DRN-4702452

The complaint

Mr E 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 2008, Mr E invested around £15,000 to £20,000 with a company which I'll refer to as "I". But when he wanted to withdraw his investment he received an emailing claiming to be from HMRC stating the company was being shut down due to fraud and that his funds were being sent to Cypriot government.

In 2022, Mr E was contacted by someone who I'll refer to as "the scammer" who claimed to work for a company which I'll refer to as "A" and that he could recover his lost funds. Mr E checked the Financial Conduct Authority ("FCA") website and while there was nothing to verify the scammer's identity, he was reassured because the scammer said he was moving to a well-known company in February 2023.

A Revolut account was opened in Mr E's name on 19 December 2022, which required his name, surname, date of birth, email address, phone number, address, and a selfie. And between 16 January 2023 and 24 January 2023, ten payments totalling £45,013.06 were made to six different beneficiaries from the Revolut account. Five of the payments were made to cryptocurrency exchange companies using a debit card. And there were six faster payments to two individuals, one of which was refunded the following day. Before the first faster payment to each new payee, Revolut presented a scam warning which said the payment was suspicious. It also asked whether the payment could be a scam before the payments were processed.

Mr E contacted Revolut when he realised he'd been scammed but it refused to refund any of the money he'd lost and so he complained to this service stating he didn't make any of the payments and he didn't see any of the warnings.

Responding to the complaint, Revolut questioned how the scammer could have opened the Revolut account without the use of a screensharing application. It said the five debit card payments were authenticated by 3DS which would have required Mr E to enter a passcode or use biometric authentication. It also said the payments were made to genuine cryptocurrency merchants that had provided a service, so it couldn't raise a chargeback request. And the funds were transferred to accounts in Mr E's control, so the fraudulent activity didn't occur via Revolut.

Revolut said the account was newly created so there were no historical transactions to compare the payments with, and when the account was opened, the purpose of the account was to "make transfers". It said Mr E was shown a proportionate and appropriate warning

before the faster payments on 18 January 2023 and 20 January 2023, but he chose to clear the message and send the payments.

It explained its terms and conditions state it won't refund any money if the customer has acted fraudulently, or intentionally or carelessly failed to keep their security details or Revolut Card safe and it said that Mr E had failed to explain why he sent funds to the scammer when he was expecting to receive funds.

Our investigator didn't think the complaint should be upheld. He was satisfied Revolut had produced evidence that the card payments were made using the same mobile device as the one used to make the faster payments, and that they were authenticated by 3DS. He was also satisfied Mr E had allowed the scammer to open the Revolut account and set up the cryptocurrency wallets on his behalf and that this probably included giving him his personal and security details. And he explained that whether Mr E made the payments himself, or allowed the scammer to make them for him, all the payments should be treated as authorised – either through apparent authority or otherwise. So, he was satisfied the disputed payments were authorised and therefore Mr E was liable for them.

Our investigator explained there would have been no prospect of a successful chargeback claim against the cryptocurrency exchange companies because Mr E had received the service he'd paid for.

He noted the first faster payment to each new beneficiary had triggered a written warning, but he thought Revolut should have intervened when the first card payment was processed. However, based on what happened when it did intervene, he didn't think an earlier intervention would have made any difference.

He explained Mr E had said he didn't recall seeing any warnings from Revolut and so he thought it was likely the scammer had gained remote access to his device using a screen sharing app. So as the scammer was in control of his device, they could've clicked though the warning and answered any questions in the same way the must have done later in the scam period. Because of this he didn't think Revolut's failure to intervene sooner represented a missed opportunity to prevent the scam.

Our investigator also noted Revolut contacted the receiving bank when it became aware of the fraud, by which time there would have been no chance of a successful recovery because the funds had already been removed from the receiving account.

Mr E has asked for the complaint to be reviewed by an Ombudsman arguing that Revolut didn't send him a text message and the payments weren't authenticated by 3DS verification. He says he didn't have the Revolut app on his phone and has no idea how the scammer could have set that up.

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 E 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.

Were the payments authorised?

Authorisation has two limbs – authentication and consent. So, Revolut needs to show the transaction was authenticated as well as showing Mr E consented to it.

I'm satisfied that whoever made the faster payments would have had access to the Revolut app via Mr E's phone. And Revolut has explained the debit card payments were 3DS authenticated, meaning Mr E would have received a push notification to the Revolut app and been prompted to confirm the transaction in the app to complete the payment. For the 3DS to be approved, he would have had to enter his passcode or use a biometric authentication, and it is not enough to just press "allow". So, I'm satisfied the payments were authenticated either by Mr E or someone to whom he gave the passcode.

Turning to the issue of consent, Mr E has said he didn't make any of the payments himself. But the consumer can be bound by the acts of a third party which appear to have been made with the consumer's authority – this is called apparent authority. Our investigator concluded that Mr E provided apparent authority to the scammer by granting him access to his computer using remote access software.

Mr E accepts he previously allowed someone from a computer company to access his computer using remote access software, but he doesn't recall the scammer using remote access. He told our investigator that the scammer sent £50,000 from his Revolut account. He also said he saw some information about the beneficiaries in an email on his Revolut account, and that the scammer set up the Revolut and cryptocurrency accounts using information that was stored on his computer. This is all consistent with the use of remote access software.

Considering this evidence, which supports that the scammer had access to Mr E's device, I think this explains how the scammer could have clicked through the warnings without Mr E's knowledge before proceeding with the payments. So, if Mr E didn't set up the accounts, make the payments or see the warnings, the most likely alternative is that the scammer had access to his device via remote access software, meaning he permitted him to appear as if he had his authority to make transactions on his behalf. So, the payment transactions can be considered 'authorised' even where Mr E didn't ask the third party make any payments or know about them.

Consequently, I'm satisfied Mr E '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 E is presumed liable for the loss in the first instance.

Chargeback

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 E).

Ms E's own testimony supports that he used cryptocurrency exchanges to facilitate the transfers. 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 E'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.

Prevention

There's no dispute that Mr E was the victim of a scam, 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.

Revolut was an emoney/money remittance provider and at the time these events took place it wasn't subject to all the same rules, regulations and best practice that applied to banks and building societies. But it was subject to the FCA's Principles for Businesses and BCOBS 2 and owed a duty of care to protect its customers against the risk of fraud and scams so far as reasonably possible.

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 did enough to warn Mr E when the payments were made.

Two of the payments flagged as suspicious on Revolut's systems and it presented a scam warning which had to be clicked through before the payments were processed. Unfortunately, as Mr E says he didn't make the payments or see the warnings and I'm satisfied the scammer most likely had control of Mr E's device having been granted access by him using remote access software, it seems the scammer disregarded those warnings and went ahead with the payments. In those circumstances it wouldn't have made any difference if Revolut had intervened when Mr E made the first debit card payment.

I've also considered whether there was anything else Revolut could have done to prevent the scam and in the circumstances I don't think there was. Considering the value of the debit card payments and the fact they were to accounts in Mr E's own name from a newly opened account, I'm satisfied a written warning would have been proportionate to the risk. And even if I concluded that Revolut should have given warning tailored to cryptocurrency scams, Mr E wouldn't have seen it so it wouldn't have made any difference. So, I don't think there was anything else Revolut could reasonably have done to stop the scam.

Compensation

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

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr E paid accounts in his own name and moved the funds onwards from there. Revolut has explained it didn't attempt to recover the faster payments as soon as Mr E reported the scam to it because he did provide enough information and by the time the request was made, no funds remained. I'm satisfied this explanation is reasonable.

Overall, I'm satisfied Revolut took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Mr E 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 E to accept or reject my decision before 15 July 2024.

Carolyn Bonnell
Ombudsman