

The complaint

Ms H is unhappy that HSBC UK Bank Plc trading as First Direct won't refund the money she lost as part of a romance scam.

Ms H has appointed a representative to bring her complaint, but for ease, I will refer to Ms H throughout.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again in detail. Briefly, Ms H fell victim to a romance scam in February 2022 after she met an individual on a dating website.

The scammer gave Ms H various stories about his card not working or needing money for health care while working abroad. The scammer also asked Ms H to take out various loans, which she agreed to. Ms H finally realised that she had been the victim of a scam when the individual concerned asked her to send money to help him after he'd been arrested.

Ms H made the following payments from her First Direct account:

Transaction	Date	Type of transaction and merchant	Amount £
1	27 February 2022	International card payment to Rapido	21.49
2	3 March 2022	International card payment to Rapido	26.49
3	5 March 2022	International card payment to Rapido	21.49
4	9 March 2022	International card payment to Mobiletopup	101.49
5	9 March 2022	International card payment to Mobiletopup	21
6	11 March 2022	International card payment to Mobiletopup	49
7	11 March 2022	International card payment to Mobiletopup	51.49
8	21 March 2022	International card payment to Mobiletopup	40.48
9	21 March 2022	International card payment to Mobiletopup	6.49

10	21 March 2022	International card payment to Mobiletopup	26.49
11	21 March 2022	International card payment to Mobiletopup	51.49
12	21 March 2022	Card payment to CB Payments Ltd	75
13	23 March 2022	Card payment to CB Payments Ltd	150
14	26 March 2022	International card payment to MoonPay	2,606.04
15	27 March 2022	Card payment to CB Payments Ltd	156
16	28 March 2022	Card payment to Blockchain.com	1,200
17	28 March 2022	Card payment to Blockchain.com	228
18	28 March 2022	Transaction fee	6.27
19	28 March 2022	Card payment to Blockchain.com	1,200
20	28 March 2022	Card payment to Blockchain.com	159.50
21	28 March 2022	Card payment to Blockchain.com	228
22	28 March 2022	Transaction fee	6.27
23	28 March 2022	Card payment to Blockchain.com	255
24	28 March 2022	Transaction fee	71.67
25	31 March 2022	Card payment to CB Payments Ltd	125.35
26	2 April 2022	Card payment to Blockchain.com	5
27	2 April 2022	Card payment to Blockchain.com	157.50
28	7 April 2022	Card payment to Blockchain.com	32
	9 April 2022	<i>Transfer payment to an individual</i>	9,650
29	9 April 2022	International card payment to Mobiletopup	202.98
30	14 April 2022	International card payment to Mobiletopup	51.49
31	18 April 2022	Card payment to Blockchain.com	50
32	20 April 2022	Card payment to Blockchain.com	50
33	25 April 2022	Card payment to Blockchain.com	315

34	25 April 2022	Card payment to Blockchain.com	1,200
35	25 April 2022	Card payment to Blockchain.com	906
36	26 April 2022	Card payment to Blockchain.com	505
37	25 April 2022	International card payment to MoonPay	50
38	29 April 2022	Card payment to Blockchain.com	50
39	7 May 2022	Card payment to Blockchain.com	83
	23 June 2022	<i>Refund from First Direct</i>	9,650

Our investigator didn't uphold Ms H's complaint. She noted that Ms H didn't complain about payments 8-11 and 25. Although Ms H said she made a payment of £9,650 as part of the scam, First Direct had already refunded this to her, so it didn't form part of her current complaint.

Our investigator explained that First Direct could not consider the disputed card payments under the Contingent Reimbursement Model (CRM) Code.

Our investigator thought that payments 1-15 were small value payments to legitimate merchants and in line with Ms H's usual account activity. So, she wouldn't have expected these payments to trigger further checks by First Direct.

First Direct told our investigator that it stopped a couple of payments on 26 March 2022. Our investigator listened to the calls Ms H had with First Direct about these transactions. Our investigator didn't think a pattern of fraud had been established at this point. She thought First Direct's intervention – to ask whether the transactions were genuine – was proportionate to the value of the payments. So, our investigator didn't think that First Direct missed an opportunity to prevent further payments to the scammer.

Our investigator didn't think that payments 16 – 28 should have triggered an intervention from First Direct given they were made to existing beneficiaries and the cumulative values of any multiple payments were not high enough to have been of concern.

Our investigator didn't think that First Direct's intervention when she tried to make the payment of £9,650 was proportionate. Although First Direct gave Ms H an online warning to alert her to the possibility of a scam which included 'not paying someone she had recently met online,' our investigator thought First Direct should have stopped the payment and spoken to Ms H. However, our investigator wasn't persuaded that this would have made a difference to First Direct processing the transaction or subsequent payments. This is because our investigator was satisfied that Ms H was under the spell of the scammer and had discussed various scenarios to mislead lenders. So, even if First Direct had questioned Ms H further about the payment of £9,650, our investigator thought it unlikely that she would have been truthful about it.

For the same reasons that our investigator thought the earlier payments wouldn't have triggered further checks, she didn't ask First Direct to take any action in relation to payments 29 – 39.

As the disputed payments were made by debit card, our investigator considered whether

First Direct should have tried to use the chargeback process but didn't think this would have been successful.

Ms H disagreed with the investigation outcome. She thought it was poor practice to impose an arbitrary payment limit when considering whether a business should have detected fraudulent payments.

Ms H didn't think that by stopping a few payments, First Direct went far enough. Ms H thought that as she made multiple payments to a cryptocurrency exchange on some days, First Direct should have enacted the Banking Protocol.

Ms H thought that with an earlier intervention, First Direct could have prevented payments 16 – 28 and 29-39.

As Ms H doesn't agree with the investigation outcome, the complaint has come to me to make a 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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I am required to consider 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.

The CRM Code doesn't apply in this case because it does not cover card payments.

I don't think it is in dispute here that Ms H 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 First Direct, 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, First Direct 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 First Direct 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.

Considering 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 First Direct 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 First Direct acted fairly and reasonably in its dealing with Ms H when she authorised payments from her account or whether it could and should have done more before processing them.

I am sorry to disappoint Ms H but I would not have expected most of the disputed card payments to have prompted First Direct to intervene. I say this as most of the payments were made to legitimate merchants for small amounts. Although multiple payments were made on a couple of days, the cumulative value of the payments remained relatively modest. And payments made to cryptocurrency accounts aren't always made because of a scam.

There was a point around 26 March 2022 when First Direct stopped a couple of payments from Ms H's account. My understanding is that this was because First Direct blocked an earlier payment to a cryptocurrency merchant on 24 March 2022 for around £5,800. As Ms H didn't confirm the payment was genuine, it didn't go through. Although a few subsequent payments were held up, I agree with our investigator that First Direct's checks – to ask whether the payments were genuine – were proportionate to the amounts involved. So, I don't think First Direct missed the opportunity to prevent the scam at this point. Even if it had intervened, for the same reasons as I go on to outline below, I don't consider an intervention would have uncovered the scam.

I agree that First Direct should have done more to intervene when, on 9 April 2022, Ms H made the payment from her account to an individual for just under £10,000. Although First Direct displayed an online warning, given the value of the payment a proportionate intervention should have involved speaking with Ms H. However, like our investigator concluded, I don't consider a proportionate intervention by First Direct would have led Ms H to decide not to make payments 29 – 39 and will explain why.

From reading the messages which Ms H has kindly supplied, I can see that the scammer showered her with daily compliments and promises to fly to the UK. The scammer asked Ms H for small amounts of money before pushing her to take out credit to help him. In one message, Ms H asked the scammer not to mention the money she had lent to him to her friends and family as they would be shocked about it. Ms H told the scammer that she was the only one who really knew him and his intentions.

When it came to taking out loans, the scammer coached Ms H to lie about their purpose. He talked about working on Ms H's credit and said that lenders would want to know why she needed the money. Ms H suggested she use home improvement as the reason for needing to borrow money. The scammer said this would work but also talked about Ms H telling the lender she needed the money for a sick relative. The scammer coached Ms H to install a cryptocurrency app – sharing screenshots and options to choose for payment. There was also a point when First Direct declined some transactions in late March 2022, so Ms H and the scammer discussed splitting payments into smaller transactions.

The messages show that Ms H trusted the scammer implicitly. She followed his instructions and was prepared to mislead her bank and other lenders. Despite Ms H picking up on several inconsistencies in the scammer's story – such as his addresses in the UK, and changes to his profile name - he was able to reassure her every time. The scammer often pressured Ms H into agreeing to make payments on the basis he was alone, hungry, or injured. Ms H appeared to be under the scammer's spell, so I am not persuaded that a proportionate intervention by First Direct in April 2022 would have uncovered the scam.

Ms H has also referred to the Banking Protocol, but this only applies to payments made in branch in situations when branch staff have concerns that a customer may be falling victim to a scam. Even if the payments were made in branch, I don't consider First Direct would have had any obligation to invoke the Banking Protocol. This is because, as I have outlined above, I don't consider the payments were so unusual and out of character that First Direct ought to have intervened and asked questions about them.

Recovering the payments Ms H made

When payments are made by card – as was the case here – the only recovery option First Direct has is to request a chargeback. The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The scheme is subject to limitations and we would only expect a bank such as First Direct to raise a chargeback if there is a reasonable prospect of success.

Ms H didn't make the debit card payments to the scammer direct. Instead, she paid the money to accounts held in her name with third party merchants. So, First Direct could have only processed chargeback claims against the merchants Ms H paid. By carrying out transactions such as purchasing cryptocurrency or mobile top-ups, the merchants involved had provided the service Ms H requested. The fact that money was later transferred elsewhere to the scammer, didn't give rise to a valid chargeback claim against the merchants Ms H paid. So, any chargeback claim would likely have failed.

I have listened to some of the calls which Ms H had with First Direct when she reported the scam. I am satisfied that First Direct responded sympathetically to her situation.

I realise that my decision will be disappointing for Ms H who was cruelly tricked into placing her trust in the scammer. But I can't fairly say that First Direct could have prevented her loss, so I don't ask it to refund any of the payments she made.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 1 May 2025.

Gemma Bowen
Ombudsman