told it that she was investing in cryptocurrency when she was asked.

Overall, I'm satisfied that a warning to Miss F from HSBC on 4 April 2022 would have probably led her to discover that she was likely being scammed and exposed the broker's false pretences. Even if Miss F had not worked out that this was a scam, it is likely that a warning would have alerted her to the common issues arising in relation to cryptocurrency scams, which in turn would have revealed the truth behind the supposed broker's representations. This would have probably stopped Miss F in her tracks. So, but for HSBC's failure to act on clear indications of potential fraud or financial harm during its call with Miss F on 4 April 2022, she probably wouldn't have lost her money.

I appreciate that Miss F was presented with a scam warning when she selected "making an investment" for the payment she made on 13 April 2022. But this warning was about investment and pensions scams in general. I don't think it was tailored or specific enough to the circumstances of the scam she was falling victim to. So, I don't think this is enough to say that Miss F would've likely ignored any specific warning HSBC could have given her over the phone when she spoke to it on 4 April 2022. And I'm persuaded that such a warning from an actual person from HSBC would have been more impactful and prevented any further losses. I therefore intend asking HSBC to refund the money Miss F lost from the £500 payment she made on 4 April 2022 onwards.

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000). In this case, I do not think that Miss F can *fairly or reasonably be blamed for what happened, and I don't think she could have reasonably foreseen the risk of this sort of harm.*

Miss F has explained that she checked whether any of the investment brokers featured on the FCA warning list, which they didn't. She also says she validated both sites using a Google safe browser transparency report which stated that no unsafe content had been found on either site. I also cannot see that there was any negative information or warnings online about either Perfectmegatrade.com or Todaysstockmarket.net at the time. So, even if Miss F could have carried out further checks, it's unlikely this would've led to her discovering that the brokers were likely operating a scam.

HSBC also say it was implausible of Miss F to think she would have to pay more than the value of her original investment in order to withdraw funds from the platform. But I don't agree. It's very common for investment scammers to manipulate fake trading platforms to make their victim think they have made significant profits in order to encourage them to either invest more, or to pay large withdrawal/commission fees in order to access the money, as was the case here. And given Miss F had been led to believe she had made a lot more than she originally invested, I don't think it was wholly unreasonable of her – as a first-time investor – to think that she would need to pay certain fees and commissions to access her funds, particularly when scammers are very adept at persuading their victims that they won't receive any profits without paying such fees upfront.

Overall, I do not think Miss F could have foreseen the risk that the company she was dealing with was a scam and the trading account she was viewing was likely to be a simulation. In the circumstances, I do not think it would be fair to reduce compensation on the basis that she should share blame for what happened.

I invited further comments and evidence from both parties. Miss F accepted my provisional findings and proposals, but HSBC disagreed. In summary, it said:

- It still considers its questioning of Miss F to have been proportionate when it spoke to her about the payment she made on 4 April 2022 and doesn't believe she would have revealed further information if it had asked further questions.

- It considers a reasonable person would have foreseen the risk of harm such that Miss F should be held jointly liable for her loss.

- The majority of payments made as part of the scam appear to have been made from a savings account, so any interest awarded should be limited to the rate of that account rather than 8% simple interest.

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 have also carefully considered the points put forward by HSBC in response to my provisional decision. And aside from the rate of interest I originally intended awarding in this case, my conclusions and outcome otherwise remain unchanged.

<u>*Intervention and Causation*</u>

HSBC considers its line of questioning to have been proportionate and doesn't think it would have obtained honest responses from her. I acknowledge that a payment of £500 would not normally be enough in itself to trigger an intervention by a bank. But the fact is in this case, it did trigger HSBC's fraud prevention systems. So, given it had the opportunity to ask Miss F about the nature of the payment, I would've expected it to have asked appropriate questions, which includes responding and asking for further information in light of the information given by its customer. It cannot simply ignore certain risk factors that can be identified in the answers Miss F gave just because it was a low value payment.

In any event, it's clear that HSBC already had concerns about who Miss F was paying, as it blocked the payment and asked her to double check the account details with the beneficiary. But what it didn't do was ask detailed enough questions in light of those concerns.

HSBC says that its suggestion to call the beneficiary was a result of Miss F saying the payment details had been received by email, which would have led her back to Moonpay, rather than the scammer. But given she was seemingly transferring money to her own crypto wallet with Moonpay – where she said she was investing in cryptocurrency for the first time – the fact that she had received payment details from another beneficiary via email ought to have been enough cause for concern and prompted questions around who was sending her these payment details, rather than simply asking her to check they were correct.

HSBC says that during the second call it had with Miss F, where it was asking about how she could see her investments performing, that it would have been the ideal time for her to mention either of the merchants she was investing with. However, Miss F was a first-time investor and was simply responding to the questions HSBC was asking. The bank is the professional in financial matters here and ought to have known to ask for this information in light of its knowledge about cryptocurrency scams, rather than expecting Miss F to know what sort of information to offer up. Miss F cannot fairly be held at fault for failing to give information to questions that HSBC did not ask.

HSBC has also suggested that Miss F gave an inaccurate answer when she said that no third party was asking or forcing her to make the payment. But I don't consider this to be an inaccurate answer. Miss F was not being asked or forced to make the payment by a third party. She was making the payment of her own volition under the guise of an investment. Based on the phone calls I have listened to, Miss F answered HSBC's questions honestly and accurately, and I still don't consider there to be enough persuasive evidence to suggest that she was coached to lie to the bank or would have likely been dishonest if it had asked her further questions. HSBC has pointed towards Miss F at one stage selecting the option "buying goods or services" as the reason for her payment. But again, this does not suggest that Miss F had been told to lie to the bank. She simply chose this option as she was buying cryptocurrency, which isn't incorrect in the context of the payment she was making.

Overall, I'm still not persuaded HSBC did enough when it spoke to Miss F over the phone. It failed to respond appropriately to the answers she was giving and instead gave unhelpful advice that wouldn't help Miss F protect herself in the context of a cryptocurrency investment scam. In my judgment, it missed a clear opportunity to prevent any further loss, so the conclusions set out in my provisional decision remain unchanged.

Contributory negligence

HSBC also submits that Miss F should be held jointly liable for her loss. It has said that a reasonable person would not think it reasonable to pay around £23,000 in fees to access the profits of their investment, and that her returns must have been too good to be true.

I've already set out why I don't think it would be fair to hold Miss F jointly liable in this case, which still stands. I accept that Miss F may have been naive to think that she would have to pay as much money as she did in withdrawal fees in order to access her money. But I don't consider this amounts to *negligence,* or that she could be considered as having courted an unreasonable risk in this instance.

Miss F was not an experienced investor. And given the returns some legitimate investors have seen through investing in cryptocurrency, I don't think it was wholly unreasonable for her to have thought she could make significant profits. Cryptocurrency does not work in the same way as investing in traditional assets such as stocks and shares, and the volatility of cryptocurrency means that high returns (as well as significant losses) are often possible. And, as I set out in my provisional decision, Miss F also would not have found any adverse information about either of the merchants online at the time. So, HSBC's comments have not altered my conclusions with regards to contributory negligence, and I still don't consider it would be fair and reasonable to hold Miss F jointly liable in the circumstances of this case.

Interest

In terms of HSBC's arguments about the rate of interest applied, I can see that the majority of the money Miss F lost as part of the scam was paid in from her savings account. Miss F has also confirmed that this is correct.

I appreciate that Miss F's savings account may not have been the *sole* source of funds lost to the scam. But having reviewed her statements, it certainly accounts for the vast majority of it. As a result, instead of 8% simple interest, I consider it would be fair and reasonable to instead awarded interest at the applicable savings account rate, as this is closer to what Miss F would've otherwise earned, had her money not been lost to the scam.

My final decision

For the reasons given above, I uphold this complaint and direct HSBC UK Bank Plc to:

- Refund the money Miss F lost to the scam from the payment she made on 4 April 2022 onwards.
- Pay interest on this amount at the applicable savings account rate at the time, from the date the payments were made to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss F to accept or reject my decision before 19 September 2023.

Jack Ferris
Ombudsman