DRN-4521386

The complaint

Mr K is unhappy that Citibank UK Limited will not refund the money he lost as the result of an authorised push payment (APP) scam.

Mr K has brought his complaint through a representative, for ease of reading I will refer solely to Mr K in this decision.

What happened

As both parties are now familiar with the details of the scam I will not repeat them here in full. In summary, between 2 May and 12 May 2023 Mr K made 15 faster payments to an account in his own name at a cryptocurrency exchange as set out below:

date	value, £		date	value, £
02/05/2023	15,000		09/05/2023	5,000
02/05/2023	15,000		09/05/2023	3,000
03/05/2023	10,000		09/05/2023	1,000
09/05/2023	28,000		10/05/2023	49,500
09/05/2023	12,000		10/05/2023	21,000
09/05/2023	10,001		10/05/2023	15,500
09/05/2023	10,000		12/05/2023	44,000
09/05/2023	5,000		total	244,001.00

Mr K moved £4,653.05 back from his crypto account (£25 as an initial test and the balance on 15 May 2023 when he was concerned he had been scammed) so his total loss was £239,347.95.

Mr K understood he was making payments to allow him to access tasks that he would complete for a company that developed apps. He would then be paid a commission in cryptocurrency. As Mr K could see his commission increasing on the scammer's website, he tried to withdraw it. When he was told he would first need to pay fees he realised he had been scammed and made no further payments.

Citibank says Mr K authorised the transactions using a one-time passcode and it followed its legal obligations to complete the payments. It said this should be progressed as a civil dispute and a loss on an unregulated investment, rather than a scam.

Mr K says the bank only spoke to him twice during this period and its calls were not effective. Had it asked the right questions it could have uncovered the scam and prevented his losses.

Our investigator did not uphold Mr K's complaint. He said he was satisfied it was a scam, not a civil dispute. He thought Citibank ought to have intervened sooner than it did (9 May 2023) but did not think an earlier intervention would have changed the outcome. He said the call recordings do not support Mr K's testimony about the calls. He found Citibank made clear what the purpose of each call was and Mr K inaccurately said the payments were for real

estate investment.

So the investigator concluded calling earlier would not have successfully broken the scam as Mr K did not answer the bank's questions in an open and transparent manner. This meant it did not have the opportunity to try and uncover the scam. And he concluded that Citibank had done what it could to try to recover Mr K's money once he contacted it.

Mr K disagreed and asked for an ombudsman's review. He said Citibank was presented with enough red flags that meant it should not have followed his instructions. It should have referred him to a branch and invoked the banking protocol because the typical hallmarks of a scam were present.

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.

The first question we typically look to resolve in cases such as these is whether the company, so here the app development company, was actually operating a scam. I am satisfied it was and disagree with Citibank's comment in its final response letter that this is a civil dispute about an unregulated investment. This has all the traits of an employment or task scam – where a victim believes they are completing tasks online and will be paid for the tasks completed. To gain access to these tasks, users typically have to pay an 'unlocking fee'. And there will often be 'combination tasks' that require more money to be deposited to access higher payments in return. So I am satisfied Mr K sadly fell victim to a cruel scam.

There's no dispute that Mr K made and authorised the payments. Mr K knew why he was making the payments. At the stage he was making these payments, he believed he was 'buying' access to tasks that would allow him to generate income. I don't dispute Mr K wasn't 'buying' what he thought he was, but I remain satisfied the transactions were authorised under the Payment Services Regulations 2017.

It's also accepted that Citibank has an obligation to follow Mr K's instructions. So in the first instance Mr K is presumed liable for his losses. But there are other factors that must be considered.

To reach my decision I have taken 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. To note, as the payments were made to another account in Mr K's name the principles of the Contingent Reimbursement Model (CRM) code do not apply in this case. This means I think that Citibank should have:

- been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.
- had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (amongst 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, taken additional steps or made additional checks before processing a payment, or in some cases declined to make a payment altogether, to help protect its customers from the possibility of financial harm.

In this case I don't think Citibank can fairly be held liable for Mr K's losses. I'll explain why.

I think that Citibank ought to have intervened on 2 May 2023, arguably after the first, or at the very least the second, payment given their value and proximity. Whilst Mr K did often make relatively high value payments, I can only find one payment over £10,000 (£30,000 on 16 December 2022) in the previous 12 months of his banking activity. So I find two payments for £15,000 made on the same day were somewhat out of character for Mr K's account.

This means I need to consider what the likely outcome of an effective intervention would have been. In this case I have the advantage of Citibank having spoken with Mr K on 9 and 10 May 2023 so I can better know how Mr K would most likely have responded had the bank made an earlier call to intervene.

Mr K says that he told Citibank he was paying to complete tasks and would receive payment for his work in cryptocurrency, but that is incorrect. On two separate calls Mr K told Citibank the reason for the payments was 'real estate investment'. So I am not persuaded that he would have disclosed the real reason had there been a call a week earlier. This would have meant it would be very hard for Citibank to accurately assess the risk of financial harm to Mr K. And there were no signs in Mr K's demeanour that he was being scammed – he came across as calm and confident in the conversations, so I can't fairly say there was anything there that Citibank ought to have picked up on.

I note that Citibank failed to ask any follow up questions about the alleged real estate investment when Mr K gave this false reason for the payments. And we would expect it to. However, I have seen no evidence to persuade me that had Citibank asked follow-up questions it would have led to the scam being exposed. I think it is more likely Mr K would have responded with sufficient credibility and plausibility such that Citibank would reasonably have processed the payments. The calls that did happen show he had no intention of disclosing the real purpose of the payments to Citibank.

In addition, Mr K was moving money to an existing linked account in his name that he had used previously in 2021 and three times in the previous month in 2023. So, in the round, I do not agree that Citibank ought to have acted contrary to Mr K's instructions and declined to process the payments, or asked Mr K to attend a branch, as he suggested.

I have then considered whether Citibank did what we would expect to try to recover Mr K's money after the scam was reported. I note this was two months later in July. Mr K didn't instruct Citibank to send these payments directly to the scammer, but instead to an existing cryptocurrency trading account in his own name. And that's what Citibank did. I don't think it was ever going to be likely that Citibank would have been able facilitate recovery of these payments after Mr K had moved the payments onto the scammer

This means I am not instructing Citibank to refund any money to Mr K.

I'm sorry Mr K lost a considerable amount of money which was very distressing for him. I can understand why he would like to be compensated for his losses. And I do accept Mr K has fallen victim to a sophisticated scam. But I can only consider whether the bank, which had no involvement in the scam itself, should be held responsible for what happened. For the reasons set out above I do not find Citibank can be held liable in the circumstances of this case.

My final decision

I am not upholding Mr K's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or

reject my decision before 9 February 2024.

Rebecca Connelley
Ombudsman