DRN-5383016

The complaint

Mr J complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by a job scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr J had been looking for work and discovered an opportunity to work part-time reviewing items for a platform which I'll refer to as "P". The job required him to make deposits in cryptocurrency in return for commission on completion of tasks. He was guided through the process via WhatsApp by someone I'll refer to as "the scammer", who explained that he would be required to simulate purchasing products to improve the algorithms of each product, which would improve the chances that the merchant would be able to sell the item.

Mr J checked P's website and was satisfied it was a genuine company. He wasn't given any employment documents, but he was given access to a portal which allowed him to see his account balance, which further reassured him the opportunity was genuine.

The scammer added Mr J to a WhatsApp group with others performing the same role and told him to open accounts with Revolut, and an EMI I'll refer to as "W". He also asked him to first purchase cryptocurrency and then load it onto an online wallet. Between 27 July 2023 and 31 July 2023, Mr J made eleven transfers from Revolut to seven different recipients, and on 29 July 2023, he made a card payment for £5,600 to a cryptocurrency exchange I'll refer to as "M". The total value of the payments from Revolut was £11,157.72.

On 31 August 2023 Mr J made five payments from W to M, and one payment to C. And on 1 September 2023, he made a further payment to M. The total value of the payments was £17,350 (most of which was either refunded or recovered).

Mr J was able to make a withdrawal early on and completed two sets of 40 tasks, but when his account showed a negative credit, he was told he'd have to make further deposits. He realised he'd been scammed when another bank contacted him to discuss a payment he was making from that bank, and he discovered P was operating a scam.

Mr J complained to Revolut with the assistance of a representative who said he was making payments from a newly opened account to a high-risk cryptocurrency merchant, which is a known fraud trend, and there was a large amount of money moving in and then out of the account in a short period of time, which should have been suspicious to the bank. They said that if Revolut had intervened, it would have seen that there were red flags present including the fact Mr J had found a job opportunity on social media, he hadn't received an employment contract, and he'd been asked to pay deposits in advance as well as fees to withdraw funds he'd already earned by working.

Revolut refused to refund any of the money Mr J had lost. It explained there were no chargeback rights because the card payment was verified via 3DS. It was unable to take any

action regarding the transfers until it had more information, and its recovery attempts were unsuccessful. Mr J wasn't satisfied and so he complained to this service with the assistance of his representative.

Responding to the complaint, Revolut explained Mr J was given its new beneficiary warning before payments to each new beneficiary as follows: "Do you know and trust this payee? If you 're unsure, don 't pay them, as we may not be able to help you get your money back.

Remember, fraudsters can impersonate others, and we will never ask you to make a payment." For four of the payees, he was also asked about the purpose of the payment, and he answered cryptocurrency, paying Revolut, goods and services payment, and something else. This resulted in a further, more granular warning message based on the stated purpose of the transaction. He was then presented with options to "cancel payment", "pay anyway", "get advice from agent" or "read our scam guidance", in response to which he selected "pay anyway".

Revolt argued that the fraudulent activity didn't take place primarily on the Revolut platform as it was used as an intermediary to receive funds from Mr J's main bank account before the funds were transferred to accounts held with cryptocurrency exchanges in Mr J's name. It further argued that Mr J wasn't acting in the heat of the moment and should have done more due diligence having received several warnings about the possibility of being a victim of a scam.

Our investigator recommended that the complaint should be upheld. He noted that Mr J had been asked about the purpose of the payments and shown a cryptocurrency scam warning, but for the card payment he made to M on 29 July 2023, he thought Revolut should have asked a series of questions in an attempt to narrow down the specific scam risk and once that risk had been identified, it should have provided a warning which covered off the key features of the scam risk identified. And had it done so he thought the scam would have come to light and Mr J's loss would have been prevented. He said Revolut should refund the money Mr J had lost from that payment onwards, but that the settlement should be reduced by 50% for contributory negligence because he ignored clear red flags, including the fact he'd found the job on social media, and the returns were unrealistic.

Finally, our investigator was satisfied there wouldn't have been any prospect of a successful recovery and there were no chargeback rights as the card payment was to a legitimate cryptocurrency wallet, where the funds were utilised.

Revolut asked for the payments to be reviewed by an Ombudsman, arguing that the complaint wasn't properly investigated and citing the Supreme Court's judgment in Philipp v Barclays Bank UK plc [2023] UKSC 25, where the Court held that in the context of APP fraud, where the validity of the instruction is not in doubt, no inquiries are needed to clarify or verify what the bank must do.

It argued this service irrationally failed to consider the fact the card payment was self-to-self and obviously distinguishable from transactions subject to the regulatory regime concerning APP fraud. And there is no rational explanation as to why our investigator considered it should be held responsible for 50% of Mr J's loss where the relevant transaction is self-to-self.

Finally, it argued that it gave appropriate warnings which were negligently ignored, and Mr J failed to do sufficient due diligence.

My provisional findings

I issued a provisional decision on 16 February 2025 in which I stated as follows:

I'm satisfied Mr J 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr J is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr J didn't intend his money to go to scammers, he did authorise the disputed payments. Revolut is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

Prevention

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in July 2023 that Revolut should:

• have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;

• have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

• in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;

• have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi- stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

I've thought about whether Revolut could have done more to prevent the scam from occurring altogether. Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr J when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Revolut to intervene with a view to protecting Mr J from financial harm due to fraud.

I've taken into account the 2023 Supreme Court judgement in the case of Philipp v Barclays. But nothing within that judgement said that firms couldn't make fraud-related enquiries with

customers or provide warnings (which Revolut, in any case, does), for example by providing a warning during the payment journey or giving itself the right under its terms and conditions to decline a payment in order to establish the circumstances surrounding it. And, in circumstances where its customer might be at risk of financial harm from fraud, as a matter of good industry practice, and taking into account the FCA's Consumer Duty, as well as what's fair and reasonable, I think that Revolut ought, in some circumstances, to have made additional checks or provided additional warnings before processing a payment.

The first six payments were to individual payees, there wouldn't have been any indication that he was buying cryptocurrency, and the payments were low value, so I'm satisfied a new payee warning and questioning about the purpose of the payment was a proportionate response to the risk presented by the payments. I'm also satisfied that the warning messages based on the responses Mr J gave were proportionate.

However, on 29 July 2023, Mr J made a card payment to M for £5,600 and based on the amount and the fact the payment was identifiably for cryptocurrency, I agree with our investigator that Revolut ought to have done more.

I think a proportionate response would have been for Revolut to have provided a written warning covering some of the key features of cryptocurrency-related investment scams, including that victims are usually targeted via social media or email, scammers will utilise fake positive reviews from other individuals, or fake celebrity endorsements and fake online trading platforms.

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case, and, on the balance of probabilities, I don't think it would have. This is because Mr J was the victim of a job scam and so I don't think a warning about investment scams would have resonated with him because he considered he was earning money and not investing it. So, I don't think an intervention at this point would have stopped the scam.

I've considered whether Revolut could have done anything else to stop the scam and as the rest of the payments Mr J made from Revolut were low value, I wouldn't have expected it to have intervened again.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr J made the card payment to an account in his own name and moved the funds onwards from there. And Revolut has explained that it didn't receive a response from the accounts to which Mr J made the transfers.

Mr J's own testimony supports that he used a cryptocurrency exchange to facilitate the card payment. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchange would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr J's payment, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Revolut's decision not to raise chargeback request against the cryptocurrency exchange company was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr J to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think he is entitled to any compensation.

Developments

Mr J's representative has made some additional comments.

They maintain Revolut ought to have intervened because the account was newly created and being funded from an external account in Mr J's name, and he was sending significant and frequent payments to a cryptocurrency merchant, which is a known pattern of fraud.

They've argued that my conclusion that Revolut ought to have provided a written warning covering off some of the ley features of common cryptocurrency scams is contradictory to other final decisions where our Ombudsman have taken the view that banks and EMIs are expected to be on alert for job/task-based scams. They've argued that there should have been a human intervention and as Mr J wasn't coached to lie, Revolut would have detected the scam and provided a written warning tailored to job scams, which could have stopped the scam.

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.

I've considered the additional comments, but I'm afraid the findings in my final decision will remain the same as the findings in my provisional decision. I agree there should have been an intervention in this case, and I maintain this should have happened when Mr J made the payment for £5,600 on 29 July 2023. However, I also maintain that an appropriate intervention in July 2023 for a payment of that amount to a cryptocurrency merchant would have been a tailored written warning relevant to cryptocurrency investment scams. And as Mr J was the victim of a job scam, this wouldn't have resonated with him because he considered he was earning money and not investing it.

I accept Mr J would likely have disclosed information which would have identified that he was the victim of a job scam if Revolut have questioned him via its live-chat facility, but I wouldn't expect it to have done that. And as there would have been no other indication that he was paying for tasks he expected to be paid for, I don't accept there would have been any reason for Revolut to have provided a warning which was relevant to job scams.

I'm sorry to hear Mr J has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Revolut is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 7 April 2025.

Carolyn Bonnell
Ombudsman