DRN-4401710

The complaint

Mr B and Ms M are unhappy that HSBC UK Bank Plc won't reimburse them for money they lost as a result of a scam.

What happened

In April 2021 Mr B became friends with someone in an online hobby forum he frequented. He began to talk about investing with this person, and as the friendship developed they shared details of the profits they said they had made from investing. Mr B was shown screenshots of a trading platform which appeared to show this person's profits and they told him about a company that was helping them and the trading platform they were using. Based on what he'd seen Mr B felt this was a good investment opportunity, and agreed to invest he and Ms M's money. He was encouraged to open a trading account and to make payments to it for trades that his "friend" was telling him about. Mr B would make payments form his HSBC accounts to a cryptocurrency account he held, and then on to the trading platform. Unfortunately, and unknown to Mr B and Ms M, the people Mr B was dealing with were scammers.

Over the following few months Mr B made numerous payments to the trading platform via his cryptocurrency account. Firstly, these payments were made from an Australian HSBC account – and I won't be able to consider any of those payments here – and then, starting on 15 September 2021, from Mr B and Ms M's UK HSBC accounts. The initial two payments, for £20,000 and £25,000, were made via internet banking, but the third payment made was large enough that it had to be made in branch, at which stage some discussion did take place regarding the reason for the payments. HSBC was satisfied with the explanations Mr B gave for the payments, and further payments were then made, both in branch, via internet banking and over the phone.

Mr B says he saw both profits and losses on his trading account, and was able to make small withdrawals (which were immediately reinvested). In early October 2021 Mr B asked to withdraw his profits, and was told he'd need to pay significant fees and taxes to facilitate this withdrawal. When he'd paid these fees, still was not able to withdraw his profits, and was then asked to pay further fees, Mr B realised he'd been scammed. But by this time he and Ms M had lost £857,760.48 to the scammers from their HSBC accounts.

Mr B and Ms M asked HSBC to consider reimbursing them for their loss. They felt that HSBC should have noticed the significant change in spending behaviours and asked more questions about what was happening. Mr B and Ms M say that they discussed what they were doing with HSBC several times but were not asked any probing questions that could have brought the scam to light.

HSBC considered Mr B and Ms M's claim. But it declined to refund any of Mr B and Ms M's losses, it said that the loss had been from Mr B's cryptocurrency account and he should direct his complaint to them. HSBC has also noted that it believes it gave appropriate warnings to Mr B and Ms M.

Mr B and Ms M referred the matter to our service. Their complaint was considered by one of our Investigators. They thought HSBC ought to have found the first scam payment – for £20,000 on 15 September 2021 – to be suspicious and that it should have made further enquiries before allowing the payment to be processed. They felt that if HSBC had made further enquiries the scam would have come to light and Mr B and Ms M would not have incurred the losses they incurred from that point onwards.

However, the Investigator did think that there should be a 50% deduction from the amount awarded for the payments made from 1 October 2021 onwards. They felt that, by this stage, the reasons Mr B was given for making the payments were implausible, and it was clear from his messages with the scammers that he was becoming concerned. So they felt there was an element of contributory negligence here.

So, the Investigator recommended that HSBC refund 100% of the payments made in September 2021, and 50% of the payments made from October onwards (minus the small amount Mr B had been able to withdraw). They also recommended that HSBC pay interest on these amounts, at the savings account rate for payments made from Mr B and Ms M's savings account and at our standard compensatory rate of 8% for payments made from Mr B and Ms M's current account.

Mr B and Ms M accepted our Investigator's recommendations, but HSBC didn't agree. It said that the first two payments made were not unusual given the usual operation of the account and that it did then intervene appropriately when the third – and much higher – payment was made. HSBC also stated that it felt even with further intervention, the likelihood was that Mr B and Ms M would have continued with the investment given the background to the scam and how taken in they appear to have been by it. HSBC also noted that it felt if there was to be a deduction for contributory negligence it should apply to all the payments as it did not feel Mr B and Ms M had done enough to ensure they were investing in a legitimate scheme.

As no agreement could be reached, the case has now been passed to me to consider afresh.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I am required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Having done so, I've reached the same conclusions as our Investigator, I'll explain why.

It's not disputed that Mr B authorised the payments that are in dispute here. So as per the Payment Service Regulations 2017 (which are the relevant regulations in place here) that means Mr B and Ms M are responsible for them. That remains the case even though Mr B was the unfortunate victim of a scam.

Because of this, Mr B and Ms M are not automatically entitled to a refund. But I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good practice at the time, HSBC should *fairly and reasonably* have been on the look-out for the possibility of APP fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

I am mindful in reaching my conclusions about what HSBC ought fairly and reasonably to have done that:

- FCA regulated banks are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6)[1].
- Banks have a longstanding regulatory duty *"to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime"* (SYSC 3.2.6R of the Financial Conduct Authority Handbook, which has applied since 2001).
- Over the years, the FSA, and its successor the FCA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the *"Financial crime: a guide for firms"*.[2].
- Regulated banks are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).
- The October 2017, BSI Code, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code, but in my view the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now.
- HSBC is also a signatory of the CRM Code. This sets out both standards for firms and situations where signatory firms will reimburse consumers. The CRM Code does not cover all authorised push payments (APP) in every set of circumstances (and it does not apply to the circumstances of these payments), but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a

[1] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

[2] For example, both the FSA's Financial Crime Guide at 4.2.5G and the FCA's 2015 "Financial crime: a guide for firms" gave examples of good practice in relation to investment fraud saying:

"A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.

A bank contacts customers if it suspects a payment is being made to an investment fraudster.

A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules."

fair articulation of what I consider to be good industry practice generally for payment service providers carrying out any APP transactions.

So, overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.
- Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.

When should HSBC have fairly and reasonably intervened to make further enquiries before it processed the payments?

Mr B made 25 payments from he and Ms M's HSBC accounts to his cryptocurrency account as a result of this scam. HSBC has argued that the earliest it should be expected to have intervened is at the time of the third payment, which was for £150,000 and was made in branch.

HSBC has said that the earlier two payments, for £20,000 and £25,000 were not unusual enough in the context of the account to have been flagged for further checks. And when the first of these payments was made, as it was to a new payee, Mr B was shown a general scam warning and asked to select the reason for the payment. He selected "friends and family" and so received a more detailed scam warning based on that reason.

Looking at Mr B and Ms M's account statements, I appreciate that there were some much larger transfers out of their account in the months prior to these payments. However, those larger transfers were to existing payees, in fact they appear to be to bank accounts in Mr B and Ms M's name. The scam payment was for a relatively large amount and to a new payee which was also a cryptocurrency provider. And I think this should have been evident to HSBC from the sort code of the recipient account, which was associated with a well-known cryptocurrency payment service provider. And while the prevalence of cryptocurrency scams has changed over time, the FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency have continued to increase since. So I consider that HSBC should have been aware that payments to cryptocurrency providers are higher risk.

In my view this combination of circumstances ought fairly and reasonably to have led HSBC to make additional enquiries, to establish the circumstances in which Mr B was making this payment. Particularly as the payment purpose chosen didn't correlate with the destination outcome – it was more likely Mr B was investing in cryptocurrency. I appreciate that HSBC

did provide a pop-up warning when this first payment was made – so it's clear that it had identified some potential fraud risk concerning this payment – but I think it would have been appropriate for HSBC to ask some open questions about this payment, rather than the generic warning and closed questioning that its pop-up messages contained.

If HSBC had made further enquiries before it processed the £20,000 payment, would that have prevented the losses Mr B and Ms M incurred after that point?

I think it's more likely than not that Mr B wouldn't have made further payments to the fraudster if HSBC had sufficiently intervened.

I say this because, when he visited the branch and did speak with HSBC about the payments he was making, he appears to have been open and honest about what he was doing – investing in cryptocurrency. So I think if HSBC had asked him at the start what he was doing and how he had come across this opportunity, it's likely he would have told it the truth. In coming to this conclusion I've considered that Mr B chose "friends and family" as the purpose for the payment, rather than saying it was for an investment. But I've seen no evidence he was coached into saying this or was trying to conceal the reason for the payment. The weight of evidence, and what happened subsequently persuades me Mr B wouldn't been dishonest if asked about what he was doing.

And I think what he would likely have said should have been concerning to HSBC – that he was being advised via WhatsApp, by someone he had not met in person, about trading in cryptocurrency. And if HSBC had then given an appropriate warning, which I think should have included details of the most common features of these types of investment scams, then it's likely that information would have rung alarm bells for Mr B given that what was happening to him bore some of the hallmarks we would expect to see in this type of scam. And, as the scam progressed, there were more points of concern that I think would have flagged to Mr B that he was at risk if appropriate warnings had been given.

HSBC has said that when it did speak to Mr B and Ms M about the larger payments it gave appropriate warnings and those warnings were not heeded, but I don't agree. I've listened to the conversations HSBC had with Mr B and with Ms M, and have considered the recollections of the branch staff and of Mr B and Ms M regarding the visits Mr B made to branch. But I'm not satisfied that what I've seen demonstrates that HSBC gave appropriate warnings about the risks and common features of investment scams.

In the phone calls I've listened to the warnings given are very focussed on whether the beneficiary account is genuine, and on whether Mr B or Ms M have been contacted by anyone claiming to be from a trusted source like a bank or a government agency. So it does appear that HSBC's warnings were focussed on the risk of safe account scams rather than on investment scams despite Mr B and Ms M telling it they were investing in cryptocurrency. HSBC did ask generally whether Mr B and Ms M were aware of the risks of cryptocurrency, but it didn't provide any context for what a cryptocurrency investment scam might look like. It seems clear to me and, I think, ought to have also been clear to HSBC at the time, that when Mr B and Ms M said they were aware of the risks they were referring to the inherent riskiness of investing, rather than of investment scams in particular.

HSBC has said that its branch staff would have provided detailed warnings as well, but the comments I've seen from branch staff again seem to all refer to whether the beneficiary account was genuine, rather than to the risks of cryptocurrency investment scams. I acknowledge that Mr B and Ms M say that Mr B was questioned at length in branch when he made the £150,000 payment, but I don't think that supports HSBC's position that the questioning was relevant or appropriate. I also note that when it comes to some of the later payments HSBC's notes refer specifically to Mr B saying that he was making payments – to

a cryptocurrency provider – for the purposes of tax. In my view this really should have been a significant red flag to HSBC given the circumstances, but I can't see any evidence that HSBC probed about this further or pointed out to Mr B how unusual, and how indicative of a scam, this would be.

So I'm not satisfied that HSBC has shown that it took the steps it should have in light of the risk of financial harm from fraud, and I'm satisfied that if it had done so, the scam would have come to light and the losses Mr B and Ms M incurred could have been prevented.

Should HSBC fairly and reasonably be held responsible for Mr B and Ms M's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr B transferred the money to a cryptocurrency account in his own name, rather than directly to the fraudster, so he remained in control of the money after he made the payments from the HSBC account, and it took further steps before the money was lost to the fraudsters.

But for the reasons I have set out above, I am satisfied that it would be fair to hold HSBC responsible for Mr B and Ms M's losses (subject to a deduction for Mr B and Ms M's own contribution towards their loss). As I have explained, the potential for multi-stage scams – particularly in relation to cryptocurrency transactions - ought to have been well known to HSBC and as a matter of good practice HSBC should fairly and reasonably have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams. I'm satisfied HSBC should fairly and reasonably have made further enquiries before the £20,000 payment and, if it had, it is more likely than not that the scam would have been exposed and Mr B and Ms M would not have lost any more money. In those circumstances I am satisfied it is fair to hold HSBC responsible for Mr B and Ms M's loss.

Should Mr B and Ms M bear any responsibility for their losses?

I've thought about whether Mr B and Ms M should bear any responsibility for their loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

I understand there were sophisticated aspects to this scam. Mr B was given access to a trading platform, which I accept might have seemed convincing to him. In addition Mr B was able to make some small initial withdrawals which would have reassured him and given the proposed investment the cloak of credibility. So I don't think Mr B's initial actions were unreasonable.

Nevertheless, by the start of October 2021 Mr B was being asked to make further payments purely in order to be allowed to withdraw his profits, including paying what he was told was capital gains tax using cryptocurrency. I'd reasonably expect Mr B to have some understanding of how, and to whom, tax is properly paid (and the HSBC account statements indicate he did).

I'm satisfied Mr B should reasonably have been concerned by the demands for more money, despite the apparent profitability of his investment. And it seems from his messages with the scammer that he *was* becoming concerned at this time, but Mr B doesn't seem to have taken any steps to check the legitimacy of what the scammers were asking him to do. I suspect, by this point, he was simply paying money out of the hope that he'd be able to access his investment.

In addition, the magnitude of the increase in value of his original investment ought to have alerted Mr B to the possibility that something might be amiss – he's suggested that he

thought he'd made a profit of several million dollars – especially given the repeated demands for unexpected fees. The returns were simply too good to be true.

So, I think Mr B did have a role to play in what happened and I think that the amount HSBC should pay to him and Ms M in compensation should fairly and reasonably be reduced to reflect that role. Given how serious I think Mr B's concerns about the legitimacy of the investment ought reasonably to have been when the scammers began to ask him to pay fees and taxes to access his profits, I think that a fair deduction is 50%.

Could HSBC have done anything else to recover Mr B and Ms M's money?

As the funds went to an account in Mr B's name before being converted into cryptocurrency and sent to the fraudsters, it could not have been recovered by HSBC.

Putting things right

Overall, having considered the matter carefully, I think HSBC should refund 100% of the payments Mr B made in September 2021, and 50% of the payments Mr B made from 1 October 2021 onwards, minus any credits he received.

Where I uphold a complaint, I can award fair compensation to be paid by a financial business of up to £355,000 plus any interest and/or costs/interest on costs that I consider appropriate. If I think that fair compensation is more than £355,000 I may recommend that the business pays the balance.

Decision and award:

I uphold the complaint. I think that fair compensation, on the basis set out above, is £555,380.24. My decision is that HSBC should pay Mr B and Ms M £355,000 plus 8% interest from the date of each payment to the date of settlement.

Recommendation:

I think fair compensation is more than £355,000 so I recommend that HSBC pays Mr B and Ms M the balance - £200,380.24.

This recommendation is not part of my determination or award. HSBC doesn't have to do what I recommend. It's unlikely that Mr B and Ms M can accept my decision and go to court to ask for the balance. Mr B and Ms M may want to get independent legal advice before deciding whether to accept this decision.

My final decision

I uphold this complaint in part. HSBC UK Bank Plc should put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B and Ms M to accept or reject my decision before 6 March 2024.

Sophie Mitchell
Ombudsman