DRN-5052877

The complaint

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

Scam 1

In December 2022, Mr R was searching online for investment opportunities when he came across an investment company which I'll refer to as "O". He looked on O's website and thought it looked professional, noting there were positive reviews, feedback from other users and an "about us" section explaining O traded in cryptocurrency and forex.

He completed an online enquiry form and was contacted by someone claiming to work for O, who I'll refer to as "the scammer". The scammer told Mr R he'd been working in finance for over 10 years and that he could make a reasonable rate of return, which Mr R thought was plausible given the fact he'd heard many success stories about cryptocurrency investments. He signed up to the trading portal, which required him to submit a copy of his ID and was given log-in details.

The scammer asked him to first purchase cryptocurrency through cryptocurrency exchange companies and then load it onto an online wallet. He made an initial deposit on his credit card in November 2022. Then, between 22 December 2022 and 22 March 2023, he made 64 payments to a cryptocurrency exchange company which I'll refer to as "B" totalling £279,108.05 using a debit card connected to his HSBC account. He could see his funds reflected in the trading account and remained in daily contact with the scammer by phone and via WhatsApp. The scammer encouraged him to invest further, explaining the more he invested the greater the returns would be.

On 16 March 2023, Mr R asked to make a withdrawal and was told he'd have to pay capital gains tax and prove the liquidity of his account for anti-money laundering purposes. The following day, he made 18 payments of £1,000, before being told he'd have to pay a conversion fee, which would contribute towards capital gains tax. He questioned why this wouldn't be paid to HMRC and was told this was due to the complexity of cryptocurrency.

Satisfied with the response, Mr R made further payments on 20 March 2023 totalling £18,000 followed by three payments on 21 March 2023 and 22 March 2023 totalling £29,000. He believed these would be the final payments, but he realised he'd been scammed when he didn't receive any funds and lost contact with the scammer.

Scam 2

After the first scam, Mr R was contacted by someone claiming to be from a recovery company, which I'll refer to as "B". Unfortunately, B turned out to be a clone of a well-known cryptocurrency company.

The scammer told Mr R he'd located his lost funds and after undertaking some research, Mr R paid £2,004.70 to begin the recovery process. The scammer asked him to first purchase cryptocurrency through B and then load it onto an online wallet. Between 27 March 2023 and 31 March 2023, he made eight payments totalling £31,634.57 using his HSBC debit card. He was subsequently able to recover £9,746.

When the scammer continued to ask Mr R for further fees, he realised he'd been scammed again. He reported the fraud to HSBC, but it refused to refund any of the money stating he'd authorised the payments and paid accounts in his own name.

Mr R wasn't satisfied and so he complained to this service with the assistance of a representative who said HSBC ought to have intervened because Mr R was making unusually large payments to cryptocurrency merchants in quick succession. He said it should have contacted him to discuss the payments and to provide effective warnings which would have positively affected his decision-making and prevented his loss.

The representative said there were multiple fraud indicators present including the fact Mr R was making payments to a new payee which was a high-risk cryptocurrency merchant, there were large sums entering and leaving the account, a rapid depletion of funds, a sudden increase in spending and multiple payments in quick succession. They said there were transfers into the account from accounts he held with other banks, which were then forwarded to the scam, including £92,750.36 in February 2023.

The representative said HSBC's fraud systems should have triggered on 8 February 2023 as Mr R paid £10,000 to a new payee linked to cryptocurrency. And there were eighteen payments on 17 March 2023, which was unusual for the account. They said Mr R hadn't been prompted to give false answers and so if HSBC had asked relevant and probing questions around what the payments were for, he'd have explained he was acting under the instructions of a broker, and it would have been apparent that he was the victim of an investment scam. They further argued that the Financial Conduct Authority ("FCA") warning went live on 31 January 2023, so it would have been clear that O was operating a scam.

HSBC questioned Mr R's account of events, stating that it spoke to him about a transaction on his credit card on 16 November 2022 when he explained he'd been scammed by O and wanted the transaction to be stopped. In a further call on 18 November 2022, he was asked whether the merchant was fraudulent, to which he answered "definitely". He said O had carried out trades on his behalf without telling him which was "bizarre" and that "alarm bells starting ringing". He also said O contacted him after he inputted his details on a website and he blocked several other calls, so he suspected it was a scam.

HSBC explained Mr R had said in his complaint letter that he began searching for investments in December 2022 to prepare himself for retirement. There was no mention of the November calls or that, by December 2022, he'd already engaged with O for some time and had concerns. He said he came across O on Google having browsed several different companies or that he had a pre-existing relationship with B (having made transactions to them between September and November 2021).

HSBC didn't accept an intervention would have prevented Mr R's losses because he'd concluded that O was operating a scam over a month before the payments commenced, yet he went on to pay out over a quarter of a million pounds. It argued that if the scammer had

been able to persuade him that the investment was legitimate, it's unlikely he'd have been receptive to further intervention from HSBC.

It also argued that Mr R made payments of over £275,000 despite not receiving any returns and that he was willing to overlook numerous red flags which he'd identified at the outset. Further, he borrowed money from his company once his personal savings were depleted, he was apparently attempting transactions as late as 12 April 2023 after reporting the scam earlier that day, and he paid money to the second scam following unsolicited contact, despite having already lost money to the first scam.

HSBC also stated that Mr R contributed to his own loss by behaving recklessly in the pursuit of unrealistic profits, paying over £85,000 (which was 50% of the capital sum invested) to attempt to secure the release of his profits, suggesting the promised returns were too good be true. It said he ought to have been suspicious that he was asked to pay tax in cryptocurrency to B rather than HMRC and the circumstances of both scams were highly suspicious, yet he failed to act with caution when making payments for implausible reasons such as withdrawal fees and taxes. Further, before he made any payments, he was unable to access O's website and the phone number didn't work. He was then provided with a new website, email address and telephone number, which ought to have raised concerns. It was also apparent from the calls on 16 November 2022 and 18 November 2022 that Mr R had seen negative reviews about the investment.

For the second scam, it said Mr R received unsolicited contact only five days after the first scam ended, he conducted inadequate research and ignored the concerns he had without taking reasonable steps such as checking the FCA register. There were also negative reviews about the scam recovery company.

Our investigator thought the complaint should be upheld. He said a chargeback was unlikely to have succeeded, because Mr R made payments to a legitimate cryptocurrency merchant who provided the cryptocurrency he paid for. And there was no scope for it to recover the payments because they funds had been moved onwards from B.

He noted the November payments were part of the same scam and even though the payments were made using Mr R's credit card, he thought HSBC ought to have placed alerts on all his accounts and been on high alert as to the activity on his current account from 22 December 2022 onwards, less any amounts already refunded.

He explained that scammers manipulate customers and persuade them that investments are legitimate and if Mr R had been given adequate warnings when he made the November payments, it would most likely have prevented him from making further payments. He noted Mr R was open and honest during the November calls, but he wasn't given any scam warnings or asked any questions. He accepted Mr R had already declared that he believed he'd been scammed, but he felt HSBC should have asked him more questions to ascertain whether he was at risk of being scammed and provided appropriate warnings to protect and educate him for the future.

He commented that the four November calls showed that HSBC didn't take any action to safeguard Mr R's account after he reported that he'd been scammed and he felt that had it done so, it's likely the payments he made from December onwards would have triggered further interventions. So, he thought it should refund the money Mr R had lost from December 2022 onwards.

Our investigator accepted Mr R had failed to properly consider the risks before going ahead with the investment and that he should have been more cautious. He noted there was an

FCA warning about O dated 31 January 2023 and if Mr R had carried out some basic checks, it's likely he'd have seen the warning. There were also negative reviews on Trust Pilot which would also have indicated there was a problem. So, he thought the settlement should be reduced by 50% for contributory negligence.

HSBC asked for the complaint to be reviewed by an Ombudsman. It maintained Mr R understood the risks involved because he'd previously invested in cryptocurrency. And his willingness to continue with the investment in spite of clear concerns in November 2022 showed he'd have proceeded with the investment if it had intervened again, particularly as it would have flagged similar issues and risks to those which he'd already identified and understood.

It maintained Mr R's conduct amounted to gross negligence and suggested that if it had carried out additional intervention, he'd likely have moved his money to an account with another firm.

My provisional findings

I thought about whether HSBC could have done more to recover Mr R's card 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 R).

Mr R's own testimony supports that he used a cryptocurrency exchange to facilitate the transfers to B. 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 them. That is, in exchange for Mr R's payments, it 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 the cryptocurrency exchange was fair.

I was satisfied Mr R '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 R is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr R 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 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'd seen, the payments were made to a genuine cryptocurrency exchange company.

Mr R started making debit card payments to the scam from his HSBC current account on 22 December 2022. But the initial payment of £854.19 was made on 15 November 2022 using his HSBC credit card, and Mr R had four calls with HSBC in November 2022 in respect of

that payment when he contacted it to report that he believed he'd made the payment to a scam.

During the four calls that took place on 16 November 2022 and 18 November 2022, Mr R said he'd been scammed, and he wanted the payment to be reversed. He was told it wasn't possible to reverse the payment, but he could raise a dispute. As part of the dispute process, he was asked a series of questions about the circumstances of the payment, which I was satisfied he answered honestly. He explained he was investing in cryptocurrency, he'd entered his details into an online contact form and was approached by someone claiming to work for O. He made the initial payment and was passed to an account manager who sent him a link and login details to open an account on the trading platform. When he was unable to access the trading platform, the account manager said the website was being updated and sent a new web address. He subsequently discovered that none of the contact numbers took incoming calls, and the web address wasn't working. He was still communicating with the scammer via WhatsApp, but he thought O was fraudulent and the reviews on Trustpilot were fake.

At the conclusion of the call Mr R was told his credit card had been cancelled and a dispute had been raised. He wasn't given any scam warnings or scam education.

It was clear from the November calls that Mr R had initially believed O was operating a scam. Unfortunately, the scammer then regained his confidence to the extent that he went on to pay out large amounts to both scams. So, the question for me to consider was whether HSBC ought to have done more to prevent that loss.

On 22 December 2022, Mr R paid £3,400 to B followed by £5,100 on 14 January 2023. Due to the amount and the fact it was to a payee which was identifiably linked to cryptocurrency, I thought HSBC should have intervened when Mr R made the second payment, notwithstanding the fact there was some spending of similar value in the months prior. It should have given Mr R a written warning relevant to cryptocurrency investment scams in a clear and understandable way when he made the second payment, and had it done so I thought it would have made a difference to his decision to make any further payments to the scam.

This investment had many hallmarks of a cryptocurrency scam including the fact Mr R had inputted his details online, he was contacted by someone claiming to work for an investment company, he was given access to a trading portal and his account was being handled by an account manager. The FCA warning wasn't published until 31 January 2023, but I think a tailored written warning would have alerted Mr R to the warning signs and notwithstanding the fact the scammer had somehow persuaded him that the investment was genuine after he'd initially concluded it was a scam, I think a tailored cryptocurrency warning from HSBC in the early stages of the scam would have reintroduced and reinforced those concerns.

I said I understood HSBC's argument that Mr R went ahead with the payments when he strongly suspected he was being scammed, so he would be unlikely to listen to anything it could have said had it intervened. But it's significant that his suspicions were never confirmed or reinforced by HSBC and that he wasn't given any scam education of tailored warnings during the November calls, so I didn't think his actions at that point can fairly be said to show how he'd likely have reacted to an effective intervention from HSBC.

Because of this, I was minded to conclude that HSBC missed an opportunity to intervene when Mr R made the second payment and so it should refund the money he lost from the second payment onwards.

Contributory negligence

There's a general principle that consumers must take responsibility for their decisions and conduct suitable due diligence and in the circumstances, I didn't think Mr R took reasonable care to check the investment was genuine before he made the payments.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I didn't think it was unreasonable for Mr R to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible. And even though he'd had previous dealings with B, he wouldn't necessarily have known that the investment had the hallmarks of a cryptocurrency scam or how to check the information he'd been give without being given scam education by HSBC.

However, it was clear from Mr R's comments during the November calls that he had identified a number of red flags, which he then ignored, relying on advice from someone he'd never met. Those red flags included the fact he'd inputted his details on an online contact form and received lots of calls within five minutes, which he felt was suggestive of a scam.

He was also concerned that the phone numbers he was given didn't take incoming calls and the first web address didn't work. He'd also ignored negative reviews about O on Trustpilot. I accepted that by the time Mr R was contacted by the scam recovery company that he was desperate to recover his lost funds, but in the circumstances and having already lost such a large amount, I thought he ought reasonably have taken greater care before sending further funds in an effort to recover the funds he'd lost to the first scam.

Consequently, I said I was minded to agree that the settlement should be reduced by 50% for contributory negligence.

Compensation

The main cause for the upset was the scammer who persuaded Mr R to part with his funds. I haven't found any errors or delays to HSBC's investigation, so I didn't think he's entitled to any compensation.

Recovery

I didn't think there was a realistic prospect of a successful recovery because Mr R paid an account in his own name and moved the funds onwards from there.

Developments

Both parties have indicated that they accept my provisional findings.

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.

Because both parties have indicated that they accept my provisional findings, the findings in my final decision will remain the same.

My final decision

My final decision is that HSBC UK Bank Plc should:

• refund the money Mr R lost from the second payment onwards, less any credits or refunds received during the scam period.
• this settlement should be reduced by 50% to reflect contributory negligence.
• 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 R with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 28 October 2024.

Carolyn Bonnell
Ombudsman