DRN-3461295

The complaint

Mr B is unhappy that HSBC UK Bank Plc trading as first direct won't refund him after he lost money to an investment scam.

Background

I issued a provisional decision on this case on 5 April 2022. I've copied the content of that document below.

Mr B has explained that he met an individual on an online dating app who he began speaking to through a popular instant messaging app. Unfortunately, unbeknownst to Mr B at the time, the individual was in fact a fraudster.

After the pair had been speaking for a few days, the fraudster explained that he had made a career out of investing, and that he worked for a company that also helped others to invest. The fraudster suggested he could teach Mr B how to invest in Bitcoin. The fraudster guided Mr B on how to open a cryptocurrency account (or 'wallet') and also to download his 'company's' online app, which Mr B did. He said the app appeared legitimate – it provided access to a trading platform, showed the account balance, payments in and out and even had a built-in customer service centre.

Mr B said that at this time, he also conducted online searches for the trading company in question, and found a website that appeared legitimate. On this basis, Mr B decided to invest £500. The investment appeared to be successful and Mr B was able to withdraw £615.50 back to his wallet, then on to another bank account.

A few days later Mr B was encouraged to invest more money. Reassured by his first success, he agreed to invest £3,000. Again the investment appeared to be profitable and Mr B was able to withdraw £3,632.50.

The following day, the fraudster told Mr B there were some positive trends and now was a good time to invest a larger amount. Mr B therefore invested £9,000 this time. However after making the transfer the trading platform stopped working. Mr B asked the fraudster what had happened but was told to contact the app's customer services. The customer service advisor then stated 'the system has detected that this account has been frozen by the system as a result of abnormal means to obtain excessive profits.' When asked how to unfreeze the account, Mr B was told he would need to pay 50% of the account funds (quoted as over $21,000) within 24 hours to cancel the abnormality. He was also told that if not completed within this time, the system would deduct 20% of the account funds every day as a fine.

Mr B acknowledges he was concerned by this and it was the first time he considered he may potentially have been scammed. He said the fraudster also begun being more dismissive at this time. Mr B decided to sleep on the decision, then the following morning paid the 'fine'. He made three payments that day of £6,000, £4,000, then £250. However once he paid these funds, the fraudster stopped speaking to him and he was still unable to withdraw anything from the app. He realised at this point he had been the victim of a scam and called first direct to log a fraud claim.

First direct reviewed Mr B's claim, but didn't consider it could assess the payments for a refund as the funds were transferred to Mr B's own wallet. First direct considered Mr B should take the matter up with the wallet provider directly.

Mr B disagreed with first direct so brought the complaint to our service. One of our investigators considered the complaint and partially upheld it. She considered that:

- *Despite payments being made to Mr B's own wallet, there were still enough indicators to suggest Mr B may be at risk of financial harm by the time he made the second payment of £3,000 towards the scam.*

- *Had first direct intervened by calling Mr B to ask further questions before processing the £3,000 payment, it would've been able to uncover that Mr B was the victim of a scam.*

- *Mr B should therefore receive a refund of funds made to the fraudster, minus the initial payment of £500 and any 'profits' Mr B had already received during the scam.*

First direct didn't agree with the investigator's recommendation. To summarise some of the key points it disagreed with, first direct said that:

- *The investigator hadn't considered a deduction to reflect Mr B's contributory negligence, particularly when making the three final payments after Mr B had good reason to consider that the investment was not what he initially thought it to be.*

- *The opinion concludes that account activity was unusual and suspicious, but there is no suggestion that there were any concerns with the named payee, or warnings concerning the wallet provider involved.*

- *Even if first direct had intervened during the payments, any concerns that Mr B was at risk of financial harm from fraud could have been no more than a suspicion. First direct doesn't consider it was obliged to make a call, it's noted that the questions the investigator has suggested it could've asked are very specific and could've been deemed intrusive and unwelcome. First direct considers it unlikely that Mr B would've revealed personal information to the agent, or that he would've accepted that this was a scam based on a single phone conversation.*

- *A recent court decision suggests that the legal standards the investigator judged first direct against were too high.*

- *Any interest applied to the refund should be at the account rate, rather than at 8% simple interest, as Mr B incurred no interest or charges related to the scam payments.*

The case has been referred to me for a final decision.

My provisional findings

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 intend to partially uphold this complaint. I'll explain why.

I am aware that first direct considers too high a standard has been applied to what is expected of it in terms of obligations to 'question' its customers instructions based on the recent Phillipp judgement and its implications to 'the Quincecare duty'. HSBC has now

received a large number of final decisions related to APP fraud, published on our website and so I see no reason to go into detail as to all our relevant considerations.

First direct doesn't consider it's liable for Mr B's losses, as payments went to a cryptocurrency wallet in Mr B's name. A voluntary code does exist to provide additional protection against APP scams (the Contingent Reimbursement Model Code – CRM Code). First direct is a signatory to this code. But it only applies to payments made directly to another person – payments made to a customer's own accounts aren't covered by the CRM Code. That means the CRM Code provisions aren't relevant to Mr B's complaint – his payment instruction was to send money from first direct to his own cryptocurrency wallet.

However, while I therefore find the CRM Code does not apply here, that code is not the full extent of the relevant obligations that could apply in cases such as this.

I've considered what first direct was obliged to do here. In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer's account. And I must take that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story:

- *The law recognises that a bank may be liable to its customer if it makes a payment in circumstances where it has reasonable grounds (although not necessarily proof) for believing that the payment instruction was an attempt to misappropriate the funds of its customer.*

- *Regulated firms like first direct are also 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).*

And as a matter of good industry practice at the time, I consider firms should also have taken proactive steps to:

- *identify and assist vulnerable consumers and consumers in vulnerable circumstances, including those at risk of financial exploitation (something recognised by the FCA in recent years and by the British Bankers Association's (BBA) February 2016 report 'improving outcomes for customers in vulnerable circumstances'); and,*

- *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 (something also recognized by the British Standards Institute's October 2017 'Protecting customers from financial harm as a result of fraud or financial abuse – Code of practice', which a number of banks and trade associations were involved in the development of).*

This means that, particularly with the increase of sophisticated fraud and scams in recent years, there are circumstances where a bank should fairly and reasonably take additional steps, or make additional checks, before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm.

So, in this case, I need to decide whether first direct acted fairly and reasonably in its dealings with Mr B, when he made six transfers from his first direct account to his new

cryptocurrency wallet over the course of around a week, or whether it should have done more than it did.

Mr B accepts he authorised the transfers himself. First direct therefore had an obligation to follow his instructions. Nonetheless, as I've noted above, there are some situations in which first direct should reasonably have had a closer look at the circumstances surrounding these transactions. I consider that as a matter of good practice, first direct should've been on the lookout for unusual and out of character transactions. I've thought about what first direct could therefore reasonably have had knowledge of at the time these payments were made.

I've considered whether the transfers made by Mr L were significantly out of character or unusual. While the transfers were made to Mr B's own wallet, scams involving transfers to cryptocurrency accounts were well known to banks by this time and I therefore think that where payments were also out of character, potential losses were foreseeable to the originating bank.

When considering what payments should be considered significantly out of character, it's often a finely balanced matter – and banks have a difficult balance to strike between identifying transactions where there a indications of higher fraud risks, and allowing customers to utilise their accounts with minimal unnecessary disruptions.

Having considered Mr B's payments to the fraudster and his account statements from the 12 months prior to the scam, I can see the second payment Mr B made to the fraudster of £3,000 was one of the largest he'd made in that 12 month period. However I still don't think a payment of this value was so out of character that first direct acted unfairly by not intervening at this point. I therefore don't think first direct should be held liable for the losses Mr B incurred when making the first two payments of £500 and £3,000 to the fraudster.

However, I do think that the third payment Mr B made of £9,000 was sufficiently out of character. This was significantly more than his usual account spending, occurred the day after the previous transfer, and was also an increased payment amount to a new payee, demonstrating a change in how he was utilising his account that is indicative of fraud. I therefore think first direct should have intervened at this point, making further enquiries with Mr B about the nature of the payment before processing it.

Had it done so, I think first direct would've had sufficient concerns that Mr B was at risk of financial harm from fraud and had it provided advice on these types of scams, I don't think Mr B would've proceeded with the payment. I say this because Mr B has explained that he believed this payment was genuine, largely due to having built a recent friendship with the fraudster, having seen the app and platform that demonstrated he was making successful investments and having also successfully received money back from those investments. These are all fairly known 'hallmarks' for these types of scams, which I think should have been known to first direct at the time. Therefore, had first direct asked how Mr B became involved in this investment, I think there would've been red flags that first direct could've advised Mr B on, which would've caused him to doubt what he had been told until that point. As first direct failed to intervene on this payment, and as I think that made a difference here, I think first direct is fully liable for reimbursing Mr B the funds he lost in this transfer. I think at this point Mr B hadn't been negligent in making the payments – I say this because Mr B had started investing a small amount to initially trial with, had valid reasons to think it was legitimate based on receiving returns and believed he had struck up a genuine friendship with the individual advising him. However I'm not persuaded the same can be said for the subsequent payments.

Mr B has explained that after he sent the £9,000 payment, his online trading app was blocked and he was told he needed to pay a 50% deposit to unfreeze it. Mr B has

acknowledged that this concerned him and he was worried at this point that he was falling victim to a scam. However, the next day he decided to pay the amount requested to avoid daily deductions to his profit.

I don't think that what Mr B was told by 'customer services' was plausible – while it's possible to imagine an app taking some form of commission on profits, I don't think 50% would be realistic. And likewise I don't think a fine of this value is realistic either. In this case particularly, Mr B was told the block was applied due to concerns over how Mr B obtained such profits – I don't see how a payment towards the app would allay these concerns so that it would unblock the account. I also think the reasons for the account block suggested Mr B might not be involved in something legitimate. Overall I think the message Mr B received from 'customer services' should've caused concerns. I appreciate Mr B was being told by both the fraudster and the 'customer services provider' to proceed, and that he was under pressured time constraints, but it seems Mr B did have genuine concerns at this point, and yet decided to proceed anyway in fear of losing profits he believed he'd made.

As Mr B had concerns when making the final three payments, but decided to proceed in spite of these, I think he should be held jointly liable for these losses, with first direct refunding 50% of the losses he incurred to acknowledge it also could've done more to stop the scam.

First direct has suggested that applying 8% simple interest to any refund would result in a 'windfall' to Mr B and that this figure is based on historic interest rates. Given the average costs of borrowing over time, its has long been our approach that this is a suitable rate to compensate for being deprived of funds and I'm satisfied it's fair to apply it in the circumstances of this complaint.

I appreciate this will be disappointing to Mr B, being a reduction in redress to what was previously recommended. But in all of the circumstances of the complaint, I think this is a fair outcome to reflect both party's responsibilities.

My provisional decision

My provisional decision is to partially uphold this complaint and for HSBC UK Bank Plc trading as first direct to refund Mr B:

- *£9,000 for the third payment Mr B made to the fraudster*
- *50% of payments four to six Mr B made to the fraudster*
- *8% simple interest from the date Mr B made these payments to the date of settlement.*

Both parties have now had the chance to respond to the provisional decision. Mr B raised the following further points:

- Many banks around the time of his fraud had banned crypto trades and some banks actively stopped any payments to the crypto wallet he used in 2021
- The FCA banned the cryptocurrency provider from trading in the UK temporarily a couple of months after Mr B's fraud had taken place
- Mr B now receives alerts for transactions he makes for any amount on his account, but this wasn't the case when the fraud occurred.

HSBC asked for clarification on whether it should make a deduction for 'profits' that Mr B received from the fraudster, as recommended by the investigator.

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 my overall findings on the case haven't changed and I'm partially upholding Mr B's complaint on the same grounds. I have thought about what Mr B has said since the provisional decision, but it doesn't persuade me to reach a different outcome.

I concluded that HSBC should have intervened when Mr B made the third payment to the fraudster, as this payment activity was out of character based on his usual account use. I agree with Mr B that payments made to cryptocurrency wallets should be deemed as higher risk by banks, based on the prevalence of scams. This is why I considered that *had* HSBC stopped the third payment Mr B made for further checks before processing it, it would've been able to identify that Mr B may be at risk of financial harm from fraud, based on what Mr B would've told it and could've stopped Mr B from proceeding with the payment.

However, not all payments towards cryptocurrency are scams – they can also be used for legitimate purposes and investments – so I don't think HSBC acted unreasonably by allowing payments to be made by Mr B towards a cryptocurrency wallet and also why I don't think HSBC should've intervened sooner than the third payment Mr B made. While I appreciate the FCA banned the wallet provider Mr B used shortly after he made these payments, as these bans weren't in place when the payments were made by Mr B, I don't consider it would be fair to have expected HSBC to treat these payments differently at the time they were made than payments to any other cryptocurrency provider.

In relation to HSBC's query, I don't consider it would be fair for HSBC to make a deduction for 'profits' it received from the fraudster. These 'profits' were linked to the first two payments Mr B made to the fraudster, which I've concluded HSBC weren't required to intervene on. Therefore these credits would've still been received by Mr B, even if HSBC had intervened at the point I consider it should've. I don't think any payments made by the fraudster in order to induce Mr B to invest further should reduce the liability of HSBC not intervening in subsequent payments.

For these reasons I remain of the view that Mr B and HSBC should each be partly liable for Mr B's losses, as set out in my provisional decision.

My final decision

My final decision is that I partially uphold Mr B's complaint and for HSBC UK Bank Plc to refund Mr B:

- £9,000 for the third payment Mr B made to the fraudster
- 50% of payments four to six Mr B made to the fraudster

8% simple interest from the date Mr B made these payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 1 June 2022.

Kirsty Upton
Ombudsman