DRN-5041736

The complaint

Mr W complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment 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.

In March 2023, Mr W saw an advertisement on social media for an investment company I'll refer to as "O". The advert claimed that O used expert brokers to train beginners how to trade, and that he'd be able to start trading with a small deposit.

He completed an online enquiry form and was contacted by an individual who I'll refer to as the "scammer", who explained he'd help him to invest in cryptocurrency. Mr W thought the scammer seemed professional and knowledgeable and when he checked O's website, he was satisfied it appeared genuine, and he didn't see any negative reviews.

The scammer told Mr W to open an account on O's trading platform, which required him to provide photo ID. He also told him to download AnyDesk remote access software to his device which would allow the scammer to trade on his behalf.

The scammer told Mr W to open an account with Revolut and to first purchase cryptocurrency through a cryptocurrency exchange company and then load it onto an online wallet. Between 15 March 2023 and 22 May 2023, he made sixteen faster payments and three debit card payments to five different beneficiaries totalling £190,696 (£42,600 was received back into the account through refunds).

Between 20 March 2023 to 31 March 2023, Mr W could see his profits increasing on the trading portal and when the scammer told him that further profit was almost guaranteed due to the condition of the market, he deposited a further £52,140. He was then assigned another broker who explained that he'd need to pay 80% of his profit to withdraw his funds, in response to which he paid another £40,000 to the scam.

Mr W realised he'd been scammed when the scammer kept telling him to deposit more money and he was unable to make a withdrawal. He complained to Revolut on 21 June 2023 with the assistance of a representative who said Revolut should have intervened because he was sending multiple unusual payments to new cryptocurrency payees in quick succession from a newly opened account which was funded with several high value credits.

They said it should have asked him whether there were any third parties involved, whether he'd been promised a plausible rate of return, and whether he'd checked the FCA website, and as he hadn't been coached to lie, he'd have explained that he was acting under the guidance of a cryptocurrency broker, and the scam would have been detected.

But Revolut refused to refund any of the money Mr W had lost. It said a chargeback claim was raised on 28 November 2023, but it was rejected because the card payments were authenticated via 3DS. And it didn't have enough information to assess the reported transfers.

Mr W wasn't satisfied and so he complained to this service. He explained that he thought the investment was genuine and made the later payments because he didn't think he'd be able to withdraw his funds without doing so.

Responding to the complaint, Revolut said Mr W opened the account on 15 March 2023 and selected 'crypto' as the reason for opening the account. It said Mr W was sent a new payee warning before the first payment to each new beneficiary and it intervened on 16 March 2023, 20 March 2023, 11 April 2023, and 2 May 2023, but he provided inaccurate information during live chat interactions, which prevented it from giving appropriate warnings.

Revolut explained that on 16 March 2023, Mr W selected 'safe account' as the payment purpose and was asked whether he'd been told he'd been a victim of fraud and rushed into making the payment and whether he'd been asked to ignore scam warnings. He was then escalated to a live chat where he said he hadn't been told to download remote access software before being warned: "*please be aware that scammers are using increasingly sophisticated techniques to gather personal information and convince customers to transfer funds in complex scams. They can pretend to be a financial institution, government institutions, trusted online merchants, an exciting investment opportunity or even people you know."* He was then shown a set of dynamic educational story messages warning that there was a high probability that the payment was a scam and offering the opportunity to consult with customer support specialists, which he declined.

Revolut argued that Mr W's decision to select an inaccurate payment purpose hindered its ability to issue suitable and relevant warnings. It also argued that the payments were sent to accounts in his own name, so the fraudulent transactions didn't originate from the Revolut platform. It argued that it would be irrational to hold it liable for losses in circumstances where it is merely an intermediate link, and there were other authorised banks and other financial institutions in the payment chain that have either comparatively greater data on Mr W. It also cited 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. The bank's duty is to execute the instruction and any refusal or failure to do so will prima facie be a breach of duty by the bank."

It also said Mr W failed to do sufficient due diligence despite having had plenty of time to reflect on his actions. It said there was a warning on the FCA register dated 31 January 2023 the first payment and had he done reasonable due diligence he'd have likely seen the warning and decided not to go ahead with the transactions.

Our investigator didn't think the complaint should be upheld. She didn't think Revolut needed to intervene when Mr W made the first payment because it was relatively low value, and she said the second payment wasn't suspicious because Mr W was sending funds to an account in his name with another EMI. But she agreed there should be concerns when Mr W paid £17,600 to C on 16 March 2023 because it was a significant payment from a newly opened account to a cryptocurrency merchant and he said he was paying a safe account.

Our investigator explained that Mr W was engaged in a live chat, and as he'd said he was transferring funds to a safe account, he was warned the payment was a scam and that a bank would never ask him to move his money. He was also asked if he'd downloaded any screen sharing applications, whether he'd received any calls from anyone telling to him to

create a Revolut account, whether he'd been contacted or encouraged to invest by someone he didn't know or had only met online recently, whether he'd been promised returns which seemed too good to be true, whether he'd conducted any research, whether he had access to or owned the cryptocurrency account, and whether anyone was pressuring him to act quickly at risk of missing out on an investment opportunity.

Our investigator was satisfied that then intervention was proportionate to the risk presented by the payment, because he was engaged in a live chat, given an appropriate warning and asked probing questions, but his responses were misleading, and this prevented Revolut from detecting the scam.

She also noted that Bank H spoke to Mr W on 16 March 2023 and asked similar questions in response to which he said no one was coaching him, he wasn't asked to move money, he'd opened the Revolut account the day before and was transferring £17,600 to the new account for online shopping. Bank H asked if anyone had asked him to mislead the bank, if anyone was asking or forcing him to make the payments, if he'd downloaded any screen sharing applications such as AnyDesk, and if anyone had asked him to create the Revolut account.

Mr W said the purpose of the Revolut account was for online shopping and Bank H gave him a safe account warning. He was then required to attend a branch with ID to unlock his internet banking on 18 March 2023, when he said Revolut had a better interest rate. On that occasion he was told to speak to the fraud department and was given another safe account warning and asked more questions.

Our investigator was satisfied that Mr W went ahead with the payments notwithstanding general scam warnings from Revolut and Bank H, and that he'd failed to do any due diligence, which showed he was determined to make the payments, and had complete trust in the scammer. She concluded that Revolut's interventions were proportionate to the risk associated with the payments and there was nothing else it could have done to prevent his loss.

She noted Mr W's representative had argued that Payment 21 should have triggered another intervention, but she didn't agree it was out of character because by that time he'd made other large payments to cryptocurrency exchanges, so the payment wasn't unusual. And she didn't think another intervention would have made a difference because Mr W was clearly determined to make the payments and was misleading his banks about the circumstances of the payments in an effort to do so.

Finally, she was satisfied that Revolut taken steps to recover Mr W's funds as soon as it was aware of the fraud. Mr W paid a legitimate cryptocurrency exchange and would have received a service from the cryptocurrency exchanges. And she didn't think he was entitled to any compensation.

Mr W has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that the main focus of Revolut's questioning was safe account scams. They said the account should have been blocked as soon as Mr W said he was sending funds to a safe account because this option should put the bank on notice that the consumer is at risk of financial harm.

They also said Revolut missed several opportunities to intervene and ask open ended questions arguing that the questions it did ask weren't probing enough, especially as it knew or ought to have known that payments to cryptocurrency providers carried a high risk of being associated with fraud. They also said the warnings provided lacked the necessary impact to deter Mr W from proceeding with the transactions.

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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr W has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr W '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 W is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr W 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 March 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;

• 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. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to genuine merchants. However, 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 did enough to warn Mr W 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 W from financial harm due to fraud.

The first payment wasn't high enough to raise concerns, and the second payment was to another EMI, so Revolut didn't need to intervene. It did intervene on 16 March 2023 when Mr W transferred £17,600 to C and so I've considered whether it did enough on that occasion. As described above, Revolut contacted Mr W via its live chat facility, and I'm satisfied this was appropriate because he was sending a large amount to a cryptocurrency exchange from a newly opened account, and he'd said he was sending the funds to a safe account.

Mr W's representative has argued that Revolut should have blocked the account when Mr W said he was sending funds to a safe account, but I'm satisfied he was taken to a live chat and asked questions which were relevant to cryptocurrency investment scams and presented with a warning about safe account scams, which I'm satisfied was proportionate. Unfortunately, Mr W's responses prevented Revolut from detecting the scam and as he had been coached to lie, I don't think there was anything else it could reasonably have done to detect the scam.

Further, based on the fact Mr W selected safe account when he was asked to give a payment purpose, I'm satisfied a warning about safe account scams was appropriate. But as he was paying a cryptocurrency merchant, I think Revolut could also have shown him a warning which was tailored to cryptocurrency scams, but I don't think this would have made any difference. As our investigator has explained, Mr W's behaviour around this time show that he was being coached by the scammer and that he trusted the scammer to the extent that he misled both Revolut and Bank B during the interactions he had with them. So, if Revolut had shown him a written warning covering off the key features of cryptocurrency investment scams, even though there were red flags present, I don't think it would have prevented his loss.

Mr W's willingness to lie to his banks, including in person in one of Bank H's branches, demonstrates that the trusted the scammer to an extent that I think Revolut would have found difficult to counter through written a warning. Mr W has said the scammer seemed professional and knowledgeable and that he hadn't seen any negative reviews about O. I understand it was his difficulty in withdrawing money that led him to the realisation that he was being scammed, and I don't think a written warning at the beginning of the scam period would have been impactful enough to have made him pause and look more closely into the scammer before proceeding. So, while I think Revolut could have given Mr W a better warning, I don't think it would have made any difference.

Revolut intervened several more times, engaging Mr W in a live chat and giving warnings relevant to safe account scams. Each time, he was asked whether he'd been contacted by anyone asking to move his money to another account and, also, whether he'd been asked to install AnyDesk. He was also given a warning about safe account scams.

I've considered whether these interventions were proportionate to the risk presented by the payments, and I remain satisfied that Mr W misled Revolut and that this prevented it from detecting the scam or providing relevant warnings. I accept the fact he was sending funds to cryptocurrency merchants means Revolut could have provided more tailored warnings, but for the reasons I've explained above I don't think this would have made any difference to the outcome.
So, while I accept Revolut could have done more, I don't think it missed opportunities to have prevented the scam.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr W paid an account in his own name and moved the funds onwards from there.

I've thought about whether Revolut could have done more to recover the card payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme - so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr W).

Mr W's own testimony supports that he used cryptocurrency exchanges to facilitate the payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr W's payments, 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 a chargeback request against either of the cryptocurrency exchange companies was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr W 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.

I'm sorry to hear Mr W 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

For the reasons I've outlined above, 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 W to accept or reject my decision before 18 June 2025.

Carolyn Bonnell
Ombudsman