DRN-3677853

The complaint

Mr P is unhappy Citibank UK Limited wont refund money he lost as a result of a third-party scam. Mr P believes Citibank failed in its due diligence and failed to protect him from the scam.

What happened

Mr P told us that in July 2021, his friend recommended him to a trading site (I will refer to as H). Mr P says H appeared to be endorsed by a famous and influential businessman. Shortly after completing his details online, he was contacted by a representative from H. The initial transfer ($250) was declined by the bank and Mr P was directed by H to another page. Over the following days Mr P was provided with tips and education on how the platform worked and this was done through an interactive session using a remote desktop application.

Mr P then made a further transfer of $40,000. This was also declined by the bank. So, H suggested transferring the money via a cryptocurrency exchange – which Mr P did. When Mr P made the transfer of 33,756 Euros to the cryptocurrency exchange on 17 July 2021, the bank did call before making the transfer.

Citibank didn't provide much information and stopped responding to the investigator's request for further information – in particular it didn't provide the call that took place. As I understand from earlier correspondence, it considers the loss did not occur from Mr P's Citibank account but from his cryptocurrency account where the money was moved to before being moved on to the scammer.

The investigator reached his opinion based on the evidence he had available to him. He concluded that Citibank would have been aware of investment and crypto trading scams at the time - particularly where someone is trading on the investor's behalf with funds going to the consumer's own cryptocurrency account, is a well-known and common scam trend. He believed the scam could have been exposed and prevented.

I issued my provisional decision on 31 October 2022 explaining why I had reached an outcome that differed in some respects to the investigator.

Citibank responded, providing the call recording and further file submissions. Briefly it said:

- The agent was not advised the consumer was in a hurry and the tone of the call did not suggest this and the client mentioned he was happy to receive such calls.

- The agent did ask who he was paying his cryptocurrency to and how he had heard about the trader but the level of detail provided by the consumer to the ombudsman, was not provided by the client on the call, even after probing.

- Even without the withheld information (later provide to the ombudsman) the agent still managed to cause audible doubt with the consumer; however, he still opted to proceed.

Mr P also responded and, having had the opportunity to listen to the call recording, provided the following comments:

- The call is very short for such a large transaction and questioning weak in determining which trading platform was being used.

- The recommendation from a friend was based on an advert from a national newspaper.

- Whilst his tone may not have suggested he was in a rush; he was late for picking up his son.

- There should have been enough doubt form his answers that he was in the middle of a scam and the bank could have insisted he looked at the trading platform in more detail before going ahead.

- The agent did not push for any detail on the trading company.

- Asking whether he trusted them is not getting to the fact of who the trading company is and whether they should be trusted.

In relation to my provisional decision Mr P made the following comments:

- Modern communication methods such as WhatsApp are now accepted as a messaging service and no less secure than text message which is commonplace with financial institutions. It is not like other social media where unauthorised access has been reported. The UK mobile number used to set up the WhatsApp service did not create cause for concern coupled with the comprehensive account setup process. Many landline calls were made form H which appeared to be a London prefix and the scammer sounded credible.

- Being an experienced IT professional, he is conscious not to save sensitive details on devises that haven't been password protected or encrypted. Therefore he didn't consider the sharing of screens risky.

- The advert from one of the most influential businessmen today on a recognized national newspaper website did not raise suspicion particularly with such a comprehensive enrolment process.

- In respect of being told to lie to his bank about the purpose of the transaction, whilst

this may seem naïve, he believed it would help speed up the administration process.

- There wasn't enough in the media at the time to make the public aware of such scams having seen no FCA adverts or communications. Seeking out such warnings proactively from the FCA website doesn't seem reasonable and the bank could have verified H through the questions which could have resulted in pointing him to the FCA website.

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 consider the comments both parties have made, I see no reason to depart from the conclusions set out in my provisional decision. I have concluded that the fair and reasonable outcome, in all the circumstances, would be to uphold this complaint in part. For completeness, I have set this out below and addressed any relevant comments within my decision.

Should Citibank have prevented the payments from being made?

In broad terms, the starting position at 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 have taken that into account when looking into what is fair and reasonable in this case.

It is not in dispute that Mr P authorised the scam payments. It is also not in dispute that Mr P was duped by the scammers into instructing the bank to transfer money to a cryptocurrency account and on from there into the scammer's account. The scammers deceived him into thinking he was making a legitimate cryptocurrency investment for further trading. As I understand it, payments to the cryptocurrency provider were used to purchase cryptocurrency which was then placed in a wallet in Mr P's name and from there the scammer moved the money into his own wallet. So, although Mr P did not intend the money to go to the scammers, under the Payment Services Regulations 2017, and the terms and conditions of his account, Mr P is presumed liable for the loss in the first instance.
But, taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Citibank 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 make 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.

Citibank says that, as the fraud occurred on the cryptocurrency account, it is not liable for any loss. But, I don't agree that Citibank is not liable simply because the money was transferred to an account in Mr P's name and the fraud then happened from there. As I've mentioned above, Citibank had a responsibility to be on the lookout for unusual activity and protect consumers from financial harm.

As a financial services professional, I think Citibank would have been aware at the time that fraudsters use genuine firms offering cryptocurrency as a way of defrauding customers and that these scams often involve money passing through more than one account.

Cryptocurrency scams had been increasing in frequency and both the Financial Conduct Authority (FCA) and Action Fraud had published specific warnings about these scams in 2018. In my view, by the time of these transactions, Citibank had had time to understand these warnings and be on the look at for this particular type of fraud.

And it seems that there were fraud triggers in this case because Citibank did in fact intervene and called Mr P to ask about the second much larger transfer. The fact that this did trigger suggests that Citibank did identify a fraud risk. I don't think the first transfer of $250 was sufficiently large to have caused Citibank to intervene but the second, much larger transfer ought to have done.

So, the bank was sufficiently concerned about the possibility of fraud to ask questions and warn of warn of fraud and scams. Accordingly, it's just a question of whether it did *enough* in all the circumstances.

Citibank provided the call recording in response to my provisional decision and Mr P has had the opportunity to comment on the call. Staff had noticed the payment was being made to a cryptocurrency provider and were calling to check whether Mr P had authorised the payment.

Having listened to the call, the agent confirms there have been a number of cases where customer have been duped into transferring money to cryptocurrency and then had their money stolen from the cryptocurrency account. And the agent explains that from there - it's hard to trace. In response to the agent, Mr P explained he is doing the investment through a reputable broker - recommended by a friend. When the agent repeats back to Mr P - *so you're doing it through a reputable broker and you know them personally*, Mr P responds that *it's a good point actually - I don't know whether I should do such a large amount maybe I should do a smaller amount and see what happens*. The agent recommends doing a smaller amount. And Mr P then goes on to confirm that he will just double check because the agent had got him thinking.

I do think the call is quite good (and it does cast some doubt in Mr P's mind which I will discuss below). It does talk about the specific scam that Mr P fell victim to, and some basic questions are asked. But I do think Citibank could have probed more about who the trader was and how he'd heard (or his friend had heard) about the trader – particularly given the audible doubt in Mr P's response.

And, I do think with more probing that Mr P would have told them his friend had told him about H and that it was endorsed by a celebrity/influential businessman in a national newspaper. And if Citibank had given Mr P some warnings about cryptocurrency scams including telling him that scam investment companies often contact their victims after they've reacted to an advert involving celebrities on social media platforms, help them set-up genuine third-party accounts for payments to pass through and request remote access to their computers. With further questioning, I think Citibank would have been concerned and put on notice that Mr P was falling victim to a scam. I think this would have caused sufficient

doubt in Mr P's mind not to proceed with the payment. In other words, if Citibank had carried out further or better questioning in line with the bank's duty of care, it seems probable that Mr P would have become credulous about the scam in time and stopped the payment in its tracks. The fraud would have failed; and Mr P would not have lost 33,000 Euros.

Could Mr P have done more to mitigate his losses?

I've thought carefully about what Citibank's obligations were, as set out above. But another key issue is whether Mr P acted reasonably taking into account all the circumstances of the scam. So, I have also considered whether Mr P should bear some responsibility by way of contributory negligence.

It's clear that the call did cast some doubts in Mr P's mind. I do think Citibank said things that caused Mr P concern and he did say he would check things out further. He was also told by the agent to transfer a smaller amount – but didn't do this. By his own admission, Mr P didn't do proper research until after his wife asked him the sort of questions, he considers the bank should have asked him. He relied on the fact that the opportunity was endorsed by a celebrity/influential businessman and national news medium. As I outlined in my provisional decision I think there were a number of red flags that ought to have caused Mr P concern, such as the communication method, sharing of computer screens, advice by the scammer to lie to the bank about the purpose of the transfer. I have noted Mr P's comments in response to these points and whilst I acknowledge that there could be an explanation behind each of the points I've mentioned, when they are all taken into consideration together and holistically - they should have caused concern. Perhaps more significantly, in the context of the conversations during the call about the transfer, I don't think Mr P did enough to disregard some of the clearer warning signs here.

There were warnings on the FCA website about H at the time. I am not saying that Mr P should have specifically gone to the FCA website. But Mr P did say when he did do some research after the event, he quickly realised it was a scam. So, it seems that information was easily available, and I think even a basic search on the internet about cryptocurrency investments and/or H would've provided at least some results which would've indicated that the offer was probably fraudulent.

On that basis, I think it's reasonable for Mr P to share the responsibility with Citibank and reduce the refund on the payment by 50%.

I realise Mr P has been the victim of a cruel scam. I sympathise with him for that and I know he will be disappointed by this decision. But I do think this is the fair and reasonable outcome in all the circumstances of this complaint.

Putting things right

I require Citibank UK Limited to refund 50% of the payment Mr P made on 14 July 2021 (33,000 Euros), along with simple interest at the rate of 8% per annum from the date of transfer to the date of settlement to compensate Mr P for the loss of use of his money.

If Citibank is legally required to deduct tax from the interest, it should send Mr P a tax deduction certificate so he can claim it back from HMRC if appropriate.

My final decision

My final decision is I uphold this complaint in part, and I require Citibank UK Limited to put things right for Mr P as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 12 December 2022.

Kathryn Milne
Ombudsman