DRN-3449273

The complaint

Miss Y complains that HSBC Bank UK Plc ("HSBC") have failed to refund over £18,000 she lost as part of an investment scam.

What happened

The details of this complaint are well known to both parties, so I will not repeat everything again here. In summary, Miss Y sent over £18,000 in payments to various legitimate cryptocurrency trading platforms, such as Moonpay, CEX.io and COINMAMA using her HSBC credit and debit cards in January 2021, where the funds were subsequently transferred on to a fraudulent broker ("expertcryptomining.com") from the crypto platforms. The following transactions were disputed by Miss Y:

Date	Merchant	Amount	Running total
02/01/2021	Moonpay	£216.69	£216.69
03/01/2021	Moonpay	£57.92	£274.61
06/01/2021	Moonpay	£1076.75	£1351.36
06/01/2021	Moonpay	£4301.81	£5653.17
06/01/2021	Moonpay	£4301.84	£9955.01
06/01/2021	COINMAMA	£925.05	£10,880.06
07/01/2021	CEX.io	£90.66	£10,970.72
08/01/2021	Moonpay	£6452.11	£17,422.83
09/01/2021	Moonpay	£808.50	£18,231.33
12/01/2021 (CC)	CEX.io	£651.35	£18,882.68
Total			**£18,882.68**

She realised she had been scammed when she was unable to make a withdrawal and the broker ceased all contact with her.

Miss Y reported the fraud to HSBC on 23 January 2021 where she falsely told the bank that she had no knowledge of the transactions and blamed a third party who she said had stolen her handbag. HSBC discovered this was false as they had contacted the crypto platforms who confirmed that Miss Y had opened the accounts with them. Miss Y subsequently confessed to the story being false and admitted the payments had been authorised, albeit on false pretences as she had been scammed. However, HSBC refused to provide her with a refund.

Our investigator upheld Miss Y's complaint. He considered there was an unusual pattern of spending, such that HSBC ought to have intervened in the payment to question Miss Y about what it was for, which would have prevented any further loss. He therefore recommended that HSBC refund the payments made from the £4,301.81 payment on 6 January 2021 onwards. HSBC disagreed. They said that Miss Y's dishonesty meant that her testimony should be treated with scepticism, and that she hadn't provided any evidence of her dealings with the merchant. As a result, the matter has been escalated 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.

It isn't in dispute that Miss Y authorised the disputed payments she made to the crypto platforms using her HSBC debit and credit cards (where her funds were subsequently transferred on to the scammers from her crypto wallets). The payments were requested by her using her legitimate security credentials provided by HSBC, and the starting position is that banks ought to follow the instructions given by their customers in order for legitimate payments to be made as instructed.

HSBC have suggested that the merchant (Expertcryptomining.com) may not even be a fraudulent trader. However, based on what I've seen, I'm satisfied the merchant was not carrying out legitimate binary options/crypto investment trades but were instead dishonestly defrauding customers, e.g. by not actually making trades/bets with the money received from the clients but simply manipulating their online 'trading platform' to show purported gains in order to induce further 'investments'. In the absence of evidence to the contrary, I have concluded this because:

- Miss Y says she was approached by the merchant with the investment opportunity on social media, which immediately gives cause for concern as this would not be the usual practice of a legitimate and regulated investment broker. The tactics that Miss Y has described also sound typical of a scam, i.e. being told by the merchant that her investment had made profit, and that she would need to make further deposits in order to withdraw her money. After paying to withdraw her money, the merchant ceased all contact. This is a complaint repeated across many disputes against similar firms.
- Similarly, Miss Y was also asked to download remote access software to her phone to give the merchant remote access to place trades on her behalf. Unlike legitimate traders, all the payments Miss Y made were first paid into a crypto wallet before being transferred to her 'trading platform', which is a typical tactic used by scammers.
- There's a body of external information available through various regulators, law enforcement agencies, government agencies, press cuttings and the card schemes that repeat the same tactics used by the merchant. Which does lead me to seriously question whether any actual trades were being placed on the outcomes of financial markets or whether in fact the merchant was offering little more than a simulation.
- There is also further evidence in the form of warnings placed online by 'scam watch' websites and forums that warn investors about Expertcryptomining.com, which includes accounts of other victims that have shared similar experiences to that of Miss Y. In addition, at the time Miss Y made her payments, they were not regulated by the Financial Conduct Authority, and neither can I see that they were regulated or licensed in any other jurisdiction either, which is also strong evidence that they were operating fraudulently.

Having considered all of this together, I don't think it's likely the merchant was operating a legitimate enterprise. I've therefore considered whether HSBC should have done more to prevent Miss Y from falling victim to the scam, as there are some situations in which a bank should reasonably have had a closer look at the circumstances surrounding a particular transfer. For example, if it was particularly out of character.

HSBC is aware of our general position on a Payment Service Providers' safeguarding and due-diligence duties to protect customers from the risk of financial harm due to fraud. We

have published many decisions on our website setting out these principles and quoting the relevant rules and regulations. It is unnecessary to rehearse them again here in detail.

Having reviewed Miss Y's account history, I'm satisfied there were reasonable grounds for HSBC to suspect fraud, such that they ought to have intervened to have a closer look into the circumstances of the payment Miss Y was making. I accept that the payments Miss Y made on 2 January 2021 and 3 January 2021 to Moonpay would not have been unusual enough to have triggered HSBC's fraud detection systems given their low amount. But a few days later, on 6 January 2021, Miss Y made a series of payments to Moonpay in quick succession, where she paid over £10,000 within the same day through the following debit card transactions:

Date	Time	Payee	Amount
6 January 2021	10:16	Moonpay	£1,076.75
6 January 2021	10:52	Moonpay	£4,301.81
6 January 2021	15:23	Moonpay	£4301.81
6 January 2021	18:38	COINMAMA	£925.05

I appreciate the first payment would not have appeared unusual in terms of the amount. But when she sent a second payment to the same company for £4,301 within the same hour, I think this ought to have triggered HSBC's fraud detection systems. This was an identifiably unusual and uncharacteristic pattern of spending for Miss Y which ought to have alerted HSBC to the risk of financial harm.

Therefore, I'm satisfied they ought to have intervened by blocking this payment and questioning Miss Y about it before allowing it to be processed. But I've not seen any evidence of HSBC contacting Miss Y or blocking any of the disputed payments, despite there being several more sent on the same day, which can be indicative of someone that is in the process of being scammed.

At the time the payment was made, HSBC ought to have had a good understanding of how investment scams commonly work. And given the size of the payment, and that it was being used to purchase cryptocurrency from an online platform, I would have expected the bank to have asked additional questions about the context and purpose of the transaction. While it is not up to our service to dictate which questions a bank should ask, HSBC could've, for example, asked how Miss Y had come to make the purchase in the first place, and whether she was being 'assisted' by a third party in the purchase. They could've also asked if she had opened the crypto accounts herself, as this would have also given a strong indication that she was in the process of being scammed. This would have formed part of a reasonable line of enquiry to protect a consumer from the potential risk of a prominent type of scam.

Had HSBC asked such questions on 6 January 2021, I'm satisfied it would have become apparent at that point that Miss Y was falling victim to an investment scam. HSBC have raised the point that Miss Y has provided inconsistent testimony and gave misleading information when she reported the fraud.

I acknowledge that Miss Y initially gave a dishonest account of what had happened, where she originally told the bank that she had no knowledge of the transactions. She has explained that she was panicked and had followed advice from a friend about what to say in order to give her the best possible chance of recovering the money she had lost. However, while Miss Y was not forthcoming with the truth about the payments *after* she had lost the money, I'm not persuaded she would have had any cause to lie to the bank if they had asked her what the payments were for *before* she realised it was a scam.

Based on what I have seen, Miss Y wasn't coached by the scammers to hide the true purpose of what she was doing. She has also since given a full and frank version of what happened and how she came to authorise the transactions, which is supported by the evidence and is a similar account to numerous other examples of how investment scammers operate. Miss Y has also provided evidence of her interactions with expertcryptomining.com in the form of emails and WhatsApp messages, which give destination wallet addresses for her to send the cryptocurrency onto once she had made her deposits. She has also provided emails of the merchant saying they have received her withdrawal charges. The evidence Miss Y has provided corroborates her account of what happened, so I'm satisfied she has given an honest account.

So, despite Miss Y's initial dishonesty, I consider her testimony to be truthful and compelling, and I'm satisfied her money was lost to a scammer. So, if HSBC had asked further questions and probed for more of the basic surrounding context of the payments, I consider it's likely that Miss Y would have explained what she was doing and that everything had originated from a third party broker, who had said she had to invest further money and pay 'withdrawal charges' in order to release the money she had already invested – which would have been a clear indication she was being scammed.

I appreciate that Moonpay and COINMAMA are legitimate platforms. But I think HSBC should still have provided a scam warning in light of all the information known to banks about the increasing number of scams associated with cryptocurrency at the time.

After all, at the time, there was information in the public domain – which a bank ought to have known even if a lay consumer ought not – about the very high risks associated with crypto trading, including many warnings of potential fraud. For example, the FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018. Regulated businesses ought reasonably to take notice of such insight. By the time Miss Y made the payments to Moonpay, cryptocurrency scams had risen greatly in frequency and it's reasonable to conclude that banks, such as HSBC, had also had time to digest these warnings and put mechanisms in place to detect and prevent this type of fraud.

By the time Miss Y made the payments on 6 January 2021, HSBC ought reasonably to have been alive to the fact that consumers often first purchase a crypto asset or send money to a platform, where the money is subsequently moved on to or taken by the fraudster. So, it is with this in mind that I think HSBC ought to have probed further about the nature and context of the payments Miss Y was making.

In light of this, I think Miss Y's losses were foreseeable to HSBC despite the payment on the face of it not leaving the consumer's control. And I'm satisfied that had the bank contacted her and asked relevant questions of Miss Y, it would have been apparent that she was falling victim to a scam. In other words, but for HSBC's failure to make further enquiries, it would have been on actual notice that Miss Y was going to suffer financial harm from fraud.

I accept that there wasn't an FCA warning in place about Expertcryptomining.com. But there is anecdotal evidence online of others who have been scammed by the merchant. Miss Y is also not an experienced investor. So, had HSBC provided her with a warning it would have likely alerted her to the common issues arising in relation to cryptocurrency scams which, in turn, would have led her to second guess the broker's credentials and why she was being asked to invest more money. The result of this is that it would have likely stopped Miss Y from making any further payments on her debit and credit cards.

Therefore, I'm satisfied that HSBC can fairly and reasonably he held responsible for the loss Miss Y has suffered, as I think they could have ultimately prevented it.

Contributory negligence

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 Y was to blame for what happened. HSBC have said that Miss Y's initial dishonesty should result in a finding of contributory negligence and a reduction in her total award. But while I'm sympathetic to HSBC's position given that Miss Y has clearly misled them, it cannot be said that her dishonesty ultimately *contributed* to her loss. Her money had already been lost by the time she gave the false story to HSBC, so it would not have made a difference to the amount she lost as the scam had already happened. Therefore, I do not think it would be appropriate to make a reduction in redress for contributory negligence on this basis.

I appreciate there is also an argument to say that Miss Y ought to have carried out more thorough due diligence and checks on the merchant before investing her money. But Miss Y is not an experienced investor. She would not have known to check sources such as the FCA's watchlist or the IOSCO investor alerts portal. And even if she did, she wouldn't have found any warnings about the merchant either. So, even if she had carried out further research, she may not have likely found anything at the time that would have alerted her to the fact that it was a scam.

Miss Y has said that she was shown convincing testimonials and even spoke to other 'investors' who had successfully made money with the merchant, which would've provided her with reassurance that it was a legitimate investment opportunity. So, overall, I do not think Miss Y could have foreseen the risk that the company she was dealing with was a scam, and I do not think it would be fair to reduce compensation on the basis that she should share blame for what happened.

My final decision

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

- Refund Miss Y the disputed payments she made from her debit card, from the second payment she made on 6 January 2021 onwards (totalling £16,879.97).

- As this was a current account, HSBC should also add interest to this sum (less any tax properly deductible) at 8% simple intertest per year from the respective dates of loss to the date of settlement.

- Refund Miss Y the £651.35 loss incurred from her credit card as a result of the payment she made as part of the scam, and rework her account to reimburse any interest and charges levied as a result, as though the payment had not taken place

- Pay 8% simple interest per year on any payment Miss Y made towards the credit card balance as a result of the scam, from the date she paid them to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss Y to accept or reject my decision before 15 July 2022.

Jack Ferris

Ombudsman