DRN-4248926

The complaint

Mr T complains that Revolut Ltd ("Revolut") won't refund £5,750 he lost to an investment scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat everything again here. In brief summary, Mr T fell victim to an investment scam in July 2022 after he found an investment opportunity on social media. He was contacted by a fraudulent broker ("the scammer") who encouraged him to invest in cryptocurrency. He opened an account with a cryptocurrency platform and three payments were made from his Revolut account between 26 and 27 July 2022 totalling £5,750.

Mr T said he wasn't sure how the payments were made and that he thought it was the scammer that set up the payments via remote access software. However, Revolut didn't consider the payments to be unauthorised as it said its app restricts access if remote access software is being used, so it thought the payments would've likely been authorised by Mr T. It also said the payments did not flag as suspicious, so there was no reason for it to have intervened. Unhappy with this, Mr T referred the matter to our service.

Our investigator didn't uphold Mr T's complaint. She thought the payments were likely authorised by Mr T, as he had said he was aware that payments were being made from his Revolut account to his cryptocurrency wallet as part of the investment. And she didn't think the payments were unusual enough to have warranted an intervention or tailored scam warning from Revolut, so she didn't think it could be held liable to refund the money Mr T lost.

Mr T disagreed, so the matter has been escalated to me to determine.

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, I agree with the conclusions reached by the investigator and have decided not to uphold it. I'll explain why.

The Payment Service Regulations 2017 ("PSRs") say that a payment transaction is authorised by the payer where they have given their consent to the execution to the payment transaction. Such consent must be given in the form and in accordance with the procedure agreed between the payer and the payment service provider.

Unless the payment service provider can show consent has been given, it has no authority to make a payment or debit the customer's account. Where a payment service user denies having authorised a payment transaction, it is for the payment service provider to prove that the payment transactions in question were authorised by the customer.

Having considered the facts before me as well as the relevant law, the first question I need to determine here is whether it is more likely than not that Mr T authorised the transactions. In other words, I need to decide whether he made the transactions himself or gave someone permission to do so.

Mr T said that he made the initial payment of £500, but that it was the scammer who made the subsequent payments of £3,400 and £1,850. He says that, while using Anydesk, he opened his Revolut app and says they made the payments to his crypto wallet, saying it was for "advanced verification checks" for Binance.

The PSR 2017 do allow for payment transactions to be initiated by someone acting on behalf of the account holder, which can be agreed informally (e.g. by the account holder asking or permitting a third party to undertake a task on their behalf). And if the account holder has permitted a third party to appear as if they have the consumer's authority to make payment transactions, those payment transactions will likely be authorised, even where the consumer didn't ask the third party make any payments or know about them.

Revolut has said that it wouldn't have been possible for the scammers to take control of Mr T's device to make payments from his Revolut app as it restricts access if remote access software is detected. So, it seems unlikely that the scammers would've been able to make the payments in the way Mr T has described, and I note his representatives have also accepted that he may have been confused about how the payments were actually made. So, I think the payments were more likely than not to have been carried out by Mr T on his Revolut app, albeit I accept he may not recall doing this.

Even if the scammers could have somehow made the payments using remote access software, he knew the scammers would be transferring money out of his account and into his crypto wallet. So, if it *wasn't* Mr T who made the payments, I think it's still likely he knew that payments were going to be made from his account, and that he had therefore given permission/consent for those payments to be made on his behalf.

I have therefore treated all of the disputed payments as having been authorised by Mr T. And the starting position in this scenario is that banks ought to follow the instructions given by their customers in order for legitimate payments to be made as instructed, with Mr T being presumed liable for the loss in the first instance.

However, I've considered whether Revolut should have done more to prevent Mr T from falling victim to the scam, as there are some situations in which a firm should reasonably have had a closer look at the circumstances surrounding a particular transfer. For example, if it was particularly out of character.

Having reviewed the three payments Mr T made as part of the scam, I don't consider they were unusual or suspicious enough to have warranted any form of warning or intervention by Revolut. The payments were made to an account in Mr T's own name, and were spread across three transactions, neither of which were significantly large in value such that they ought to have given Revolut cause for concern that Mr T was at risk of financial harm. Given the account had only recently been opened, Revolut also didn't have any historical transaction data to compare this spending with to be able to determine if it was out of character or not. And overall, I'm not persuaded there were any significant indications of fraud that would have required Revolt to have fairly and reasonably made further enquiries.

So, having considered the payments Mr T made to his crypto wallet, I'm not persuaded there was anything that ought reasonably to have triggered Revolut's fraud monitoring systems, or that would have indicated he was in the process of being scammed.

I note that Mr T's representatives have also said he was vulnerable at the time of the scam due to his age. But I'm not persuaded his circumstances would amount to him being considered as *vulnerable*, and neither do I think Revolut ought to have been aware of any vulnerabilities either. Revolut's duty first and foremost is to execute transactions at the request of its customers. And given there was nothing to put it on notice that Mr T was vulnerable or lacked capacity to make his own financial decisions, I don't think it was under any obligation to put extra measures in place as a result.

I've also thought about whether there was anything more Revolut could have done to recover the funds. However, in this instance, we know the payments were made to Mr T's own crypto wallet before being swiftly moved on to the scammer, so there would've been no reasonable prospect of Revolut being able to recover any money from the receiving account in such circumstances.

I appreciate this will likely come as a disappointment to Mr T, and I'm sorry to hear he has been the victim of a cruel scam. However, in the circumstances, I do not consider it would be fair and reasonable to hold Revolut liable for his loss.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 27 December 2023.

Jack Ferris
Ombudsman