DRN-6015467

The complaint

Mrs G complains that HSBC UK Bank Plc (HSBC) is refusing to refund her the amount she lost as the result of a scam.

Mrs G is being represented by a third party. To keep things simple, I will refer to Mrs G throughout my decision.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Mrs G has told us that she was invited via social media to consider an investment with a company I will call "X". Mrs G says that in hindsight a subtle drip-fed marketing strategy was used by X.

Mrs G says multiple video calls took place where the emphasis was on guaranteed returns and the safety of the investment. X advised Mrs G to open an account with a cryptocurrency exchange to facility payments into the investment.

Mrs G agreed to invest and made the following payments in relation to the scam:

Payment	Date	Payee	Payment Method	Amount
1	26 October 2021	Payward Ltd	Transfer	£8,500.00
2	27 October 2021	Payward Ltd	Transfer	£5,250.00
3	28 October 2021	Payward Ltd	Transfer	£4,750.00
4	21 November 2021	Payward Ltd	Transfer	£375.00
5	24 December 2021	Payward Ltd	Transfer	£1,200.00
6	26 December 2021	Payward Ltd	Transfer	£10,000.00
7	29 December 2021	Payward Ltd	Transfer	£130.00
8	4 January 2022	Payward Ltd	Transfer	£6,020.00
9	3 March 2022	Payward Ltd	Transfer	£220.00
10	8 March 2022	Payward Ltd	Transfer	£1,010.00
11	27 March 2022	Payward Ltd	Transfer	£5,000.00
12	27 March 2022	Payward Ltd	Transfer	£3,500.00
13	29 March 2022	Payward Ltd	Transfer	£3,200.00
14	30 March 2022	Payward Ltd	Transfer	£4,500.00
15	4 April 2022	Payward Ltd	Transfer	£5,000.00
16	4 April 2022	Payward Ltd	Transfer	£14,000.00
17	4 April 2022	Payward Ltd	Transfer	£1,500.00
18	7 June 2022	Payward Ltd	Transfer	£1,250.00
19	25 June 2022	Payward Ltd	Transfer	£750.00
20	29 June 2022	Payward Ltd	Transfer	£60.00
21	5 July 2022	Payward Ltd	Transfer	£2,660.00
22	14 July 2022	Payward Ltd	Transfer	£900.00
23	14 July 2022	Payward Ltd	Transfer	£75.00

24	15 July 2022	Payward Ltd	Transfer	£660.00
25	18 July 2022	Payward Ltd	Transfer	£1,300.00
26	22 July 2022	Payward Ltd	Transfer	£850.00
27	26 July 2022	Payward Ltd	Transfer	£90.00
28	01 August 2022	Payward Ltd	Transfer	£4,950.00
29	04 August 2022	Payward Ltd	Transfer	£1,000.00
30	15 August 2022	Payward Ltd	Transfer	£200.00
31	8 September 2022	Payward Ltd	Transfer	£350.00
32	30 September 2022	Payward Ltd	Transfer	£1,100.00
33	17 March 2023	Payward Ltd	Transfer	£120.00
34	9 April 2023	Payward Ltd	Transfer	£150.00
35	1 May 2023	Payward Ltd	Transfer	£2,000.00
36	21 May 2023	Payward Ltd	Transfer	£1,800.00
37	24 May 2023	Payward Ltd	Transfer	£705.00
38	29 May 2023	Payward Ltd	Transfer	£750.00
39	29 May 2023	Payward Ltd	Transfer	£350.00
40	26 June 2023	Payward Ltd	Transfer	£3,500.00
41	26 June 2023	Payward Ltd	Transfer	£500.00
42	12 August 2023	Payward Ltd	Transfer	£110.00

Our Investigator considered Mrs G's complaint and didn't think it should be upheld. Mrs G didn't agree, so this complaint has been passed 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 has not been disputed that Mrs G has fallen victim to a cruel scam. The evidence provided by both Mrs G and HSBC sets out what happened. What is in dispute is whether HSBC should refund the money Mrs G lost due to the scam.

Recovering the payments Mrs G made

Mrs G made payments into the scam via transfer. When payments are made by transfer HSBC has limited options available to it to seek recovery.

In any event all the payments Mrs G made in relation to the scam went to a genuine cryptocurrency exchange in exchange for cryptocurrency that was provided to Mrs G. As it took further steps for those funds to end up in the hands of the scammer any attempt to recover the payments would have no prospects of success.

I have considered if Mrs G should have received a refund under the Contingent Reimbursement Model (CRM) code. But the CRM code only applies when domestic payments (as the result of a scam) are sent to another person. Here Mrs G sent the payments to an account held in her own name and the scam occurred when she moved her purchased cryptocurrency from that account to the scammer. I'm satisfied the CRM Code wouldn't apply in this scenario.

Should HSBC have reasonably prevented the payments Mrs G made?

It has been accepted that Mrs G authorised the payments that were made from her account with HSBC, albeit on X's instruction. So, the starting point here is that Mrs G is responsible.

However, banks and other Payment Services Providers (PSPs) do have a duty to protect

against the risk of financial loss due to fraud and/or to undertake due diligence on large transactions to guard against money laundering.

The question here is whether HSBC should have been aware of the scam and intervened when Mrs G made the payments, and if it had intervened, would it have been able to prevent the scam taking place.

The payments Mrs G made in relation to the scam were made to a cryptocurrency exchange, and some of the payments were significant in value.

With the above in mind, I think HSBC should have had concerns when Mrs G attempt to make payment 1 and it should have intervened.

HSBC have confirmed that it did intervene when several of the payments in relation to the scam were made, and several calls took place between Mrs G and HSBC. HSBC has provided us with a copy of these call recordings.

When Mrs G attempted payment 1 a call between Mrs G and HSBC took place. Mrs G confirmed:

- She had seen online payment warnings and understood them.
- She had been using a different platform and was moving to the new exchange as it was cheaper to deposit and withdraw.
- She had not sought any advice as she didn't need it.
- She was aware the exchange was not FCA regulated and was "doing it knowingly".
- She was using a personal contact that she trusted.

When Mrs G attempted payment 2 a further call took place. Mrs G confirmed:

- She had not received a call or message from a third party.
- She found the account details for the payment online as it was her online account
- She found out about the investment from someone she knew personally
- She had not been pressured to make payments
- She had carried out her own due diligence.

When Mrs G attempted payment 3 a further call took place. Mrs G confirmed:

- What had prompted her to make the payment? – she was just making a payment to her own personal Cryptocurrency account, and no one had asked her to do it.
- She had been investing in cryptocurrency for a couple of years.
- She had carried out due diligence

Mrs G was warned that there were a lot of cryptocurrency investment scams and that criminals would advertise on social media and create fraudulent websites. Mrs G should not entertain them. Websites would look professional and could include celebrity endorsements.

Mrs G was further warned that scammers could ask her not to discuss the payments with the bank and that HSBC may not be able to help recover her funds. Mrs G then confirmed she wanted to make the payment.

The answers Mrs G provided to HSBC do not match the information she has provided to us. Mrs G said X used a subtle drip-fed marketing strategy via social media to invite her to take part in the investment. So, it had not been recommended to her by a friend.

Mrs G also told us that she was advised to open an account with the cryptocurrency exchange by X. In the calls Mrs G said she opened the account because it was cheaper than another account she had been using previously.

When Mrs G was asked what prompted her to make a payment, she explained she was just moving money across to her own cryptocurrency account and no one had asked her to do it.

I think it's clear that Mrs G was willing to give inaccurate answers to have payments processed, and although she was given multiple opportunities to provide further details of what had prompted her to make the payments, she didn't provide further information. Mrs G also ignored a warning from HSBC that accurately described some of the scam elements she was experiencing such as social media advertising and convincing websites.

Proving inaccurate information would and did make it extremely difficult for HSBC to uncover the scam that was taking place. While I think HSBC could have intervened further than it did, I don't have enough to say that Mrs G would have provided more accurate information had it done so. So, I don't think HSBC missed an opportunity to uncover the scam and it is not responsible for Mrs G's loss.

Mrs G has explained that warnings were available about X, and that HSBC should have had systems in place to spot these. But Mrs G said she had carried out her own due diligence and was still happy to proceed with the investment.

Mrs G also didn't make the disputed payments to X directly. Instead, she made them to a genuine cryptocurrency exchange and when questioned about the payments told HSBC she was just making payments to her own cryptocurrency account. So, HSBC would not have been aware of X's involvement.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs G to accept or reject my decision before 13 January 2026.

Terry Woodham
Ombudsman