

## The complaint

Ms M complains about HSBC UK Bank Plc.

She says that HSBC didn't do enough to protect her from becoming the victim of a scam and would like HSBC to pay her back the money she has lost.

## What happened

Ms M was contacted by phone by an individual offering an investment opportunity in cryptocurrency. She was persuaded to invest an initial sum of £250 from a different bank and it seemed to be making profit, so she made further payments from her HSBC account totalling £81,000.

When Ms M realised she had been the victim of a scam, she made a complaint to HSBC. HSBC didn't uphold her complaint, so Ms M referred her complaint to this Service.

Our Investigator didn't uphold the complaint, but Ms M disagreed, so the complaint was passed to me to make a decision.

I have previously issued a provisional decision on this complaint where I explained I intended to partially uphold Ms M's complaint.

Ms M accepted my provisional decision, but HSBC did not. It provided further commentary that it asked me to consider. While I have considered what it said, it hasn't led me to alter my provisional decision, although I will comment on what it said.

So, I now issue my final 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.

Having done so, I'm partially upholding Ms M's complaint. I'll explain why.

### *Was Ms M the victim of a scam?*

I don't think it is in doubt here that Ms M was the victim of a scam – she was contacted out of the blue by someone offering investment in crypto and was persuaded to download Anydesk onto her computer. She was also provided with false identification documents from her supposed 'account managers' and when she came to withdraw her supposed profit was told that this was not possible unless she paid a 'security deposit' which she did.

Ms M made the following payments as part of the scam.

Date	Payee	Payment type	Amount
------	-------	--------------	--------

11 January 2022	S	Bank transfer	£25,000
28 January 2022	S	Bank transfer	£15,000
30 March 2022	N	Bank transfer	£50
1 April 2022	N	Bank transfer	£14,950
4 April 2022	N	Bank transfer	£13,000
5 April 2022	N	Bank transfer	£13,000

*Did Ms M authorise the payments?*

In line with the Payment Services Regulations 2017 (PSRs), Ms M isn't liable for payments she didn't authorise, unless she failed with gross negligence or intent to comply with the terms of the account or keep her personalised security details safe.

Ms M says that she didn't authorise the payments – but I think that she did. I say this because she spoke with HSBC on three occasions and confirmed that she wanted to make the payments. The initial payments Ms M made were also instigated by her using her own online banking to make the payment to the seller of the crypto she bought on the scammer's instruction.

I understand Ms M had been tricked into instructing HSBC to make the payments – but while Ms M never intended the payments to go to the scammers, this doesn't change the fact she authorised them and is therefore presumed liable for the loss in the first instance.

*Recovery of Ms M's payments*

After Ms M made her payments, I wouldn't expect HSBC to do anything further until it was notified of the scam.

The payments were all made via bank transfer – so HSBC could have asked the receiving business to return the funds – however, I don't think that it would likely have been successful here.

This is because S and N are legitimate crypto exchanges and provided the services that Ms M requested – the purchase of crypto and subsequently moving that crypto onto a wallet of Ms M's choosing. What happened after that crypto was successfully moved is therefore a separate matter.

*Should HSBC have reasonably prevented the payments in the first place?*

I can only uphold this complaint if I think that HSBC reasonably ought to have prevented some or all of the payments Ms M made in the first place – therefore preventing the loss before it happened.

Ms M authorised the scam payments in question here – so as I've explained above, she is presumed liable for the loss in the first instance.

That said, as a matter of good industry practice, HSBC should have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions

– that could involve fraud or be the result of a scam. However, there is a balance to be struck: banks had (and have) obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't reasonably be involved in every transaction.

Taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider having been good industry practice at the time, I consider HSBC should fairly and reasonably:

- Been monitoring accounts – including payments made and received – to counter various risks including anti-money laundering, countering the financing of terrorism and preventing fraud and scams;
- Have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer; and
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

This leads me to consider the payments that Ms M has made – and if HSBC should have intervened.

The first payment that Ms M made from her HSBC account was for £25,000. This is a significant amount of money. While I understand that Ms M has made another payment of £50,000 around six months prior to this transaction, this appears to be an account in her own name, whereas this payment was going to a seller of crypto.

HSBC say that the £50,000 payment went to an account in a slightly different name – but even if the name is slightly different or if it is to a family member, it was still going to an individual, and not a seller of crypto.

HSBC also goes on to say that Ms M made payments of £13,000 and £16,603.05 – which are similar to some of the payments Ms M made to the scammer. But again, the £13,000 was to the same account as the £50,000 – and the £16,603.05 was to repay a loan account. All of these transactions also took place six months before the scam took place – so I don't think that they can be used to establish a 'normal' pattern of spending for Ms M.

So I think that this payment was unusual - and should've stuck out to HSBC as being uncommon considering the way in which Ms M generally used her account, especially given that by January 2019, HSBC should already have had a good understanding about how scams like the one Ms M fell victim to work.

With this in mind, HSBC should reasonably have contacted Ms M to establish whether the transaction posed any possibility of placing Ms M in financial harm before processing it. But it did not do so. Had HSBC done so, I would've expected it to have questioned Ms M about the payment she was making – including what she was making the payment for and surrounding context and to proceed accordingly. The intention being to disrupt or uncover a potential fraud or scam.

Similarly, when Ms M made the second payment for £15,000, HSBC did not intervene in this payment either – and I think that it should have.

HSBC has commented that this approach would require its automated payment systems to pick up the payment in real time, and that as they were made by 'Bill Payment' not by card

that there would not be a merchant code indicating the payment was going to crypto. It also says that the payments were spaced out and that not all payments to crypto are fraudulent. But as I have explained, it should have intervened from the first payment – so even if the payments were spread out, this doesn't make a difference. And while not all payments to crypto are fraudulent, it still had a duty to protect Ms M, and these payments were for significant amounts of money.

It is also clear that these types of payments *can* be picked up in 'real time' as HSBC did contact Ms M when she made the payments of £14,950, and the two payments of £13,000.

HSBC has provided copies of these calls, and I do think that HSBC questioned Ms M appropriately about the payments she was making – this included asking Ms M if she had been contacted by anyone, if she had been coached by anyone, and been told to lie to HSBC. It also told her about the types of scams it sees involving crypto. But Ms M was not truthful with HSBC.

Ms M has explained that by this point, she has already invested just over £40,000 – and was anxious not to lose her money. She had been coached by the scammer – and was now being told that she needed to make further investment in order to access her supposed profit and original investment.

That said, had HSBC intervened from the initial payment – I do think that its questions and warnings would have had a greater impact on Ms M – she had only invested £250 so far, and the payment for £25,000 was a very large sum of money. And I think that an intervention at this point would have altered the way that Ms M acted at this time. HSBC could have given Ms M an explanation about scams involving crypto – and how they commonly work – for example being asked to download software such as Anydesk, the use of fake trading platforms and inability to withdraw funds or only being able to make negligible withdrawals, plus being asked to pay more funds to remove money.

HSBC could also have explained that often there is pressure to pay more, and quickly – and that unrealistically quick and large promises of profit also indicate a scam. It could also have directed Ms M to the Financial Conduct Authority's (FCA's) scam smart webpage, given the large amount of money Ms M was about to part with, and I think it's likely she would have made further checks before doing so – or divulged more information to HSBC that she ultimately did when it questioned her later on and had already paid out a large sum of money.

HSBC says that more weight should be placed on the fact that Ms M wasn't truthful with it when she spoke to them, so it's likely that she would have done so had it intervened earlier as she was likely determined to make the payments. It also says that she had previously invested from elsewhere and thought that she was achieving profits.

But it is not just the effectiveness of the warning – but timing too. As I've explained above, by the time HSBC intervened with the payments, she has been told that she needed to pay more money in order to access her original investment, and understandably she was anxious not to lose her money having invested so much by this point. The earlier investment was also only £250 – and Ms M hadn't been told that she needed to pay more to get it back yet. So, I don't think that this makes a difference here.

And so, I do feel that HSBC missed an opportunity to uncover the scam and prevent the loss from the first payment that Ms M made.

*Should Ms M bear some responsibility for the loss?*

While I do consider that HSBC should have prevented the payments from the outset, I do need to consider if Ms M should bear some responsibility for what happened here by way of contributory negligence.

As I've explained above, HSBC did miss an opportunity for intervene, and stop the payments from the outset, before Ms M became entrenched in the scam – and so the later payments would never have been made. However, when it did intervene, Ms M did not co-operate.

So even though I think that payments four onwards should never have happened, I do think that Ms M should bear some responsibility, as she misled HSBC about the nature of the payments. And so, I think that it would be fair that responsibility for these payments should be split between HSBC and Ms M on a 50% basis.

I understand that HSBC feels that Ms M should at least bear 50% of all the payments that were made. It doesn't feel that she was as careful as she should have been when dealing with the scammers. It considers she took risks with her money, and that she jumped from paying £250 to £25,000. It also says Ms M provided Trustpilot reviews to it of the company which are negative – and that some negative reviews were there before Ms M made the transactions.

However, there were also some positive reviews at the time, and I can't be certain when Ms M came across the reviews – before or after she was scammed. And Ms M wasn't an expert here – and the information she was given by the scammer appears like it would have been convincing to someone without experience. The scammers provided her with brochures, authentic looking identity documents and also a contract to sign, along with requiring her to supply her own identification documents. Again, HSBC was the expert in these matters, not Ms M. And I consider the above proportion of blame to be fair in the circumstances.

### **Putting things right**

HSBC should pay Ms M 100% of the first three payments. I calculate this to be £40,050.

HSBC should also pay Ms M 50% of the next three payments. I calculate this to be £20,475.

HSBC should also pay Ms M 8% simple interest (minus any lawfully deductible tax) from the date the payments were made until the date it makes payment to Ms M.

### **My final decision**

I uphold this complaint in part.

HSBC UK Bank Plc should put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 7 July 2023.

Claire Pugh  
**Ombudsman**