DRN-4529020

The complaint

Mr S complains that Revolut Ltd ("Revolut") won't refund the money he lost as a result of an investment scam.

He's being supported by a representative (Mrs S). To keep things simple, I'll refer to Mr S throughout this decision.

What happened

The background to this complaint is known to both parties, so I won't repeat all the details here. In summary, Mr S says:

- He came across a post on social media, seemingly involving well-known celebrities and clicked on a link that took him to an advert offering advice on earning money. He added his number and received a call from someone claiming to be an investor, going by the name of Eric Bartos (the scammer), who would be acting as his financial adviser.
- An initial start-up fee of £250 was paid from an account he held with another bank and he downloaded remote access software to his laptop on the scammer's instructions. He was also guided by the scammer on what he needed to do to start investing and opened a new account with Revolut and a crypto wallet as part of that process.
- A series of larger payments were made from the Revolut account between March and April 2023. The first £20,000 was intended as a further investment but the subsequent transfers were for fees which he was led to believe were needed to withdraw his money.
- He realised he'd been scammed when the scammer became unresponsive and he noticed that the transfers were sent to payees he didn't recognise.

I've listed below the transactions (as they appear on the statements) I've considered as part of this complaint. To note, I understand the Revolut account was opened in March 2023 and a payment of £500, on 27 March 2023, is not being disputed here as it was returned to Mr S's account with the originating bank.

	Date	Time	Type	Amount	Payee
1	27-Mar-23	15:05:40	Transfer	£20,000	LHV Bank
2	*30-Mar-23*	*07:38:58*	*Declined - Transfer*	*£25,000*	*LHV Bank*
3	30-Mar-23	09:13:28	Transfer	25,000	LHV Bank
4	03-Apr-23	09:15:35	Transfer	£1,000	LHV Bank
5	11-Apr-23	08:55:30	Transfer	£100	Clear Junction
6	11-Apr-23	09:10:47	Transfer	£19,900	Clear Junction

A fraud claim was submitted in April 2023 and declined by Revolut in May 2023. A complaint was also raised and declined by Revolut on 22 June 2023. The matter was then referred to the Financial Ombudsman. Our Investigator considered the complaint but didn't uphold it.

In summary, he was satisfied the payments from the Revolut account were likely authorised by Mr S. He also thought it was unlikely Revolut could have prevented the scam as when it

did intervene to ask questions about the nature of the payments it received responses that wouldn't have indicated Mr S was at risk of being scammed. And while the scammers may have provided those responses (using remote access downloaded to Mr S's laptop) Revolut wouldn't have known it wasn't communicating with anyone other than Mr S at the time.

As the matter couldn't be resolved informally, it's been passed to me to decide.

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 conclusions as the Investigator and for broadly the same reasons.

Authorisation

It's not in dispute Mr S was scammed and I'm sorry about the impact the whole experience has had on him. It also seems it's no longer in dispute he authorised the payments from his account. This is important as Mr S would generally be liable for authorised payments and Revolut would generally be liable for unauthorised payments. But, for completeness, I've set out below the key points as to why I agree the payments should be treated as authorised, in line with the relevant regulations – the Payment Services Regulations 2017 (PSRs).

In broad terms, as set out in the PSRs, a payment would be deemed as authorised if the account holder completes the agreed steps to make a payment or gives someone access to complete those steps on their behalf. In this case, Revolut has provided evidence to show the first payment (1 above) and the last two payments (5 and 6) were made in-app using the registered mobile device. This means those payments must have been made by someone with physical access to that device and there's nothing to suggest an un-authorised third-party was in possession or in control of Mr S's device at the time.

The middle two payments (3 and 4) were made on the web browser on Mr S's laptop – and I'm aware some limited activities can be performed on the web browser remotely. But given that payments would still have needed to be authenticated on the mobile device. And given Mr S's testimony that the payments were intended for investment (or to pay fees) and there's evidence to show he was aware the money was to go to an external wallet (before it was sent to the scammer) I'm satisfied he was aware the payments would be leaving his Revolut account such that they should be deemed as authorised for the purposes of the PSRs.

Prevention

The starting point, as noted above, under the PSRs is that a customer is liable for payments they've authorised. But there are some situations where I consider that a business, taking into account relevant rules, codes and best practice, should reasonably have taken a closer look at the circumstances of a payment – if, for example, it's particularly out of character.

In this case, it's arguable the first payment of £20,000 should have triggered an intervention given its value and the activity on a newly opened account. I'm not convinced the written warnings Revolut says were provided for that payment were sufficient at the time. That said, I also need consider whether any timely and proportionate interventions would have likely prevented Mr S's losses – and, on balance, I'm not persuaded they would have.

This because, as the evidence shows, when Revolut did intervene on an attempted payment (£25,000) on 30 March 2023 and again on the payment (£19,900) on 11 April 2023, it asked

a series of proportionate questions designed to unravel a potential scam – including whether Mr S had installed remote access software; if he'd received calls from anyone telling him to create a Revolut account; and if he'd been contacted or encouraged to invest by someone he didn't know or had only recently met online. There was nothing in the replies it received that should, from Revolut's perspective, have alerted it to a heightened risk that Mr S was being scammed. And although I appreciate Mr S says that the responses were typed by the scammer (using remote access he'd downloaded to his laptop), that's not something Revolut would have known or had the ability to detect. I'm not therefore persuaded it'd be reasonable to hold Revolut liable for Mr S's losses on the basis that it didn't do enough to protect him and failed to take additional steps to find out more about the nature of his payments.

In reaching this view, I've considered Mr S's comments that Revolut shouldn't have allowed the payments given its concerns about some of the spending and I agree Revolut was better placed to recognise how scammers work. But it's important to note that a business' primary duty is to execute payments in compliance with its customer's instructions. It's also important to note that Revolut wouldn't have known for certain that Mr S was falling victim to a scam either. As above, it's expected to take additional steps where an identifiable scam risk is present – and it did so here. But if those responses were from a fraudster who'd been given remote access, it's difficult to see how Revolut could have reasonably unravelled the scam.

I've thought carefully about Mr S's statements that Revolut's systems were inadequate as they allowed the scammer to interact on its 'scam chat'. I understand he feels if Revolut had asked security questions or limited its 'scam chat' to the mobile device, then the scammer wouldn't have been able to impersonate him. And I've taken account of his evidence relating to the cards linked to the account (and not applied for by him) in support of his case that the scammer was able to undertake financial operations without his knowledge.

But I think it's again necessary to keep in mind that Revolut wasn't able to detect where a customer had given someone else access (via AnyDesk) when using a web browser. And that, for web browser access, authentication was in any event first required on the mobile device. The activities that could be performed on the web browser were also limited. For example, transfers or new payees still needed to be authenticated on the mobile device. I can understand why these measures would have given Revolut reassurance that Mr S was aware of activity taking place on his account when the payments were made.

In addition, I can't overlook that the transfers were spread out over days. The logs show the account was accessed, on the mobile device, in between payments and at the time the payments were made. I see no reason why the chat itself wouldn't have been accessible to Mr S during the interventions (or at any other time), given also he was able to use it when reporting the scam. And I can't overlook that in the first intervention, as a further check, he was asked to upload a 'selfie' to the chat (with a handwritten note showing date and time). This too would have given Revolut reassurance that Mr S had accessed the chat and was engaging in the conversation. I'd also add here that Mr S acknowledges he'd seen part of the chat and that the scammer had typed responses at the time.

I recognise Mr S may not have appreciated the significance of what was being said. I also appreciate what he's said about not understanding the implications of online banking or crypto-currency and that, as is common with this type of scam, he placed his trust with someone he genuinely believed was a legitimate 'adviser'. At the same time, however, for the reasons above, I can't fairly say that Revolut failed to step in to check if a scam was likely taking place or that it was a lack of security measures on its part that allowed the scam to happen without Mr S's knowledge, such that it should be held responsible for his losses.

Recovery

In general, a business should attempt to recover lost funds once a scam has been reported. In this case, given the transfers were made from the Revolut account, via legitimate payees likely acting as payment processors, for the purchase of crypto-currency before it was lost to the scammer, there would have been no prospect for Revolut to facilitate a recovery of that money by the time that the scam was reported.

Other matters

Mr S is also concerned about the service he received from Revolut and that his requests for a transcript of the chats were apparently not actioned. I can see that the scam was reported to Revolut on 14 April 2023 and it took until 23 May 2023 before Mr S received a response to his claim. It was then another month before a response to the complaint was issued.

I don't think the way the claim was handled was unreasonable overall. The matter wasn't straight-forward, even though I can see that more timely updates could have been provided at times while the investigation was ongoing. The request for a transcript was twice made on 8 June 2023 after the complaint had been submitted on 23 May 2023. Although 'complaint handling' itself isn't a regulated activity – and this means I don't have the power to comment on it here – I can assure Mr S that the chat transcript was considered in this investigation.

I realise Mr S has fallen victim to a cruel and elaborate scam. I understand why he wants to do all he can to recover his money. But, for the reasons I've explained, I'm not persuaded that Revolut can fairly and reasonably be held liable for his losses in these circumstances.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 12 June 2024.

Thomas Cardia
Ombudsman