

The complaint

Mr B 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.

Mr B received a pop-up advert about an opportunity to invest with a company I'll refer to as "X". He expressed an interest and was contacted by someone I'll refer to as "the scammer" who said he'd guide him on how to invest in foreign currency.

He checked X on Trust Pilot, but he didn't check the Financial Services Authority ("FCA") website. He engaged in regular contact with the scammer, who he grew to think of as a friend. The scammer told Mr B to use AnyDesk remote access software which he already had downloaded. He made an initial payment of £250 to open an account with X and the scammer showed him how to deposit funds and make withdrawals.

The scammer opened a Revolut account in Mr B's name and an account with a cryptocurrency exchange company which I'll refer to as "C". He told Mr B to first purchase cryptocurrency and load it onto an online wallet, and between 7 June 2023 and 16 October 2023, he made thirteen debit card payments and three transfers to three different cryptocurrency merchants.

In early October, the scammer said that if he could increase the value of the account, X would match it, and he would move to more profitable trades. When Mr B said he didn't have sufficient funds, the scammer used AnyDesk to apply for three loans totalling £39,500, which he transferred to Mr B's Revolut account via Bank B.

On 11 October 2023, Revolut restricted the account and engaged Mr B in a live chat to confirm the source of the funds. Mr B told Revolut about the loans and that he was paying a legitimate cryptocurrency exchange, and the restriction was eventually lifted on 15 October 2023. On 17 October, the account was restricted again. And on 8 November 2023, Revolut told Mr B the account would be closed, at which point, the scammer became unfriendly, and he realised he was being scammed.

Mr B complained to Revolut, arguing that it should have realised he was being scammed when he was asked to verify the origin of the loan funds because he was making large transfers to cryptocurrency merchants. Instead, it focussed on the origin of the funds and whether the cryptocurrency exchange was legitimate.

He said Revolut must have had evidence of a scam otherwise it wouldn't have placed the restrictions on the account. It didn't provide any evidence to support its suspicions and had it done so, he would have cancelled the transactions. He said it only gave generic warnings

and made no effort to ask questions about the investment, and had it done so, he'd have explained that he'd learned about the opportunity from a pop-up advert and was being assisted by a broker who told him to apply for the loans.

He explained that Revolut asked him if he'd been told to download AnyDesk and he said it was already on his laptop, but it didn't ask if it had been used to facilitate the transactions. He argued that Revolut missed an opportunity to stop the scam and that he was being heavily manipulated and groomed, so if Revolut had provided evidence he was being scammed, his loss could have been prevented. Finally, he said he had trusted the scammer, having found positive reviews on Trust Pilot.

But Revolut refused to refund any of the money. It said the payments were authorised and it wasn't liable for the payments. It said chargeback claims were raised on 22 March 2024, but Mr B had paid genuine merchants who offered specific services, so the claims weren't valid. It said its interventions were appropriate and proportionate and Mr B didn't do proper research and was warned several times via the app about potential scams and told it might not be able to recover his funds. It also explained the decision to terminate the account was reviewed and found to be incorrect, so the restrictions were lifted.

Mr B wasn't satisfied and so he complained to this service. He said Revolut blocked the first payment and told him he might be dealing with a scam company. It questioned why he opened the account, the source of funds and whether the cryptocurrency exchange was legitimate, but it didn't provide any evidence of why it thought it was a scam, and so he proceeded with the payment because he'd researched the cryptocurrency exchange and was satisfied it was legitimate. He said he assumed Revolut was unhappy that he was using a different cryptocurrency platform and ignored the warnings because it didn't provide evidence that he was being scammed. And the scammer had told him not to mention X as Revolut saw them as competition, and he trusted what he said because they'd become friends.

Our investigator didn't think the complaint should be upheld. She was satisfied Revolut ought to have known Mr B was sending the funds to cryptocurrency merchants and she didn't think it needed to intervene any sooner than it did because the payments weren't high enough to raise concerns or made in quick succession.

She noted the first intervention was on 11 October 2023 when Mr B paid £3,914 to a cryptocurrency exchange (R). Mr B selected 'as part of an investment' as the payment purpose and was shown in-app warnings tailored to investment scams. He acknowledged the risks and proceeded with the payment. Our investigator was satisfied the intervention was proportionate to the risk presented by the payment.

She noted Mr B then successfully made further card payments to R, before two card payments were declined, along with an attempt to transfer £19,663.30 to his own account with Bank C on 11 October 2023, when Revolut placed restrictions on the account. During the live chat conversation that followed, Mr B provided proof of his identity and proof of the source of funds paid into his Revolut account (the loans). Our investigator noted that Revolut asked probing questions to identify if he could be falling victim to an investment scam in response to which he said he'd seen an advert on television, he'd researched the cryptocurrency merchants, and he hadn't downloaded any screen-sharing software. Revolut provided relevant cryptocurrency investment scam warnings including: *'scammers often use tactics to trick you into buying cryptocurrencies from fake websites and investment platforms'*, *'Scammers will try to convince you that you will miss out on an opportunity if you do not send money quickly'*, and *'you're asked to install screen sharing applications to "help" you with the movements'*. It also provided instructions to check the investment company was authorised by the FCA, and the restrictions were eventually removed on 15 October 2023.

Our investigator didn't think Revolut should have listed the restrictions until Mr B had produced the cryptocurrency account statements, but even if it had done more, she didn't think it would have prevented Mr B's loss.

She explained further interventions occurred on 16 October 2023 when Mr B attempted to transfer £500 and £19,000 to a cryptocurrency exchange (P). For the £500 payment, Mr B went through the automated in-app warning flow and acknowledged the risks before making the payment. For the £19,000 transfer, he was engaged in an in-app chat which our investigator was satisfied this was reasonable and proportionate, considering the increased, and unusually high value of the payment. During the live chat Mr B was shown warnings tailored to cryptocurrency investment scams, including *'if you make this transfer, the most likely outcome is that you'll lose your money permanently'*.

The payment was eventually processed followed by another payment for £9,000, but on 17 October 2023, Revolut placed restrictions on the account for a second time due to 'strong scam indicators on the account'. Mr B said in the live chat that he was buying cryptocurrency, and no one had advised him to do it. He sent screenshots showing the payments he made to P had successfully deposited in the cryptocurrency account, and that the cryptocurrency was subsequently withdrawn from the wallet. Revolut identified that the cryptocurrency was sent out to and asked him where he was sending the cryptocurrency and Mr B provided evasive responses, so the restrictions remained in place, despite Mr B's objections.

Our investigator noted that Revolut ought reasonably to have insisted that Mr B provide the cryptocurrency account statements before it lifted the restrictions, which would have stopped him from making the final three payments. However, she didn't think this would have prevented his loss because when the account was restricted on 11 October 2023, he created an account with Bank C. And when Revolut restricted the account on 17 October 2023, he refused to tell it where he was sending the cryptocurrency. He said, 'if it is a scam, and I'm unaware of it and I lose my money, then Revolut can't be held responsible' and withheld information about X. He had also lied about the purpose of the loan applications and went ahead despite having been warned by one of the loan providers that there was an increasing trend in loans being applied for as a result of cryptocurrency investment scams.

Commenting on Mr B's complaint that Revolut didn't provide evidence to prove he was the victim of a scam, our investigator said Mr B had been coached not to mention X, which meant it didn't have the evidence it needed to expose the scam. She explained that Mr B had believed the scammer was genuine and had followed the advice to lie to the loan providers and to Revolut, despite having been presented with relevant warnings. And he only accepted he'd been scammed when he was unable to withdraw funds to repay the loans. So, if Revolut had prevented Mr B from paying P on 16 October 2023, he'd have used another account.

Mr B has asked for his complaint to be reviewed by an Ombudsman. He doesn't accept he'd have found another way to send the funds if Revolut hadn't lifted the restrictions on 15 October 2023. He accepts he opened an account with Bank C so he could make withdrawals from the investment and service the loans. But if Revolut had refused the final three transactions, he'd have had time to reflect and question the scammer.

He maintains he believed Revolut's warnings related to the cryptocurrency merchants, so he was happy for the payments to proceed. And he doesn't understand why Revolut applied restrictions after allowing the transactions to proceed.

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 B 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 B '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 B is presumed liable for the loss in the first instance.

There's no dispute that Mr B was scammed, but although he 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 October 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 Mr B's loss. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to genuine cryptocurrency exchanges.

Revolut intervened on several occasions and so I've considered whether it did so at the right time and whether the interventions were proportionate to the risk presented by the payments. Revolut first intervened on 11 October 2023 when Mr B made a payment for £3,914. I've considered whether it should have intervened any sooner and even though the earlier payments were identifiably for cryptocurrency, they were relatively low value and so I don't think Revolut needed to intervene.

I've considered what happened during the first intervention and I agree with our investigator that Mr B was shown relevant warnings, and that the intervention was proportionate, so I've gone on to consider what happened during the next intervention.

As described above, Revolut restricted the account on 11 October 2023, and the restrictions were lifted on 15 October 2023. Our investigator explained that Mr B sent a screen shot showing the source of funds on 12 October 2023 and that Revolut asked for the cryptocurrency account statements on 14 October 2023, but he didn't send them until 16 October 2023. She felt it shouldn't have lifted the restrictions until Mr B produced his cryptocurrency account statement, and had it done so – based on what happened on 17 October 2023 - it wouldn't have lifted the restrictions.

I've considered whether Revolut should have lifted the restrictions before Mr B produced the cryptocurrency account statements and, having requested them, I think it should have waited before lifting the restrictions. Had it done so, it would have discovered sooner that Mr B was sending cryptocurrency to another wallet.

However, if Mr B had been prevented from making any further payments from his Revolut account after 11 October 2023, I think it's likely that he'd have tried to make the payments from another account. He's explained that Bank C didn't allow payments to cryptocurrency, but as he continued to make payments to the scam after the restrictions were lifted on 15 October 2023, I think it's likely that he'd have transferred funds from his Revolut to another account and continued to make payments to the scam.

Mr B has said his loss would have been prevented if the restrictions had stayed in place and I accept there were no further payments after the account was finally restricted on 17 October 2023. But I think that was because he'd run out of funds and not because he believed he'd been scammed because he continued to believe the investment was genuine after 17 October 2023, despite Revolut's concerns and repeated warnings. He'd fully trusted the scammer to the extent that he lied to Revolut and the loan providers and didn't mention X, and he ignored the warnings he was given. And even though I haven't seen evidence of coaching, it's clear he was prepared to mislead the banks, and ignore the relevant scam warnings he was given.

So, while I agree with our investigator that Revolut missed an opportunity to detect the scam sooner than it did, I don't think this represented a missed opportunity to have prevented his loss.

There were two further interventions on 16 October 2023, and I agree with our investigator that because Mr B was sending £19,000 to a cryptocurrency merchant having received loan funds into the account, Revolut should have asked more probing questions and provided more robust warnings. But for the reasons I've outlined above, I don't think he'd have paid attention to more robust warnings, and I don't think he'd have been honest about the circumstances of the payment, so a better intervention wouldn't have detected the scam.

Mr B has questioned why Revolut placed restrictions on the account having processed transactions shortly before, but I note the first restrictions were placed after a series of declined payments including an attempt to transfer £19,663.30 to Bank C from where he

presumably would have tried to send the funds to his cryptocurrency account, which isn't unreasonable.

I'm sorry to hear Mr B 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.

Recovery

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

I've thought about whether Revolut could have done more to recover the debit 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 B).

Mr B's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. It's 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 B'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 the cryptocurrency exchanges was fair.

Compensation

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

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 B to accept or reject my decision before 28 July 2025.

Carolyn Bonnell
Ombudsman