

The complaint

Mr R complains that HSBC UK Bank Plc (“HSBC”) won’t refund over £1.2 million he lost to two scams between June 2021 and May 2022.

What happened

Mr R fell victim to a cryptocurrency investment scam after he was contacted by Group 500 (“the scammer”) in June 2022 after registering his interest on their website.

The scammer instructed him to open various crypto wallets to send money to as part of the investment, where the funds were subsequently transferred on to the scammer. Mr R made the following payments from his HSBC account as part of the scam, either as part of the investment, or towards taxes and commission he was told he had to pay in order to access his profits:

Date	Payee	Amount	Method of payment used
22/06/2021	Binance.com	4,999.00	Card payment
22/06/2021	Binance.com	5,000.00	Card payment
23/06/2021	Binance.com	4,995.00	Card payment
23/06/2021	Binance.com	4,990.00	Card payment
24/06/2021	Binance.com	2,000.00	Card payment
24/06/2021	Binance	977.88-	Withdrawal
05/07/2021	Payward LTD	25,000.00	Transfer
14/07/2021	Payward Ltd	22,500.00	Transfer
20/07/2021	Payward Ltd	25,000.00	Transfer
22/07/2021	Payward LTD	10,000.00	Transfer
22/07/2021	Payward LTD	15,000.00	Transfer
23/07/2021	Payward LTD	20,000.00	Transfer
23/07/2021	Payward LTD	5,000.00	Transfer

11/08/2021	Payward LTD	24,999.00	Transfer
12/08/2021	Payward LTD	24,998.00	Transfer
13/08/2021	Payward LTD	24,997.00	Transfer
14/08/2021	Payward LTD	24,997.00	Transfer
01/10/2021	Payward LTD	25,000.00	Transfer
03/10/2021	Payward LTD	24,000.00	Transfer
04/10/2021	Payward LTD	23,000.00	Transfer
05/10/2021	Payward LTD	21,730.00	Transfer
06/10/2021	Payward LTD	2,500.00	Transfer
13/10/2021	Payward LTD	23,500.00	Transfer
14/10/2021	Payward LTD	25,000.00	Transfer
15/10/2021	Payward LTD	24,500.00	Transfer
17/10/2021	Payward LTD	25,000.00	Transfer
18/10/2021	Payward LTD	24,990.00	Transfer
19/10/2021	Payward LTD	23,857.15	Transfer
20/10/2021	Payward LTD	7,250.00	Transfer
19/11/2021	Payward Ltd	2,923.37-	Withdrawal
24/11/2021	Payward Ltd	2,942.71-	Withdrawal
26/11/2021	Payward LTD	24,999.00	Transfer
27/11/2021	Payward LTD	24,998.00	Transfer
28/11/2021	Payward LTD	3,500.00	Transfer
02/12/2021	Payward LTD	25,000.00	Transfer
02/12/2021	Payward Ltd	1,467.04-	Withdrawal
03/12/2021	Payward LTD	24,998.00	Transfer
04/12/2021	Payward LTD	9,000.00	Transfer
06/12/2021	Payward LTD	21,500.00	Transfer
13/12/2021	Payward LTD	25,000.00	Transfer

14/12/2021	Payward LTD	24,999.00	Transfer
15/12/2021	Payward LTD	24,975.00	Transfer
16/12/2021	Payward LTD	24,950.00	Transfer
17/12/2021	Payward LTD	24,795.00	Transfer
22/12/2021	Payward LTD	24,960.00	Transfer
23/12/2021	Payward LTD	24,850.00	Transfer
28/12/2021	Payward LTD	24,875.00	Transfer
29/12/2021	Payward Ltd	24,875.00-	Withdrawal
30/12/2021	Payward LTD	250.00	Transfer
30/12/2021	CB Payments Ltd	50.00	Card payment
03/01/2022	KN International	20,000.00	Transfer
04/01/2022	CoinJar	50.00	Transfer
04/01/2022	Coinjar	5.00-	Withdrawal
04/01/2022	CoinJar	9,945.00	Transfer
05/01/2022	CoinJar	9,985.00	Transfer
04/01/2022	CB Payments LTD	27.10	Card payment
04/01/2022	CB Payments LTD	21.61	Card payment
05/01/2022	CB Payments LTD	1,000.00	Card payment
06/01/2022	CoinJar	9,650.00	Transfer
07/01/2022	KN International	14,950.00	Transfer
08/01/2022	CoinJar	8,990.00	Transfer
09/01/2022	CoinJar	2,000.00	Transfer
10/01/2022	CB Payments LTD	118.00	Card payment
10/01/2022	CB Payments LTD	345.00	Card payment
12/01/2022	KN International	15,400.00	Transfer
12/01/2022	Doris Dax	2,500.00	Transfer
12/01/2022	Doris Dax	7,000.00	Transfer

13/01/2022	DS Keels Trading	24,900.00	Transfer
14/01/2022	CoinJar	6,250.00	Transfer
17/01/2022	CoinJar	3,000.00	Transfer
17/01/2022	CoinJar	7,400.00	Transfer
17/01/2022	CoinJar	9,000.00	Transfer
17/01/2022	Cro	640.98	Card payment
18/01/2022	CoinJar	1,631.59-	Withdrawal from scammer
20/01/2022	CoinJar	5,313.33-	Withdrawal from scammer
28/01/2022	Foris Dax MT Limited	1,749.52-	Withdrawal from scammer
24/02/2022	CoinJar	1,300.00	Transfer
28/02/2022	CoinJar	24,769.00	Transfer
01/03/2022	CoinJar	22,000.00	Transfer
02/03/2022	CoinJar	24,980.00	Transfer
03/03/2022	Doris Dax	1,000.00	Transfer
03/03/2022	Doris Dax	14,050.00	Transfer
04/03/2022	CoinJar	6,000.00	Transfer
07/03/2022	CoinJar	8,500.00	Transfer
07/03/2022	CoinJar	4,000.00	Transfer
07/03/2022	CoinJar	2,500.00	Transfer
30/03/2022	CoinJar	24,690.00	Transfer
12/04/2022	CoinJar	24,890.00	Transfer
13/04/2022	Doris Dax	24,994.00	Transfer
14/04/2022	CoinJar	24,794.85-	Withdrawal from scammer
14/04/2022	Doris Dax	24,965.00	Transfer
15/04/2022	Doris Dax	24,997.00	Transfer

16/04/2022	Doris Dax	24,998.00	Transfer
26/04/2022	Doris Dax	17,500.00	Transfer
26/04/2022	CB Payments LTD	3,000.00	Card payment

Mr R realised he had been scammed after the broker's website and trading platform disappeared and he couldn't get in contact with anyone. In an attempt to try and recover his money, Mr R researched companies that could help recover financial losses. He found a company called "Spright Vestige" ("the second scammer") who said they would be able to recover his money from Group 500.

Mr R was told he would have to pay an advanced fee for the company's services, as well as several other payments for things like decrypting his trading wallet and verifying his account. The second scammer instructed him to open another crypto wallet and he preceded to make the following payments from his HSBC account:

Date	Payee	Amount	Method of payment used
07/05/2022	Doris DAX MT Limited	11,995	Transfer
15/05/2022	Doris DAX MT Limited	24,999	Transfer
16/05/2022	Doris DAX MT Limited	12,541	Transfer
16/05/2022	Doris DAX MT Limited	2,750	Transfer

After making these payments, Mr R was told that he wouldn't be able to withdraw his funds as they had come from a fraudulent address. He realised he had been scammed again after he was told he would need to invest 10% of the value of the funds in order to "clean the wallet". He reported both scams to HSBC on 25 May 2022.

HSBC refused to refund any of the payments Mr R had lost to the scam. It said that it had spoken to Mr R in relation to several payments throughout the scam but that he had misled the bank as to their true nature. So, HSBC said that any further intervention it could have made would have made no difference in the prevention of the scam.

HSBC acknowledged that four payments Mr R made as part of the scam (to KN International and DS Keels Trading) were made to another person, and to a UK account, such that they would be covered by the Contingent Reimbursement Model (CRM Code). However, it didn't consider Mr R had a reasonable basis for believing the payments to be genuine. So, it said he wouldn't be eligible for a refund.

Our investigator upheld the complaint in part. He didn't think HSBC was liable to refund any of the payments that were not covered under the CRM Code as Mr R had misled the bank when it asked him about the payments. So, he didn't think any further or earlier intervention would have likely revealed the scam. However, in terms of the four payments covered under the CRM Code, the investigator thought that HSBC should refund 50%. He didn't think that Mr R had a reasonable basis for believing the payments to be genuine, but also said that

HSBC hadn't shown that it had provided an effective warning in line with its own obligations under the Code.

HSBC accepted the investigator's findings and agreed to settle the complaint by reimbursing 50% of the payments covered under the CRM Code. Mr R disagreed. He thought that HSBC's intervention didn't go far enough and that it had missed an opportunity to prevent the scam when it spoke to him. As Mr R didn't agree, the matter has been escalated to me to determine.

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 satisfied that HSBC's offer to settle the complaint is fair and I'm not persuaded it would have to compensate Mr R any further. I'll explain why.

It isn't in dispute that Mr R has fallen victim to two cruel scams here, nor that he authorised the disputed payments he made from his HSBC account. The payments were requested by him using his 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. But I've considered whether there is any fair and reasonable basis for HSBC to reimburse any of the payments.

Payments not covered under the CRM Code

The vast majority of payments Mr R made as part of the scam unfortunately do not fall within the scope of the CRM Code for reimbursement. These include any card payments he made, as well as any bank transfers to his own crypto wallets (as the Code only applies where money is transferred to another person).

However, I've considered whether HSBC should have done more to prevent Mr R from falling victim to the scam outside its obligations under the CRM Code, 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.

It's common ground that some of the payments were considered unusual given that they did trigger the bank's fraud prevention systems and were automatically blocked pending further enquiry, including those made on 1 October 2021, and also on 4 and 7 January 2022. Accordingly, it's just a question of whether the bank went far enough in all the circumstances with its interventions.

Having listened to the call recordings of the occasions HSBC spoke to Mr R, I accept that it sometimes could have gone further in its questioning, and that there also may have been cause to intervene earlier. But even accepting this as the case, on balance, I'm not persuaded that any further questioning or earlier intervention would have ultimately uncovered the scam and prevented the loss.

I say this because Mr R said he had been told by the scammer to mislead the bank, and they had coached him on what to say if he was asked any questions. This was an issue which HSBC specifically warned about in a call on 7 January 2022. And I can see that when HSBC asked him about the nature of the payments on 4 January 2022, he did not say he was investing, and instead misled the bank and told it the payment was to set up a travel card for foreign currency to use abroad. HSBC also specifically asked Mr R if the payments were to fund investment trades in a phone call on 9 January 2022, which he denied and continued to

maintain it was just currency exchange.

It was based upon the answers Mr R gave that the bank was satisfied the payment wasn't likely being made as part of a scam. If he had answered the questions accurately and said he was in contact with a third-party broker and was investing in cryptocurrency, then I accept it would have been incumbent on HSBC to maintain suspicion about the payment and probe further into the circumstances. But seeing as Mr R was not forthcoming with these details, I don't think any further probing from HSBC would have likely revealed that he was being scammed.

I also note that when HSBC spoke to Mr R on 4 January 2022, it asked him if he had checked the FCA register to look up the company he said he was paying. He said that he hadn't but that he was willing to take the risk. So, even if Mr R had been honest about the nature of the payment he was making, any warning HSBC could have given him to do further research would have been unlikely to reveal the scam either.

So, in these circumstances, I don't consider it would be fair and reasonable to hold HSBC liable for Mr R's losses that are not covered by the CRM Code, because it seems more likely than not that he would have always made the payment to the scammers, notwithstanding any intervention made by the bank.

In terms of the second scam Mr R fell victim to, I don't consider there was any cause for HSBC to have intervened in these payments. They were going to a payee Mr R had paid before, and the amounts were not out of character when compared with his normal spending. So, I don't think HSBC can fairly be held liable for these payments either.

Payments covered under the CRM Code

As I've outlined above, four payments Mr R made as part of the scam would fall in scope for reimbursement under the CRM Code:

- 3 January 2022 - £20,000 to KN International
- 7 January 2022 - £14,950 to KN International
- 12 January 2022 - £15,400 to KN International
- 13 January 2022 - £24,900 to D Skeels Trading

HSBC has accepted that it did not provide an effective warning when Mr R was making these payments and has therefore agreed to reimburse 50% in line with the Code. As such, I do not intend exploring this point any further given it is no longer in dispute. What does remain in dispute, however, is whether Mr R had a reasonable basis for believing the payments he was making were genuine or going towards a legitimate investment.

Having considered the evidence, I'm not persuaded Mr R had such a reasonable basis of belief for the following reasons:

- Despite having previously made all his transfers directly to his crypto wallets, Mr R was instead asked to send money directly to other UK accounts. He says he was told that they were crypto brokers who would exchange the sterling to Bitcoin. Mr R has acknowledged that this was an odd request and I also think it ought to have given him cause for concern. There was no reason for him to have to suddenly start sending his money to a broker to exchange it to Bitcoin when he already had several crypto accounts where he could do this himself. There is also nothing to suggest that the companies he

was paying even offered such services, and neither was there any clear connection between these companies and Group 500 either.

- Mr R was told by the scammer to mislead the bank if he was questioned about the payments. If it was a legitimate investment being made through a legitimate broker, there would have been no reason for him to mislead the bank as to the purpose of the payment. And I think this ought to have given him cause for concern that something was not right.
- By the time Mr R came to make these payments in January 2022, He was under the impression that he had made £2.87Million, which would have represented an increase of over 300% in his trading account value. While I understand some people have made a lot of money from cryptocurrency, such returns should have still appeared wholly unrealistic and far too good to be true.
- Mr R was told by the scammer that they were upgrading his account to the “Millionaires Club”, which would give him 70% insurance against any future losses. Again, being told that he would have his investment losses indemnified to such an extent should have appeared too good to be true. The scammers were also misspelling well-known names such as “Goldman Sacs” in their correspondence with Mr R when discussing this.
- The scammer told Mr R there had been a crash in the market, prompting him to desperately invest over £250,000 in October to recoup his losses. However, there are no signs of any crash in Bitcoin value during this period, so it appears he did not do enough research to independently verify what he was being told by the scammer, where he could have easily discovered he was being misled.

So, I’m satisfied there was enough going on at the point Mr R was making these payments that should have given him significant cause for concern that something simply wasn’t right. Therefore, I’m not persuaded he had a reasonable basis for believing the payments were genuine and I don’t think HSBC needs to pay anything over and above the 50% it has already agreed to reimburse.

Recovery

I’ve also thought about whether HSBC could have done more to recover the funds Mr R lost. In terms of the payments covered under the Code, I can see that HSBC reached out to the beneficiary banks but was unable to recover any funds, which isn’t surprising given the amount of time that had passed between the payment being made and the fraud being reported.

In terms of the faster payments made to Mr R’s own crypto accounts, there would have been no prospect of recovering these funds either given we know they were subsequently transferred on to the scammer from those accounts. And finally, with regards to the debit card transactions, there would have been no reasonable prospect of a chargeback claim succeeding given Mr R would have received the asset he paid for (i.e. cryptocurrency). So, I’m not persuaded there was anything more HSBC could have done to recover the funds in these circumstances.

I appreciate this will likely come as a disappointment to Mr R, and I’m sorry he has been the victim of such a cruel scam. I do not underestimate the impact this must have had on him. However, for the reasons given above, I don’t think HSBC can fairly or reasonably be expected to reimburse anything over and above what it has already agreed.

My final decision

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

- Refund 50% of the payments Mr R made that I've listed above as being covered by the CRM Code.
- Mr R funded these scam payments via director's loans from his company account. He has not been able to provide evidence to demonstrate what rate of interest, if any, would be payable on these loans, so I will not be asking HSBC to pay any interest on this award.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 20 November 2023.

Jack Ferris
Ombudsman