DRN-3910502

The complaint

Mr S complains that HSBC UK Bank plc (trading as First Direct Bank) didn't do enough to protect him when he was the victim of a crypto investment scam.

Mr S is being supported by a representative, but for ease, I'll refer to Mr S throughout this decision.

What happened

In November 2020, Mr S was telephoned by someone (the scammer) about investing in crypto. The scammer told Mr S they were from an investment company (who I'll refer to here as 'P'). Because Mr S had seen crypto investments were doing well and was impressed by the professional approach used by the scammer, he decided to start trading with 'P'. He'd also carried out some online checks about 'P' and was reassured by the professional look of its website.

The scammer set up a trading account with 'P' and an account with a well-known crypto exchange (which I'll refer to here as 'K'). Both accounts were in Mr S's name. The scammer used remote access software to make the trades on Mr S's behalf.

Between 21 November 2020 and 27 January 2021 Mr S made nine payments to 'K' from his current account with First Direct via his online banking App. The payments ranged from £4,000 to £9,950 (a total of £57,374).

First Direct declined the first payment for £5,000 made to 'K' on 21 November 2020. After speaking to Mr S, First Direct released the payment, and allowed the subsequent eight payments to be processed without further interaction with Mr S.

Mr S initially had access to his trading account with 'P' which reassured him of its legitimacy, and he could see his investment was doing well. But Mr S was then unable to access the account and was told by the scammer it was being updated.

Mr S continued to communicate with the scammer over the telephone and was reassured his investment was doing well. He decided to withdraw some of his profits and was convinced by the scammer that to do this – he needed to pay a fee for the money to be released. When the withdrawal wasn't forthcoming, Mr S realised he'd been the victim of a scam. He reported the scam to First Direct in July 2021.

Unhappy with how First Direct was handling his case, Mr S complained. First Direct said it had contacted the beneficiary to try and recover the funds - but as Mr S paid the funds to an account in his own name with 'K' and it was unable to see where the money went after that – First Direct suggested Mr S contact 'K' to see if it could recover the funds for him. And because Mr S still had control of the funds after they left his First Direct account, First Direct said it couldn't take any further action.

First Direct also said it had spoken to Mr S about the first payment in November 2020 and he'd received online fraud alerts in respect of the subsequent payments.

Mr S remained unhappy and so referred his complaint to the Financial Ombudsman. He thought First Direct should've done more to protect him, irrespective of where the funds were paid to. And that it should've asked more questions specific to crypto investment scams when they'd spoken. Mr S said had First Direct asked appropriate questions when the first payment was made, then the scam would've been uncovered, and the loss prevented.

One of our Investigators considered the complaint but didn't uphold it. She was satisfied, given Mr S's appetite for risk, that he would've continued with the payments – regardless of any warnings First Direct gave. And she accepted First Direct was unable to recover the lost funds.

Mr S didn't agree and has asked for an Ombudsman's review. He said he didn't remember speaking to First Direct about the first payment – nor did he remember being asked any '*probing*' questions. He said had First Direct asked more questions, he would've said how he was contacted by the scammer and how the scam had unfolded. Mr S said First Direct should've recognised this as clear signs of a scam – and stopped the payment going through.

On 13 January 2023, I issued a provisional decision upholding this complaint in part. For completeness, I repeat my provisional findings below:

I should first point out that First Direct had an obligation to protect Mr S from financial harm, irrespective of what happened to the money after if left his First Direct account. And so, I'm considering Mr S's complaint about First Direct on that basis.

I accept the transactions Mr S made were authorised payments, even though he was the victim of a sophisticated crypto investment scam. So, although he didn't intend the money to go to the scammers, under the Payment Services Regulations 2017 and the terms and conditions of her account, Mr S is presumed liable for the loss in the first instance.

However, taking into account what I consider to have been good industry practice at the time, I consider First Direct 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 financial institutions 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*

Did First Direct do enough when it identified the risk?

First Direct identified the first transaction of £5,000 as suspicious. It tried to contact Mr S – but was unable to do so, so the transaction was reversed. Mr S telephoned First Direct on 21 November 2020 to ask why the payment hadn't gone through. Where there is interaction

between a bank and its customer in relation to a payment, we'd expect the bank to take this opportunity to find out more about the nature of the payment it declined.

Mr S doesn't recall the telephone call he had with First Direct – but also thinks First Direct should've asked more probing questions when they spoke to fully understand what was going on. I can confirm a telephone call did take place between Mr S and First Direct on 21 November 2020. And as part of my review, I've listened to that telephone call.

The telephone call starts by Mr S explaining that he'd tried to make an online payment, but it hadn't gone through. First Direct asked where the payment was going to, and Mr S confirmed it was going to 'K' – which he said was a 'Bitcoin wallet'.

Having checked its fraud records, First Direct confirmed it had reversed the payment as it hadn't been able to contact Mr S to confirm if the payment was 'genuine'. Mr S confirmed the payment was genuine and the payee details were correct.

First Direct asked Mr S how he'd got the details of 'K'. Mr S said he already had a trading account with 'K' and was happy it wasn't fraudulent – saying he'd 'been dealing with this guy for quite some time'.

Mr S told First direct that 'K' was a well-known online company and was used by many people as 'Bitcoin is going through the roof at the moment'. He said he'd set the account up with 'K' specifically to trade – and that every time he tries to move money he gets 'this problem with First Direct'.

First Direct said 'K' didn't offer a confirmation of payee check – and asked Mr S if he was happy to proceed or whether he wanted to do any more checks. It said if the payee was incorrect, Mr S might not be able to recover the money. Mr S said he was happy to go ahead with the payment to 'K' without further checks.

First Direct processed the payment and said it would contact the fraud team to ensure no further payments to 'K' would be declined.

I've thought carefully about whether First Direct asked the right questions during its interaction with Mr S to fully understand the nature of the transaction he was trying to make. And I do think it could've done more.

First Direct knew Mr S was trying to pay 'K' – a crypto exchange platform. But no questions specific to crypto investment scams were asked. By January 2019 we think firms had or ought to have had a good enough understanding of how these scams work. There's often no dispute that the payee (the crypto exchange) is legitimate and in the business of providing crypto because of a 'genuine' payment. But the heart of the scam is understanding whether anyone is in the background 'assisting' the customer and whether anyone has access to his crypto, and explaining the risks involved with that.

Whilst it's not up to us to dictate which questions firms should ask, First Direct could've, for example, asked how Mr S had been contacted, whether there was a 'broker' or 'account manager' helping him in the background, what checks he'd done, whether he had a trading account, whether he'd been able to successfully withdraw requested amounts from his trading account, whether the investment opportunity was linked to a prominent individual, advertised on social media etc. These are all typical features of crypto investment scams.

First Direct asked Mr S how he got the details for 'K' – but it didn't refer to trading accounts or contact he might have had from a broker. Nor did it ask whether anyone had taken control

of his computer or ask what checks he'd done – there was no reference to the Financial Conduct Authority (FCA).

First Direct's focus was very much on whether Mr S was making the payment himself, and whether he had the right details for 'K'. I don't consider these to be relevant to potential crypto investment scams. First Direct are the experts here – and so should've known that it is often the case a legitimate crypto exchange is used in the scam process to make it look more convincing and harder to detect. Ultimately 'K' was a legitimate company. But despite Mr S referring to his dealings with 'this guy', the line of questioning used by First Direct didn't draw out the involvement of 'P' – the scammer – or other common hallmarks of crypto investment scams.

So, I think First Direct didn't do enough once it identified the risk to Mr S.

Would appropriate intervention have made a difference?

I've thought very carefully about what Mr S would've said in response if First Direct had asked more detailed questions when they spoke. Of course, I can't know for sure, so I've thought about what I think is more likely than not to have happened, taking into account the particular circumstances of this case.

Mr S wasn't given a cover story by the scammer. And I think if First Direct had quizzed him more deeply on the investment itself - rather than purely focusing on 'K' - the presence of 'P', the fact he'd been 'cold called' and the use of remote access software would more than likely have all come to light. I also think Mr S would've divulged that he'd been the victim of a crypto scam before. Even if it was used as a way of him trying to convince himself (and First Direct) that this time everything was above board.

But Mr S being scammed before and the involvement of 'P' ought to have been a great concern to First Direct, and I'd have expected it to have questioned Mr S more deeply before being satisfied he'd carried out robust enough checks. Mr S is likely then to have explained that he'd checked information online about 'P', including its website, and had no cause for concern. And that he was able to access his account with 'P' and see how his investment was doing. But given how sophisticated crypto scams can be, and how they can involve cloned companies, cloned websites, and fake trading accounts, I'd still expect First Direct to have strongly reiterated to Mr S the need to check that 'P' was legitimate and whether there were any FCA, or other industry warnings, in place.

I must now think about whether this would've made a difference and prevented Mr S's loss. Given the number of scam hallmarks relevant to Mr S's investment that First Direct should've alerted him to, coupled with the fact he had already lost money in a crypto investment scam - I think it more likely than not that Mr S would've done more checks before proceeding with the £5,000 payment.

It's a common tactic of scammers to clone companies to make the scam appear genuine – and I can see there's a warning on the FCA website from December 2019 about this applying to 'P', and how an investor should be particularly weary if they've been 'cold called' – as was the case here. And because Mr S had already lost money through a scam – I think he would've followed the FCA guidance to check with the real 'P' – to make sure that was who he was dealing with. At which point the scam would've been uncovered, and the £5,000, together with all the subsequent payments (totalling £57,374), wouldn't have been lost.

Should Mr S bear some responsibility for his loss?

I have thought carefully about whether Mr S should bear some responsibility for his loss by way of contributory negligence (which might justify a reduction in compensation). And I think he should.

It's clear the material cause of Mr S's loss came from being tricked by sophisticated scammers. But his loss could also have been prevented had First Direct taken appropriate steps to intervene when his first transaction to 'K' appeared unusual.

But I think it's fair to say Mr S wasn't as careful as I reasonably think he ought to have been before choosing to invest with 'P', given he'd lost circa £50,000 six months previously through what he knew to be a crypto investment scam. Despite this, he was happy to invest again, albeit through a different trading company and crypto exchange, fully aware of the risks involved. He also didn't warn First Direct that he'd been the victim of scam when he lost the money in June 2020, instead waiting until the summer of 2021 to report either scam to First Direct. This all suggests to me that Mr S wasn't afraid of taking financial risks and accepted the consequences of doing so.

The investment with 'P' also had hallmarks that were very similar to the scam he'd fallen victim to six months before. While the method of contact was different between the two scams – with the first Mr S was contacted in response to an enquiry he made, whereas with the second scam Mr S received a cold call – it seems the scams were otherwise operated in a very similar way.

In both scams, a 'broker' was involved who said they would trade on Mr S's behalf, and remote access software was used. And Mr S was given access to his trading accounts which appeared to show his investments making good returns.

When asked what had convinced Mr S to invest on each occasion, he explained that in both cases he thought the scammer was 'highly personable'. In relation to 'P', Mr S – had found the website to be 'flawlessly professional'.

Mr S doesn't appear to have done any checks on the broker in relation to the first scam – but did do some online checks in respect of 'P'. I appreciate Mr S could reasonably have been convinced by the professional presentation of the initial scam and the personable nature of the scammer. But I would've expected him to be more cautious before attempting to invest with 'P' given he now had knowledge and experience of how a crypto investment scam could operate and had lost a considerable sum of money as a result.

As such, I think a reasonable person in the same position as Mr S would've carried out more thorough research into 'P' and wouldn't simply have relied on its professional online presentation before attempting to enter into a new risky investment opportunity. While I appreciate Mr S carried out some rudimentary checks online before investing in 'P', had he carried out further research or sought guidance before investing, I think it would've come to light that there was an FCA warning against 'P' and that the investment opportunity once again bore the hallmarks of a scam.

Overall, while I appreciate Mr S carried out some checks before investing with 'P', I don't think he carried out sufficiently thorough checks to enable him to establish the legitimacy of the company he was dealing with before investing very large sums in high-risk trading. I think he ought reasonably to have done more.

So, in the circumstances, I think it's fair that he bears 50% of the responsibility of the losses he incurred because of the second scam.

For the reasons given above, I currently intend to uphold this complaint in part and direct HSBC UK Bank plc (trading as First Direct Bank) to refund Mr S all his disputed payments, less 50%. The total disputed payments are £57,374, that would amount to an award of ***£28,687.***

This was a current account and so First Direct should add interest to that sum (less any tax properly deductible) at 8% simple per year, from the respective dates of loss to the date of refund.

I invited Mr S and First Direct to provide me with any additional evidence or information they wanted me to consider before issuing my final decision.

First Direct accepted my provisional decision but disputed the level of interest I was awarding. It said the funds had originated from Mr S's savings account (Bonus Saver) – and so interest applicable to that account should be awarded.

Mr S also accepted my provisional decision and confirmed that the funds originated from his savings account.

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.

As both parties accept my provisional decision, I see no reason to depart from what I said. But having now had confirmation from Mr S that the funds originated from his savings account – I agree with First Direct that an award of 8% interest isn't appropriate.

Putting things right

First Direct should've done more to protect Mr S from the risk of financial harm from fraud. But Mr S should've taken more action to mitigate the risk. So, First direct should refund Mr S all his disputed payments, less 50%, and pay interest at the rate he was receiving on the savings account the funds originated from - from the respective dates of loss to the date of settlement.

My final decision

My final decision is that this complaint is partly upheld. HSBC UK Bank plc (trading as First Direct Bank should:

- Refund **£28,687** of the £57,374 Mr S transferred to the scammer.
- Pay simple interest at the rate applicable to the originating savings accounts on this amount, per year (less any tax properly deductible) from the respective dates of loss to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision **before 21 February 2023.**

Anna Jackson
Ombudsman