DRN-3762289

The complaint

Mr M complains that HSBC UK Bank Plc didn't do enough to protect him from the financial harm caused by an investment scam company, or to help him recover the money once he'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.

On 19 November 2021, Mr M came across an article online about an investment company I'll refer to as "B", which was endorsed by a well-known celebrity. The article recommended investing in cryptocurrency and Mr M followed the link provided and submitted his contact details. The next day he received a call from someone claiming to be a broker who said he could help him to invest in cryptocurrency.

The broker asked Mr M for proof of ID and the last four digits of his bank card. He also sent a code via WhatsApp and explained that whenever he was contacted by someone from B, they would tell him this code. He was then allocated an 'account manager' who advised him to download AnyDesk so he could help him to open a trading account and set up an account with a cryptocurrency exchange company I'll refer to as "C". The account manager asked Mr M to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet.

Between 22 November 2021 and 15 December 2021, Mr M made nine transfers to C totalling £42,701 and two payments totalling £304.28 using a Visa Debit card connected to his HSBC account. During the scam period he received credits totalling £72.47.

Mr M could see his profits on the trading account, but the account manager said he needed to deposit more money if he wanted access to better profits. This led him to borrow money from his mother, his daughter and a friend until the account manager advised him to take out a loan. When Mr M discussed this with his brother, his brother raised concerns and he realised he'd been scammed. He contacted HSBC in December 2021 and it said it was unable to refund any of the money he'd lost because the funds had been moved into an account in his name.

It said that when Mr M made the first two payments, he was given a written warning that fraudsters can offer what appear to be genuine investment opportunities and advised to check the Financial Conduct Authority ("FCA") website. It said he would need to contact the cryptocurrency merchant he paid, and it was unable to recover the funds.

Mr M complained to this service with the assistance of a representative. He explained he'd never invested before, so he thought the use of AnyDesk was an ordinary investment practice. HSBC had contacted him when the first payment bounced, and he wasn't asked any questions about the investment.

He also explained that he was extremely stressed when making the investments and he felt the various brokers wanted him to succeed even though they made him feel guilty. He said HSBC had failed to recognise the unusual account activity and if it had asked probing and open-ended questions, it would have realised he was being scammed. He believes the written warnings he received were ineffective.

Mr M's representative said the payments were unusual, noting that in August 2021, the largest payment was £501.58 and in September and October 2021, the largest payments were £1,512.72.

HSBC said the card payments weren't covered under the Contingent Reimbursement Model ("CRM") code. The claim was declined because the payments were sent to Mr M's own cryptocurrency account, and he was presented with effective warnings on 26 November 2021 and 1 December 2021.

Our investigator thought the complaint should be upheld. He was satisfied there was no prospect of a successful chargeback request in relation the two card payments and that the CRM code didn't apply because the funds were paid to an account in Mr M's own name. He listened to the call that took place when Mr M contacted HSBC to check funds had been returned to his account and he didn't think he said anything which should reasonably have alerted HSBC to the fact he'd been scammed.

He didn't think the initial payments were suspicious. But he thought the £6,000 payment Mr M made on 9 December 2021 was unusual because even though C was no longer a new payee, in the year prior to the payment, the only transaction over £6,000 was a mortgage payment, and there were no other large payments in or out of the account.

Our investigator thought HSBC should have asked Mr M questions about the payment and as he hadn't been told to lie, he was satisfied he'd have answered the questions truthfully, which would have alerted HSBC to several red flags. These red flags included the fact the investment opportunity was endorsed by a prominent celebrity and involved a "broker" who had advised him to make an onwards payment from the cryptocurrency exchange platform and to use AnyDesk. Because of that, he thought HSBC should refund the money Mr M had lost from 9 December 2021 onwards.

HSBC has asked for the complaint to be reviewed by an Ombudsman, arguing that the scam took place from the cryptocurrency exchange. It maintains Mr M was presented with written warnings which were relevant to the scam, yet he chose not to take the advice and conduct further checks or to seek independent financial advice, so a warning on 9 December 2021 wouldn't have made a difference to the outcome because he was clearly satisfied that the investment was genuine.

It has argued that by the time he made the £6,000 payment, Mr M had made several smaller payments to the same beneficiary and received two credits, so its systems would have treated C as a trusted beneficiary. And Mr M didn't carry out any checks before making the first payment, which was extremely reckless as the volatility of cryptocurrency is well known. It has also argued that £71.47 was an unrealistic return for an investment of £305.28 and it doesn't accept it could have uncovered the scam because Mr M chose to ignore relevant warnings and other significant warning signs. And there was no negative information available online about B, so a human intervention wouldn't have made a difference.

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.

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

I've thought about whether HSBC could have done more to recover Mr M's payments when he 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 (Mr M).

Mr M's own testimony supports that he used a cryptocurrency exchange to facilitate the transfers to C. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of it. That is, in exchange for Mr M's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined 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 Mr M 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr M is presumed liable for the loss in the first instance.

It's not in dispute that this was a scam, but although Mr M didn't intend his money to go to scammers, he 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 ought to fairly and reasonably 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 Mr M when he 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 Mr M from financial harm due to fraud.

Mr M was given pop-up warning messages on 26 November 2021 and 1 December 2021, but none of the scam payments triggered a call. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how Mr M normally ran his account and I think they were. All the payments were to a legitimate cryptocurrency exchange and the first six payments were relatively low value, so I don't think HSBC needed to intervene. But on 9 December 2021, Mr M made a payment for £6,000, having made a

payment earlier the same day for £1,500 and, even though by this point he had paid C on six previous occasions, and he was paying an account in his own name, there wasn't a history of large payments on the account, and I think HSBC should have intervened because the activity was unusual.

I would expect HSBC to have contacted Mr M to ask him some questions about the payments including why he was paying a cryptocurrency merchant, whether there was a third party involved and if so, how he met them, whether he'd been advised to download AnyDesk, whether he'd been promised unrealistic returns, whether he'd been allowed to make small withdrawals and whether he'd been advised to make an onwards payment from the cryptocurrency exchange. And as there's no evidence he was coached to lie, I think he'd have told it the investment had been endorsed by a celebrity, he'd been told to download AnyDesk, he'd been allowed to make a small withdrawal and he'd been advised to make an online payment from the cryptocurrency merchant.

Even though there were no warnings about B on either the Financial Conduct Authority ("FCA") or International Organisation of Securities Commissions ("IOCSO") websites, I think there were enough red flags present for HSBC to have identified that Mr M was being scammed and that it should therefore have provided a tailored scam warning. And as there's no evidence that Mr M was keen to take risks with his money, I think he'd have listened to a very clear warning from HSBC and thought twice about going ahead with the payment.

HSBC has argued that Mr M went ahead following the written warnings it gave on 26 November 2021 and 1 December 2021, but I agree with our investigator that a conversation would have had more of an impact than a written warning and this is supported by the way he responded to the concerns raised by his brother when he first learned he'd been scammed.

Because of this, I think that HSBC failed to intervene on 9 December 2021 in circumstances which might reasonably have prevented Mr M's loss, so it should refund the money he lost from that point onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence but, in the circumstances, I don't think Mr M was to blame for the fact he didn't foresee the risk.

Mr M wasn't an experience investor, and he was impressed by the professional nature of B's website and the people he thought were assisting him with the investment. He was also reassured by the fact he could see what he believed were his profits on the trading account and because he'd been able to make a small withdrawal, which he didn't realise was a red flag for fraud.

HSBC has said that Mr M was promised unrealistic returns, but the credit into the account was a withdrawal, not a return on the investment. And instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for him to have believed what he was told by the broker in terms of the returns he was told were possible.

Mr M wasn't an experienced investor. He wouldn't have known that the use of remote access software is a red flag, and this unfamiliarity was compounded by the sophisticated nature of the scam. He has explained that his personal circumstances impacted his decision making and I don't accept his job title means he should have been any more able to foresee the risk. So, I don't think he can fairly be held responsible for his own loss.

My final decision

My final decision is that HSBC UK Bank Plc should:

- refund Mr M the money he lost from the seventh payment onwards, minus any credits he received.
- 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 Mr M with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 29 December 2023.

Carolyn Bonnell
Ombudsman