

## **The complaint**

Ms S complains that HSBC UK Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam company, or to help her recover the money once she'd reported the scam to it.

## **What happened**

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Ms S paid to join a dating website where she met someone I'll refer to as "the scammer". They eventually began to communicate via Whatsapp, and discussed their careers, lifestyles and interests, such travelling, sport and reading. She thought he seemed wealthy, which aligned with the website's claim to attract rich and successful millionaires and he sent photographs of himself on extravagant holidays and wearing expensive watches. He expressed an interest in getting married and said his culture meant he only dated for marital purposes.

The scammer told Ms S he was a financial advisor and seemed knowledgeable about the stock market. She told him she was keen to invest, and he said she should begin investing in gold and that he'd devise an investment plan for her. He told her she could make transactions via cryptocurrency or international transfers and as Ms S had some experience with cryptocurrency, she was happy to proceed.

He sent her a link to a trading platform I'll refer to as "J" and told her to create a gold account, which required her to complete KYC and verification checks by providing her photo ID, proof of address, and credit card details. The account was incredibly professional and well organised and replicated other genuine trading platforms Ms S had seen.

The scammer told Ms S he had his own broker who was essential for investors to succeed in getting returns from the London gold market. He provided a wallet address to transfer her existing cryptocurrency to J, and between 24 April 2021 and 30 May 2021, she made nine transfers totalling £44,505 from her HSBC account.

On 18 April 2021, Ms S processed two credit card payments of £500 each to the cryptocurrency exchange company. The scammer told her there would be a sudden drop, in the value of gold on 19 April 2021 so on 20 April 2021, she processed a further four credit card payments of £500. Ms S told the scammer she had no more money to invest but he said he would place double the amount she would so that if anything went wrong, it would happen to them both. Ms S had already exceeded her overdraft and credit card limit, so she increased her overdraft limit to £5,000, and took out a loan of £20,000.

While she was waiting for the loan to be processed, Ms S processed a payment of £4,000 from her HSBC account. HSBC blocked the payment and in the subsequent call, she was asked what the payment was for, whether she was making the transaction, and whether she was being forced to make the payment.

Ms S received the loan on 25 April 2021 and made a further payment of £10,000 from her HSBC account. HSBC blocked the payment and asked her questions around the purpose of the payment. She told it the reason for the payment was private, and it was released with no scam education or advice.

Ms S continued to see profits on her trading account and on 28 April 2021, she processed a further payment of £2,005 from her HSBC account. On 5 May 2021, she took out a second loan and when she received the loan, she processed two payments of £10,000 from her HSBC account. On 13 May 2021, she transferred a further £4,000 from her current account, which was the remaining balance on her overdraft.

In June 2021, Ms S was notified that J had frozen her account due to suspicion of money laundering and that to reopen the account she would have to pay a risk release fee of £172,000. The scammer tried to persuade her to borrow money from friends or to take out a further loan, offering to pay 50% of the fees. When Ms S refused to do this, the scammer became threatening and threatened to post photographs of her online, at which point she realised she was the victim of a scam.

Ms S complained to HSBC with the assistance of a representative. The representative argued the two interventions were basic and ineffective as Ms S had been coached to lie. They said it failed to question Ms S further when she said the reason for the payment was private, despite the fact she was paying a cryptocurrency merchant. And it failed to provide any advice or scam education.

HSBC refused to refund any of the money she'd lost. It said it was signed up to the Contingent Reimbursement Model ("CRM") code but as the payments were to an account in Ms S's own name, they weren't covered by the code.

Ms S complained to this service with the assistance of her representative. She said it was clear she was at risk of financial harm as the transactions were unusual, and HSBC failed to intervene and protect her against the scam. She explained HSBC sounded patronising during the phone calls and she was unhappy with the customer service it provided when she reported the scam to it.

Her representative said there should have been a greater level of intervention as the payments had the hallmarks of an investment scam and multiple known fraud indicators. They argued HSBC ought to have asked more questions around the reason for the payment as she sounded frustrated, and this should have alerted it that she was possibly being coached.

They said it should have directed Ms S to the Financial Conduct Authority ("FCA") website, asked her whether she'd been able to make any withdrawals and warned her it was unusual for third parties to be involved in investments, and had it done so she might have discovered there were negative reviews online about J.

The representative explained Ms S was in her overdraft throughout the scam and took out loans which were quickly paid out, which ought to have raised concerns. Before the scam, her daily expenditure was low for example in January and February 2021, the highest payments were £825 and £550. And in March 2021, the highest payment was £649.95.

They also said HSBC failed to raise a chargeback request in respect of the card payments and that it should provide a refund under Section 75 Consumer Credit Act 1974.

HSBC said the cryptocurrency exchange company offered useful information to consumers and warned that transactions can't be reversed. It said warnings were issued in accordance

with its understanding that Ms S was paying an account in her own name, and there was no suggestion the funds would then be used for a cryptocurrency investment.

Our investigator didn't think the complaint should be upheld. She said the CRM code doesn't apply to card payments, international payments or payments to accounts in the name of the consumer. She explained the interactions on 24 and 25 April 2021 didn't prevent Ms S from going ahead with the transactions and that she would have expected HSBC to have asked additional questions about the context and true purpose of the payments. Specifically, it should have asked how she was contacted, whether she'd parted with personal details to open a trading account and whether the investment opportunity was linked to a prominent individual or advertised on social media.

But she noted Ms S had been coached on what to say and that when she applied for the loan, she didn't provide a detailed reason for the application. Because of this, she thought that even if HSBC had provided a scam warning, or asked further questions, Ms S wouldn't have disclosed the real reason for the payments, so she didn't think further questioning from HSBC would have made a difference.

Finally, she said Ms S had moved the funds out of the account, so there would be nothing to recover.

Ms S has asked for her complaint to be reviewed by an Ombudsman. Her representative has argued that HSBC ought to have asked open ended questions to get Ms S to explain what the payments were for and if she'd been contacted by anybody about the transactions. It should have also explained the risks involved in lying to the bank. And if it had asked more questions and provided a full scam warning, it would have been able to break the spell of the scammer and prevented the loss.

They said HSBC ought to have asked Ms S more questions on 5 May 2021 when she told it the payment was for private reasons including more questions about the context and true purpose of the payment, how she'd been contacted, whether she'd parted with personal details to open a trading account and whether the investment opportunity was linked to a prominent individual or advertised on social media. And if it had looked at the account holistically, it would have seen she'd made over £15,000 of payments to a cryptocurrency wallet using money from loans, which is an obvious pattern of fraud. And regardless of her responses, it had the account history and an unwillingness to respond with specific answers to determine that she had fallen victim to a scam.

### **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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Ms S has been the victim of a cruel scam. I know she feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Ms S says she's fallen victim to, in all but a limited number of circumstances. HSBC has said the CRM code didn't apply in this case because the code doesn't apply to card payments and international payments, or payments an account in the customers own name, and I'm satisfied that's fair.

I've thought about whether HSBC could have done more to recover Ms S's payments when she reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will

ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two presentments. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. HSBC) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Ms S).

Ms S's own testimony supports that she used a cryptocurrency exchange to facilitate the transfers to J. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Ms S's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined to fail, therefore I'm satisfied that HSBC's decision not to raise a chargeback request against the cryptocurrency exchange company was fair.

I'm satisfied Ms S 'authorised' the payments for the purposes of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of her bank account, Ms S is presumed liable for the loss in the first instance.

Not every complaint referred to us and categorised as an investment scam is in fact a scam. Some cases simply involve high-risk unregulated investments that resulted in disappointing returns or losses. Some of these investments may have been promoted using sales methods that were arguably unethical and/or misleading. However, while customers who lost out may understandably regard such acts or omissions as fraudulent, they do not necessarily meet the high legal threshold or burden of proof for fraud, i.e. dishonestly making a false representation and/or failing to disclose information with the intention of making a gain for himself or of causing loss to another or exposing another to the risk of loss (Fraud Act 2006).

I've carefully considered the circumstances, and I am satisfied J was operating a scam. However, although Ms S didn't intend her money to go to scammers, she did authorise the disputed payments. HSBC is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

### *Prevention*

I've thought about whether HSBC could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, HSBC had an obligation to be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Ms S when she tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect HSBC to intervene with a view to protecting Ms S from financial harm due to fraud.

The payments did flag as suspicious on HSBC's systems and there were calls on 23 April 2021, 24 April 2021, 25 April 2021, 28 April 2021 and 5 May 2021. The first payment of £4,000 on 24 April 2021 flagged for checks and Ms S contacted HSBC to tell it she wanted it to release the payment. The call handler told her they were asking questions to make sure she wasn't being scammed and asked whether she'd been forced or threatened to make the payment. Ms S said she was paying her own account and that she'd opened it herself. She said she wasn't forced or threatened or told to lie, and the payment was released. She wasn't asked any questions around the purpose of the payment, whether there was a third

party involved or the nature of the checks she'd completed, and she wasn't given any advice about scams.

The next intervention took place on 25 April 2021 when Ms S tried make a payment of £10,000. This was a long and difficult call during which Ms S was obviously distressed and upset at how she perceived the call handler was speaking to her. The call handler told Ms S she wanted to check her money was safe and asked whether anyone had forced her to make the payment. Ms S said that she was paying her own account, and no one had forced her to do it. The call handler required confirmation that pervious payments had been received, but Ms S was only able to confirm receipt of funds from her credit card. The call handler also asked questions around how she got the account details and why she wanted to transfer the money. Ms S insisted the reason for the payment was personal. She was also asked why she got the £25,000 loan, and again she said it was for personal reasons.

The next call took place on 28 April 2021. During this call, Ms S was asked if she'd made the payment of her own free will. She confirmed the payment was to her own account and that no one had advised her to make the payment. She also said no one else had access to the account and when asked about the purpose of the payment she said it was for personal reasons. The call handler asked if she'd read the fraud warning and Ms S said she read it every time she made payments. The call handler said she wanted to make sure she wasn't the victim of a scam and released the payment.

The final call took place on 5 May 2021. The call handler said she needed to make sure Ms S wasn't the victim of a scam and asked her about the purpose of the payment. Ms S said it was for private reasons and that she was paying her personal account. The call handler checked Ms S had confirmed the details of the beneficiary account and warned her it was important that she knew who she was paying, and that fraudsters try to get to know people on social media and then ask for money. They pressed her on the reason for the payment and she maintained that she didn't have to tell her why she wanted to transfer the money. After several attempts, the call handler warned Ms S that HSBC wouldn't be able to recover the funds and released the payment.

I've thought carefully about what took place during the four interventions and I'm satisfied HSBC intervened when I would expect it to. And I don't think it needed to intervene when she made the later payments, which were for increasingly smaller amounts.

During each call, Ms S was asked why she was making the payments and each time she said it was for personal reasons or refused to give any detail. On 25 April 2021, the call handler pushed Ms S to tell her the reason for the payment, but she refused to give any more information.

Our investigator said HSBC ought to have asked more questions around the context and true purpose of the payments and to have given a scam warning. I agree with this because it would have been clear that Ms S was paying a cryptocurrency exchange. But, based on the answers she gave to the questions she was asked, I don't think Ms S would have volunteered any more information, so wouldn't have had enough information to enable it to identify that she was being scammed. And I don't think she'd have listened to a scam warning because she clearly trusted the scammer to the extent that she was unwilling to engage at all with HSBC.

The representative has said some of the questions were irrelevant and misleading, but across the four calls, Ms S maintained her position in the face of repeated attempts to encourage her to disclose the reason for the transfers, so HSBC didn't have the information it needed to properly tailor the advice and warnings.

Overall, while I think HSBC could reasonably have done more during the calls, I don't think this represented a missed opportunity to have prevented Ms S's loss.

### *Recovery*

I'm satisfied there was no reasonable prospect of a successful recover because Ms S transferred the funds out of the beneficiary account.

### *Customer service*

I understand Ms S felt patronised during one of the calls, but I'm satisfied the service she received was reasonable throughout.

I'm sorry to hear Ms S has lost money and the effect this has had on her. But for the reasons I've explained, I don't think HSBC is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

### **My final decision**

For the reasons I've outlined above, 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 S to accept or reject my decision before 17 November 2023.

Carolyn Bonnell  
**Ombudsman**