DRN-6066578

The complaint

A company, which I'll refer to as E complains that Revolut Ltd has declined to reimburse payments made as part of a scam.

Mr P, who is a director of E, brings the complaint on E's behalf.

What happened

Mr P received a call in February 2024 from a scammer impersonating Revolut. After he passed "security", Mr P was told that there had been several attempts to use E's account and that he needed to log in and decline them.

Mr P was then persuaded by the scammer to sign in to a "secure link" on his laptop believing he was helping with the fraud investigation. We now know that this was a remote access browser designed to look like Mr P was dealing with "Revolut Business". As part of this Mr P logged into different banking accounts and unfroze his Revolut card on the belief that Revolut was closely monitoring his account.

Mr P's card details were added to the scammer's Apple Pay and E's disputing four payments totalling around £34,000.

Revolut declined E's claim and said that multiple authentication checks had taken place before the disputed payments. Including the use of an email, QR code, and OTP codes sent to Mr P which were all clear as to their purpose to set up Apple Pay and change Mr P's passcode. Revolut didn't think it was responsible for E's loss, but it said it had attempted to recover the funds via the chargeback process.

When Mr P referred the complaint to our service, Mr P told us that he doesn't know how Apple Pay was added. He did receive the email and SMS messages with one-time passcodes (OTPs), but says he didn't share these with the scammer. Mr P said that he may have had his email open on his laptop and his WhatsApp message are also accessible from his laptop, so it's possible these were compromised using the remote access the scammer had in place.

The investigator upheld the complaint. In summary they concluded that the disputed payments were likely unauthorised, and they didn't think Mr P had been grossly negligent in failing to keep the secure information safe. So, they didn't think Revolut had acted fairly in declining the claim. They recommended Revolut reimburse the disputed payments and pay interest to reflect the time E had been without the funds.

Revolut didn't agree, it said it thought the steps Mr P had taken did amount to gross negligence.

The matter was passed to me for consideration by an ombudsman. I let both parties know that I thought a fair outcome would be for Revolut to reimburse 50% of E's loss plus interest.

Revolut accepted this outcome, but Mr P disagreed on behalf of E. In summary Mr P said:

- He disagreed with my findings about what likely happened:
    - He didn't receive or share a QR code.
    - He doesn't recall unblocking his card more than once.
    - He doesn't know how the OTPs were shared; he might have shared one but not three.
    - The remote access timing might not be accurate.
    - The payment to a jewelry store at 16:52 was before the call with the scammer.
    - There was also fraudulent activity on his account with another provider.
    - The scammer could have changed the passcode without the OTP using remote access to his laptop when he was signed in.
    - He didn't authorise any payments and only wanted to protect E's funds.
- Revolut's fraud issues have been broadcast on well-known television programmes.
- He thought Revolut should be responsible for E's consequential losses:
    - E is in financial difficulty – Mr P provided evidence of some of its debts.
    - He provided evidence that he had personally lent E almost £18,000 to mitigate the impact of the fraud on E.

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'm upholding this complaint – I have carefully considered Mr P's comments, but I still think a fair resolution is for Revolut to reimburse E 50% of the loss plus interest. I'll explain why.

Has Revolut acted fairly in holding E liable for the payments?

Under the relevant law - the Payment Services Regulations 2017 (PSRs) – the starting point is that E is liable for payments Mr P authorised. Revolut is generally expected to reimburse unauthorised payments.

Where a payment is authorised, that will often be because the customer has made the payment themselves. But there are other circumstances where a payment should fairly be considered authorised, such as where the customer has given permission for someone else to make a payment on their behalf or they've told their payment service provider they want a payment to go ahead.

It's common ground that Mr P fell victim to a scam in which he thought he was speaking to Revolut. But there are discrepancies between what Mr P recalls doing and the evidence Revolut has provided.

Where evidence is incomplete, missing or contradictory, I need to determine what I think is more likely than not to have happened. I do this by weighing up what I do have and making a finding on the balance of probabilities.

Mr P says he doesn't recall sharing any OTPs or a QR code, accessing his email or unblocking his card more than once. So, he hasn't provided us with an explanation of why he would have done so. He does remember giving remote access to his laptop, logging into his online Revolut account and seeing a purchase. Mr P says he declined the purchase and froze his account and card but *that "The Caller didn't like the fact I froze the card and they*

asked if I would unfreeze. I wasn't happy doing this because I wanted to protect my money. They understood and told me to hold for a senior colleague. The senior colleague asked me to verify security. They convinced me that they were closely monitoring fraudsters and scammers and asked me to help them. They asked me to go to Anydesk as my money was still under threat despite freezing the account."

Revolut has shown that the following took place:

- It sent an SMS to Mr P's phone number containing a code to set up Apple Pay.
- The Revolut banking app was set up to access E's account on a new device.
- An email was sent to Mr P to confirm log-in from a new device.
- Mr P's card was blocked and unblocked three times – it was unblocked twice from Mr P's genuine device and once from a new device.
- It sent an SMS to Mr P's phone number containing a code to reset the password in the Revolut banking app on the aforementioned new device.
- It sent an SMS to Mr P's phone number containing a code to confirm the change to the aforementioned new device.
- E's account was accessed using a browser on the aforementioned new device.

Who unblocked the card?

- Mr P appears to be saying he initially blocked and unblocked the card before the disputed payments took place, in an attempt to protect the account before being persuaded to unblock it. I accept this as it was completed on his device. As this was completed around 16:30 it follows that Mr P was already on the phone to the scammer at this time.
- I also think it was likely to have been Mr P who unblocked the card at 16:44, after the first occasion Revolut blocked it, as it is also done on Mr P's device. Mr P says the scammer had remote access to his laptop when he signed into his Revolut account, but the evidence I have from Mr P of the AnyDesk session shows the start time as 17:17 (after this event). Even if this timing is inaccurate, Revolut has also told our service that if it detects remote access to the device being used to log in using a web browser then it limits the activity that can be carried out, including that cards cannot be tokenised (including the set-up of Apple Pay) and customers are unable to unfreeze their card. So, I think it's more likely than not that it was Mr P who unblocked the card on this occasion.
- However, I think it's likely that scammer unblocked Mr P's card at 17:08 as this took place on a new device that appears to belong to the scammer.

How were the payments made?

- It isn't in dispute that the scammer made the disputed payments. The evidence we have supports the payments being made with a newly set up Apple Pay token.
- Secure codes were needed by the scammer for them to set up the Apple Pay token and to be able to log-in and unblock the card and before any successful disputed payments were made i.e. before any loss occurred.

- This was only possible following the use of secure codes, including:
    - An OTP sent to Mr P via SMS to set up the Apple Pay token.
    - An OTP sent to Mr P via SMS to change the password on the account.
    - An OTP sent to Mr P via SMS to confirm the change in phone accessing the Revolut Banking app.

- I think it's more likely than not that Mr P shared these codes with the scammer – this is because he's told us he never gave remote access to his phone and there's no other explanation for how the scammer could have obtained this information. As Mr P has not recalled doing this, he hasn't been able to share why he did so. I'm not persuaded it's likely the password was changed using the remote access to Mr P's laptop as the SMS message specifically refers to the new device that was being used to change the password.

- In terms of other security measures in place, Revolut sent Mr P an email to enable a new login. It's been suggested that the scammer could possibly have accessed Mr P's email from Revolut, as he's told us his email account might have been logged in on the device they had remote access to. But this was before the AnyDesk session Mr P provided us with evidence of began. Revolut has told us that a QR code is needed if the Confirm button is clicked on a different web browser device to the device requesting access. The screenshot Mr P provided of his WhatsApp appears to show him sending the scammer a QR code after a request at 17:06 saying "verification needed" – this was just before the OTP to change the passcode was sent. Mr P says his WhatsApp might have been linked to his laptop that they had remote access to, but again this was sent before the AnyDesk session appears to have begun. And if the scammer had remote access, it's not clear why they would have needed to forward it as they would have already had access to it or why they would have sent Mr P a message first saying verification was needed. So, I think it's more likely than not that Mr P sent the scammers the QR code.

Can Revolut fairly treat the payments as authorised?

Mr P says the scam started with the premise that there had been several attempts to use E's account. There are a number of possibilities about how this scam evolved, and how Mr P was supposed to help them.

Sometimes customers are tricked into sharing secure codes under the belief they are giving access to their account so it can be protected or to prevent payments. Alternatively, sometimes customers are persuaded payments need to be made before they can be refunded, to help their provider investigate fraud, or to keep their funds safe. Without knowing why Mr P shared the OTPs and took the steps he did (as I've concluded above) we can't know which it was.

However, the act of Mr P unblocking his card on one or two occasions would indicate he was aware payments would be made. In relation to when Mr P was asked to unblock the card, he's said *"They convinced me that they were closely monitoring fraudsters and scammers and asked me to help them."* This could also indicate Mr P was tricked into assisting the scammer investigate the fraud by allowing payments. Ultimately though, without an explanation from Mr P about why he shared OTPs and unblocked his card on the second occasion, I don't think it would be reasonable to conclude that the payments were unauthorised and that Revolut had acted unfairly in holding E liable for the payments. This is because if Mr P had agreed to payments being made, even if he wasn't expecting to lose those funds permanently, they would be considered authorised.

For these reasons I think Revolut can fairly hold E liable for the payments under the PSRs.

Did Revolut miss an opportunity to prevent E Ltd's loss?

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 PSRs and the terms and conditions of the customer's account.

But, taking into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice, Revolut ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances

Revolut has now agreed with my indicative findings that by the first successful payment it ought to have identified that E was at an increased risk of financial harm from fraud. It has also accepted that a proportionate intervention would likely have prevented the loss. So, I don't think it's necessary to go into detail as to why I consider that to be the case. It follows that Revolut should fairly reimburse the loss it ought to have prevented.

Should E bear any responsibility for its loss?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I accept that Mr P was manipulated into taking the steps that he did, and that it was a high-pressured situation. I understand scammers often use sophisticated social engineering techniques to create a sense of panic. I've also taken into account that the scammer did call themselves "Revolut Business" on WhatsApp and Any Desk.

But I've also considered that the scammer doesn't appear to have spoofed Revolut's phone number when calling Mr P or on WhatsApp. Nor did they share any information with Mr P about the account to verify themselves. At the time the scammers called Mr P, there wasn't any suspicious activity on the account to support what they were saying – I can see this because Mr P received the OTP to set up an Apple Pay token which was then used by the scammer before the first declined payment from E's Revolut account was attempted.

Mr P was also persuaded to unblock the card twice, even though he appeared to have recognised this contradicted protecting the account which he was told was still at risk.

When Mr P shared the OTP to reset the passcode on the account, this was after he had seen payment attempts, unblocked his card, and shared a QR code to give access to E's account. This was also about half an hour after he received and shared the OTP to set up Apple Pay and after he received two SMS messages from Revolut saying they had blocked his card to prevent fraud. So, by this point it appears there was an obvious risk to E's account. Without knowing why Mr P shared the OTP to reset the password, which ultimately was then used by the scammer to access the account and unblock the card a further time before any of the successful payments could be made, I don't think it would be reasonable to conclude that he hadn't been negligent in a way that contributed to E's loss

For these reasons I think it would be fair to hold E responsible for 50% of the loss in the circumstances.

Other considerations

Mr P has explained that the scam and financial loss had a significant impact on E and on

him personally. As the complainant here is E, I can't make an award for any distress the matter has caused him personally. Similarly, Mr P appears to have taken out personal loans which are separate from E and so I am not making an award for the costs to Mr P personally in relation to that.

I've asked about the impact on E and accept in principle that a large financial loss can impact a small business' ability to operate. But I don't consider that I've received sufficient information to support making an award for consequential losses to E. Mr P has referenced a contract E couldn't fulfil but with very limited detail. However, Mr P lent E a larger amount than the award I'm making within a couple of weeks of the fraud to mitigate the impact of the fraud. So, I'm not persuaded that Mr P has shown E would have fulfilled the contract he's referenced and operated successfully without amounting the debt it is now in had Revolut reimbursed this sooner. I think it's more reasonable to award interest to reflect the time the company was without the funds.

While I note Mr P has made a wider point about Revolut and media attention it has received in relation to fraud, I've considered the individual circumstances of this complaint when reaching an outcome.

My final decision

My final decision is that Revolut Ltd should:

1. Reimburse E Ltd 50% of the disputed payments – which is £16,956.86.

2. Pay E simple interest at a rate of 8% on this amount from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask E to accept or reject my decision before 6 February 2026.

Stephanie Mitchell
Ombudsman