DRN-4748319

The complaint

Mrs W complains that HSBC UK Bank Plc didn't do enough to protect her from the financial harm caused by an investment scam, 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.

In July 2021, Mrs W saw an advertisement on social media for an investment opportunity which was endorsed by a well-known celebrity. She registered her interest online and was contacted by someone who claimed to work for a company I'll refer to as "T".

Mrs W's research revealed nothing negative about T. She could see the website appeared near the top of the search results and featured the company logo. The website claimed T was a leading cryptocurrency market trader with offices around the world. There were complaints, enquiries, legal and 'About Us' sections and there was also a social media page. Mrs W said she had some inheritance and was told she could invest as little as £500 and that she could withdraw her profits at any time. She would be assigned a senior account manager who would contact her with her username and password and that he would help her to make lots of money.

Mrs W was contacted by the account manager, who I'll refer to as "the scammer". The scammer told Mrs W he'd been working in the finance industry for years and used to work for a reputable firm that she'd heard of. He told her he liked to build relationships with his clients as he believed trust was key. When it was time to begin trading he instructed Mrs W to download AnyDesk and to provide her ID for money laundering and verification purposes. He said he would take an 8% commission from successful trades.

The scammer told Mrs W to open an account with a cryptocurrency exchange company I'll refer to as "K". Between 5 July 2021 and 24 September 2021, she made two debit card payments and four transfers to international accounts from her HSBC account totalling £153,467.63.

Mrs W was able to log into her trading account and watch as the scammer made trades on her behalf. In November 2021, she was unable to access her trading account and began to have trouble contacting the scammer. She assumed she'd just made a bad investment but in June 2022, the scammer re-approached Mrs W and said they could recover her funds if she paid a large sum to T. Mrs W didn't want to send more funds, and she realised she'd been scammed when he became threatening towards her.

She contacted HSBC to report the scam in December 2022 but it refused to refund the money she'd lost. It said it was unable to refund the money because she'd authorised the payments and it had contacted the beneficiary bank but no funds remained. It explained it was unable to take any action in respect of the international payments in line with the Best

Practice Standards for Authorised Push Payments and they weren't covered by the Contingent Reimbursement Model ("CRM") code.

It explained it has a Fraud Detection System in place for all types of payments and if a payment is verified using a customer's photographic identification or their personal security details, it won't usually score highly. It said it had asked Mrs W who she was making the payments on 26 July 2021, 6 August 2021 and 12 August 2021 and she'd said she was making an investment. She was then given relevant on-screen fraud and scam advice and referred to its Fraud Centre for further guidance.

Mrs W wasn't satisfied and so she complained to this service with the assistance of a representative. She said all the payments debited her account with no intervention apart from a pop-up asking if she wanted to proceed with the payments, which wasn't an effective warning. She said HSBC should have made enquiries about the true context of the payments, which could have saved her from financial harm. She doesn't recall receiving warnings on 6 August 2021 and 12 August 2021, indicating they were ineffective.

She said the fact the fact the card payments were me-to-me payments wasn't an excuse for HSBC to sidestep its responsibilities and the loss was foreseeable because she was engaging with a cryptocurrency exchange. She explained her usual spending activity had increased from £3.99, £5.07, and £7.55 to lump sums of £17,635 and £50,000 to a new payee linked to cryptocurrency.

Mrs W's representative said HSBC had failed to raise a chargeback request. And they argued that should have intervened from 26 July 2021 as there were obvious red flags including the fact she was paying a new payee linked to cryptocurrency, there was a sudden increase in spending, she started with a small initial amount, there was a large amount of money coming into and then leaving the account, and the payments were made in quick succession. Further, she had never used her account to make cryptocurrency transfers and card payments before, and the size of the payments was extremely unusual.

They said HSBC should have contacted Mrs W and asked her probing questions around why she was making the payments, who she was trading with, how she found out about the company, whether she'd researched the company, whether she'd checked the Financial conduct Authority ("FCA") website, whether she'd received any withdrawals and whether she'd discussed the investment with anyone. Had it done so, it would have established Mrs W was likely falling victim to a scam and provided a scam warning.

HSBC further stated that effective warnings were provided before or during the payment journey and that the claim was declined because it had contacted the beneficiary banks in a timely manner, but international payments cannot be recalled and provide no guarantee of a refund.

It said K is a legitimate cryptocurrency exchange so there wouldn't have been any concerns about the payments and as the funds were paid to the fraudster from K, the payments from HSBC couldn't be considered fraudulent.

It also said Mrs W had made international payments in May and June to a cryptocurrency merchant. She didn't meet the requisite level of care as no independent investigation was undertaken to verify the validity of the investment and it provided clear warnings when Mrs W made the payments, yet she went ahead without attempting to make any withdrawals.

Our investigator didn't think the complaint should be upheld. He explained the CRM code didn't apply to debit card or international payments. And there would have been no prospect

of a successful chargeback because Mrs W paid a legitimate cryptocurrency exchange who had provided the service she'd paid for.

He didn't think payments one or two were unusual for the account. He thought the international payments ought to have triggered an intervention because they were out of character for the usual spending on the account. However, he noted that HSBC had provided relevant and tailored scam warnings on 26 July 2021, 6 August 2021 and 13 August 2021, which he was satisfied was proportionate.

He explained that even though there was no scam warning on 24 September 2021, he didn't think a further warning would have made any difference to the outcome because Mrs W had ignored the previous warnings, so she didn't think its failure to intervene again represented a missed opportunity to have prevented her loss.

Finally, given the length of time that had passed he was satisfied there was no reasonable prospect of a successful recovery.

Mrs W has asked for her complaint to be reviewed by an Ombudsman arguing the warnings provided weren't impactful and that HSBC should have contacted her to understand the nature of the payments.

My provisional findings

I thought about whether HSBC could have done more to recover the card 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 (Mrs W).

Mrs W's own testimony supports that she used cryptocurrency exchanges to facilitate the transfers to K. Its 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 Mrs W's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that HSBC's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

The Contingent Reimbursement Model ("CRM") Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mrs W says she's fallen victim to, in all but a limited number of circumstances. HSBC has said the CRM code doesn't apply to payments to international accounts or payments to an account in her the consumers own name, and I was satisfied that's fair.

I was also satisfied Mrs W 'authorised' the payments for the purposes of the 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, Mrs W is presumed liable for the loss in the first instance.

But although Ms K 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 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's seen, the payments were made to a genuine cryptocurrency exchange company. However, HSBC ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I needed to consider whether it ought to have done mote when Mrs W made the payments.

HSBC provided the following written warning when Mrs W made payments on 26 July 2021, 6 August 2021 and 12 August 2021: *This could be a scam. Fraudsters can offer you what appears to be a genuine opportunity with high returns. They can try to pressure you to invest your savings of transfer your current pension to a new scheme. Take time to talk to someone you trust who is not involved with the investment. You must independently research who you're sending money to. Check the company is genuine and authorised by contacting the Financial Conduct Authority. Company names can be cloned. It's vital that you contact the company on an independently verified number. Visit our fraud centre to find out more. By choosing to continue you agree you've read our warning and are happy to proceed. You accept we may not be able to recover your money if its sent to a fraudster's account.*

Mrs W wasn't presented with any warnings when she made the first two payments. Both these payments were debit card payments to a new payee which was linked to cryptocurrency but based on the fact Mrs W was paying a legitimate cryptocurrency merchant, they were relatively low value and the amounts weren't unusual when compared to recent transactions on the account, I didn't think HSBC needed to intervene.

The warning was presented before payments three, four and five, which were very high value payments of £43,832.23, £50,000 and £42,000. I considered the nature of the written warning Mrs W was shown before she made the payments and I was satisfied it was relevant to the scam and that it provided information on what to look out for and how to check in investment was genuine. But these were very high value payments made following large transfers into the account. This was particularly unusual when compared to the normal activity on the account in the period leading up to 26 July 2021 to the extent that even though she'd made previous payments to a cryptocurrency exchange, I didn't think a written warning was proportionate.

HSBC should have contacted Mrs W and asked her why she was making such large payments to a cryptocurrency exchange. It should also have asked her whether there was a third party involved and if she how she met then, whether she'd been promised unrealistic returns, whether she'd made any withdrawals and whether she'd been advised to make an onwards payment from K.

There's no evidence that she'd been coached to lie and so I think she'd have disclosed that she was being assisted by someone who worked for T, that she'd found T on social media and that it had been endorsed by a celebrity. She would probably have also said that she hadn't made any withdrawals and that she'd been advised to make an onwards payment from K.

I was satisfied that there were enough red flags for HSBC to have identified that Mrs W was being scammed, so it would have been in a position to go further than the written warning by telling her there were warning signs which strongly indicated that the investment was a scam.

I accepted Mrs W went ahead with payments three, four and five in the face of a relevant written warning, but I think a detailed conversation with someone from HSBC would have been more impactful than a written investment warning. Specific elements of the investment were red flags for fraud, in particular the celebrity endorsement and I thought she'd have listened to and acted on advice to do more due diligence and ultimately decided not to go ahead with the payments. Significantly, the FCA warning wasn't published until 30 July 2021, but I hadn't seen any evidence that Mrs W was keen to take risks with her inheritance and so I thought a better intervention would have made a difference to the outcome.

Consequently, I thought HSBC's failure to contact Mrs W and question her about the payment on 26 July 2021 represented a missed opportunity to have prevented her loss and that it should refund the money she'd lost from that point onwards.

Contributory negligence

Mrs W has explained that the scammer was were very persuasive on the phone and sounded knowledgeable, competent and friendly. T had a professional-looking website and this had left her feeling confident about the investment. And she had mistakenly thought she could see her trades on the trading platform.

Having considered the circumstances of this scam, I was satisfied it was sophisticated and I didn't think it was unreasonable for Mrs W to have thought it was genuine to the extent that she didn't raise a complaint with HSBC until December 2022.

I'd seen no evidence that Mrs W was an experienced investor and so I wouldn't expect her to have known how to search for warning on the FCA website without having been advised to do so and the FCA warning wasn't published until after she'd made the first payment. So, I didn't think she contributed to her own loss in failing to check the FCA website. So, while there may be cases where a reduction for contributory negligence is appropriate, I didn't think this is one of them.

Recovery

As the debit card payments were paid an account in Mrs W's own name and the funds were moved onwards from there, I was satisfied there would have been no prospect of a successful recovery. And HSBC wasn't under an obligation to try to recover the international payments.

Compensation

I concluded Mrs W isn't entitled to any compensation or legal costs.

Developments

Mrs W has accepted the findings in my provisional decision but HSBC has made further comments around contributory negligence, arguing that the settlement should be reduced by at least 50% to reflect Mrs W's contribution to her own loss.

It has commented that since January 2021, there have been warnings online about celebrity endorsements with the particular celebrity distancing himself from any form of cryptocurrency investment and confirming that fraudsters have wrongly used his name and face to promote scams. It has argued that this is evidence that Mrs W didn't properly verify that the celebrity endorsement was a legitimate arrangement which is unreasonable considering the sums she invested.

It has argued the fact Mrs W wasn't an experienced investor doesn't absolve her from carrying out basic checks before parting with large sums of money and she invested a lot of money despite having been told she could invest as little as £500 and 'see results'. It has also commented that she was reassured that she could withdraw her funds whenever she likes but she never actually made any withdrawals.

It has argued that Mrs W appears to have relied upon promises directly from the scammer without carrying out appropriate due diligence and so she should bear at least 50% responsibility for her loss.

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've considered the further comments made by HSBC but the findings in my final decision will be the same as the findings in my provisional decision.

I accept that if Mrs W had done additional checks she might have seen warnings online about the celebrity endorsement, but I would only expect her to have done additional checks if she suspected something was untoward. However, I'm satisfied she believed the investment was genuine from the outset and she didn't feel she needed to make additional checks. And there's no evidence that she knew or suspected something might be wrong or that she chose to ignore something which meant it was unreasonable for her to have gone ahead with the investment.

HSBC has also argued the fact Mrs W was an inexperienced investor doesn't mean she didn't need to do basic checks. But as I've previously stated, this was a sophisticated scam and Mrs W was persuaded by the fact the scammer seemed professional and the website and trading platform appeared genuine. I accept that she didn't make any withdrawals but I'm satisfied she was led to believe she would be able to and I don't think it was unreasonable for her to have believe what she was told by the scammer in this regard. I also accept she relied on what she was told by the scammer, but the fact she was inexperienced meant she didn't know that she ought to have verified what she was told using other sources. In these circumstances and as there's no evidence that she ignored anything which ought reasonably to have put her on notice that she was being scammed, I don't think Mrs W can fairly be held responsible for her own loss.

Overall and having considered the additional points raised by HSBC in response to my provisional decision, I maintain that this isn't a case where the settlement should be reduced for contributory negligence.

My final decision

My final decision is that HSBC UK Bank Plc should:

- refund the money Mrs W lost from 26 July 2021, less any credits received during the scam period.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If HSBC UK Bank Plc deducts tax in relation to the interest element of this award it should provide Mrs W with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs W to accept or reject my decision before 15 May 2024.

Carolyn Bonnell
Ombudsman