

The complaint

Miss M complains that HSBC UK Bank Plc has unfairly refused to refund her losses after she fell victim to a scam.

Miss M is represented in her complaint by a professional third party but for ease I will refer to Miss M throughout.

What happened

Miss M says that when browsing online for ways to make money, she came across an investment company I will refer to as GT. Miss M says she carried out some research and thought that GT appeared legitimate. Miss M says that GT appointed an account manager who seemed very professional. Miss M told the account manager that she already had an account with a cryptocurrency merchant, and they told her to open accounts with various other cryptocurrency merchants.

Miss M sent money from her HSBC account to other cryptocurrency accounts set up in her own name. From there, money was forwarded on as part of the investment scam. Miss M says she realised she had been scammed when she tried to withdraw funds and was asked to pay withdrawal fees.

Miss M made the following disputed payments. The merchants identified on the table below as CE, C and CB are cryptocurrency merchants. The merchant identified below as G, is the merchant which GT asked Miss M to make an initial payment to. And the merchant identified as F is referred to in more detail later in my decision.

No.	Date	Type of transaction and merchant	Amount £
1	08/01/2021	Debit card payment - F	250
2	20/01/2021	International debit card payment - G	183.72
3	21/01/2021	Debit card payment - CE	2,050
4	04/02/2021	Debit card payment - CE	3,700
5	10/02/2021	Debit card payment - F	2,000
6	17/02/2021	Debit card payment - F	1,200
7	23/02/2021	Debit card payment - CE	2,000
8	01/03/2021	Debit card payment - F	500
9	01/03/2021	Debit card payment - F	500

10	03/03/2021	Debit card payment - CE	8,000
11	04/03/2021	Debit card payment - F	500
12	26/03/2021	Debit card payment - CE	1,000
13	10/05/2021	Debit card payment - C	6,060
14	16/06/2021	Debit card payment - CB	9,000
15	17/06/2021	Debit card payment - CB	3,000
16	17/06/2021	Debit card payment - CB	3,000

Our investigation so far

Our investigator upheld this complaint. He thought that by payment 10, HSBC should have been concerned when Miss M made the payment of £8,000 to an identifiable cryptocurrency merchant. Our investigator thought that if HSBC had asked Miss M appropriate questions about the payment, it would have uncovered the scam at this point.

Our investigator thought that HSBC could have prevented Miss M's loss from 3 March 2021. As our investigator thought that Miss M missed several red flags, he asked HSBC to refund 50% of the payments marked 10 onwards in the above table.

Miss M agreed with the investigation outcome but HSBC did not. In summary, it said:

- Miss M had made a debit card payment of £25,000 to NS&I a few months before she paid CE £8,000 so the transaction didn't seem unusual.
- Miss M had previously made payments to CE, so it was a known beneficiary.
- Miss M hadn't referred to the credits she received from the scammer in April 2021 totaling £3,231.
- Miss M had received invested sums larger than £8,000 plus the fact she was paying and receiving credits from NS&I indicated that she was experienced with investments.

As HSBC didn't agree with the investigation outcome, Miss M's complaint came to me to decide. Although I was minded to uphold the complaint, I didn't agree that HSBC should refund transaction 11. So, I issued a provisional decision on 18 June 2025 which said:

The Contingent Reimbursement Model Code doesn't apply in this case because Miss M carried out the transactions using her debit card.

In deciding what's fair and reasonable in all the circumstances of a complaint, I am required to take into account relevant: law and regulations; regulators' rules, guidance, and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Although we don't have a complete set of messages and chats between Miss M and the scammer, we do have copies of the dispute declaration forms which she

completed and sent to HSBC between mid-2021 and early 2022. These detail the basis on which Miss M had been scammed by GT. Also included are some messages detailing Miss M's attempts to cash out her investment in July 2021, together with a copy of the authorisation she gave to GT to make some early payments. So, I don't think it is in dispute here that Miss M was taken in by a scam – and while she never intended her money to end up with a scammer, she authorised the payments – and so is presumed liable in the first instance.

In broad terms, the starting position at law is that a bank such as HSBC, is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations 2017 and the terms and conditions of the customer's account. And I have taken this into account when deciding what's fair and reasonable in this complaint.

That said, as a matter of good 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 like HSBC need to be alert to fraud and scams and to protect their customers from fraud, but they can't reasonably be involved in every transaction.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams.*
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among 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.*
- 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.*
- Have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example, the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers when deciding whether to intervene.*

In this case, I need to decide whether HSBC acted fairly and reasonably in its dealing with Miss M when she authorised payments from her account or whether it could and should have done more before processing them.

Should HSBC have recognised that Miss M was at risk of financial harm from fraud?

While there are known fraud risks associated with cryptocurrency, this does not mean that all transactions involving cryptocurrency are related to scams. And HSBC must strike a balance between allowing customers to use their account and stopping and questioning transactions.

In the context of Miss M's account and HSBC's responsibilities, payments 1 - 9 don't seem sufficiently out of the ordinary for her usual spending to have prompted HSBC to intervene. Unlike with a typical cryptocurrency investment scam, the transactions were spread out over the course of a couple of months. Given the value of the transactions and the period of activity, I don't think HSBC missed any obvious signs that Miss M might be falling victim to a scam until she attempted to pay £8,000 to CE on 3 March 2021.

The £8,000 payment was going to an identifiable cryptocurrency merchant. And the value was higher than any of the previous payments Miss M had made. I think that a proportionate intervention at this point would have been for HSBC to speak with Miss M. The purpose of this would have been to find out more about what she intended to do with the funds after she had paid CE. This could have included questions about her understanding of how the investment worked, how she had found out about the investment and if anybody was helping in the background. The intention being to disrupt or uncover a potential fraud or scam.

I think an intervention of this kind would have made a difference because I don't have evidence to suggest that Miss M would have lied about the investment. So, if HSBC had asked some probing questions about the purpose of the March 2021 transaction (with the benefit of its knowledge about the known risks at the time of investing in cryptocurrency) I think it likely that it would have uncovered the scam.

I take HSBC's point that Miss M had already made three lower value payments to the same cryptocurrency merchant, so CE was a known beneficiary with less risk attached to it. But this overlooks the fact that Miss M – a customer who before January 2021 had not made cryptocurrency transactions – was suddenly wanting to make a large payment to CE, without HSBC trying to establish what the payment was for.

HSBC also says that Miss M had previously made payments to and received sums from NS&I which would indicate she was experienced with investments. But I don't agree with this assumption. There is a big difference between investing money with NS&I and investing in cryptocurrency. One is a secure way to save money backed by HM Treasury and the other is a potentially risky investment with no guaranteed returns. So, I don't consider the fact that Miss M had previously paid £25,000 to NS&I meant that she was necessarily an experienced investor. But even if Miss M was an experienced investor, she wasn't experienced in investment scams. As the expert, HSBC should have done more to help protect her from the risk of harm from financial fraud.

Taking account of HSBC's objections to upholding this complaint, I still think that it missed the opportunity to prevent Miss M's losses from transaction 10 onwards save for transaction 11 – the payment to F for £500 and I will explain why below.

Transactions involving F

The transactions in favour of F, relate to a firm based abroad which offered high risk contracts for difference to investors in the UK. F was not a cryptocurrency merchant like the other merchants identified on the above table. In early 2021, the FCA stopped F from conducting regulated activities in the UK. The FCA required F to close all of its trading positions and refund money to its customers.

In mid-April 2021, Miss M received refunds from F totalling £3,231 around the time when the FCA issued a press release detailing the actions it had required of F. So, it

seems likely to me that Miss M received these refunds as part of the FCA's requirements of F, rather than as refunds from the scammer.

Because our service deals with other complaints about payments made to F, I know that although F offered a high-risk investment opportunity to customers, we don't usually consider that it was operating a scam. So, I don't think it reasonable to include any transactions made to F as part of the loss Miss M incurred because of the scam involving GT.

My view that the payments to F don't form part of the same scam with GT is reinforced by the dispute declaration forms which Miss M submitted to HSBC in 2021 and 2022. The form dated 5 August 2021, says that the first scam transaction was made on 20 January 2021. I cannot see that she referred to the payments to F at any point in the dispute declaration forms. Miss M also made other payments to F which don't form part of her complaint against HSBC - £750 on 13 January 2021 and £250 on 18 February 2021.

Miss M has also provided a document which she signed electronically that is headed with GT's name. The document confirms Miss M's understanding that she was authorising two payments on 19 and 20 January 2021, with the purpose of funding her personal trading account at GT. Again, this indicates that the scam payments started later than 8 January 2021.

Given the passage of time, I can appreciate why Miss M included the transactions with F as part of her complaint. But taking all of the above factors, I consider it more likely than not that the payments made to F do not form part of the same scam involving GT. This means that HSBC doesn't need to refund payment 11 on the above table.

It also follows that HSBC cannot off set the refunds which Miss M received from F in April 2021 against any refund of disputed transactions, as they don't relate to the scam involving GT.

Should Miss M bear any responsibility for her losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that as a layman without significant investment experience, Miss M may have found parts of the scammer's explanation of the investment to be persuasive but there were elements about the scam that ought to have caused her to be concerned. For example:

- Miss M says that she looked G up online but appears to have overlooked several online reviews posted on one of the largest review sites warning that G was operating a scam.*
- The scammer put pressure on Miss M to deposit further sums to benefit from a significant reduction in swap charges. This seems unusual behavior for a purportedly legitimate investment business.*
- Although Miss M found a similarly named company as G registered at Companies House, it didn't exactly match the name she understood she was investing with. So, it seems that she decided to invest large sums of money*

based on insufficient research.

- *The scammer asked Miss M to download software giving it remote access – not something I would have expected a legitimate business to require of her.*
- *The scammer asked Miss M to make payments to multiple parties.*

So, I agree with our investigator that Miss M needs to bear a shared responsibility for her losses here. Balancing her role in this with the fact HSBC failed to intervene appropriately, I think 50% is a fair deduction to the amount reimbursed. Miss M has already accepted our investigator's recommendation on this point.

Recovery

I can't see that HSBC could have successfully raised a chargeback on Miss M's behalf as while I accept she was deceived by the scammer; the disputed transactions were separate to this. Miss M instructed the cryptocurrency merchants to use her funds to buy and then send on cryptocurrency. They fulfilled this request, so Miss M received the services she paid for.

I then said I would require HSBC to refund 50% of transactions 10 and 12-16 together with interest at 8%.

Further submissions

Miss M accepts my provisional decision. HSBC says that as a gesture of goodwill it will settle the complaint in line with my provisional decision. However, it doesn't agree that my proposed outcome is fair for the reasons it previously gave. In particular it says that the payment of £8,000 on 3 March 2021 didn't present an identifiable scam risk given Miss M's history of making larger payments and as the payment went to a known beneficiary.

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 note HSBC's objections, but I still think the payment of £8,000 going to an identifiable cryptocurrency merchant should have prompted it to intervene. As HSBC agrees to settle the complaint in line with my provisional decision and as Miss M accepts my proposed outcome, I find it reasonable to make my final decision along the same lines as my provisional decision.

Putting things right

To put things right, HSBC should:

- Refund 50% of the transactions marked 10 and 12 - 16 on the table set out above; and
- Pay 8% interest on the refunded transactions from the date of loss to the date of settlement.

My final decision

My final decision is that I uphold this complaint and require HSBC UK Bank Plc to put things

right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 19 August 2025.

Gemma Bowen
Ombudsman