DRN-5099755

The complaint

C, a limited company, complains that Revolut Ltd won't reimburse them for funds they lost as the result of a scam. They'd like the losses to be refunded.

C has appointed representatives to deal with this complaint, but for ease of reading I'll only refer to C.

What happened

In February 2024 a director of C was contacted by someone claiming to be from Revolut's fraud team, who told her that there had been some suspicious login attempts on the account. She was persuaded that she needed to take steps to secure the account. The caller went through several payments that the director recognised. To confirm that these payments were genuine the caller asked for several one-time passcodes (OTPs), which the director gave. They later asked for OTPs to suspend the card, and to block C's account.

But the caller wasn't from Revolut but was instead a scammer. They had used the OTPs to set up new payees from C's account. In less than an hour around £138,000 was taken from C's account in a mixture of transfers and card payments.

The director contacted Revolut through the app to report what had happened. Revolut contacted the receiving bank, but there were no funds available to return.

C asked Revolut to reimburse them for the losses, arguing that they didn't authorise the transactions. Revolut declined to refund them, arguing that they had sent an email with a link to confirm a new login, and this had been clicked. After this the director had given over the OTPs that had allowed new payments to be set up and a passcode changed. They also said a selfie verification and QR code check had been passed. On this basis they declined to refund C.

Dissatisfied with this C referred their complaint to our service. One of our investigators thought the complaint should succeed in part. He felt it clear the transactions were completed by a scammer, so couldn't reasonably be considered authorised. He didn't find any evidence of a selfie being sent, or a QR code test being passed. But he thought that as the director had shared security details with the scammer, Revolut could hold C liable for the transactions, under their terms.

But the investigator thought that the pattern of transactions was so unusual that Revolut ought to have taken steps to intervene and decline the payment requests. And had they done so and attempted to contact the director of C, our investigator thought it likely the scam would have come to light and prevented any further losses. But he also thought that C should bear some liability for contributory negligence. Overall, they recommended the remaining losses be split equally – along with a refund of any currency conversion fees. He also recommended 8% simple interest per annum be added to the losses, from the date of payment to the date of settlement.

Revolut accepted this outcome. But C declined, saying they didn't accept their actions should render it equally culpable to Revolut. They said by not carrying out a selfie or QR code verification, Revolut hadn't followed their own security processes. And that C shouldn't be held responsible for transactions after the point Revolut ought to have intervened.

This didn't change the investigator's mind, so the case has been passed to me to make a final decision.

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.

I've taken in to account the relevant regulations, legislation and industry guidance in place at the time – along with Revolut's terms and conditions, and what I consider to have been good industry practice at the time.

Authorisation and keeping security details safe

Revolut have accepted the investigator's outcome – so I see that it's broadly accepted that C didn't make these transactions. But I think it's important to outline my thinking on whether these payments would be considered "authorised".

The relevant regulations to this complaint at the Payment Services Regulations 2017 (PSRs). These outline the expectations on payments service providers in how to process transactions, including when payments will be considered authorised. The regulations also define when a payment service provider – like Revolut here – will be liable for any unauthorised transactions.

Broadly, the payment service provider is liable to refund any transactions the payment service user didn't agree to. Although there are caveats to this, which are outlined in Section 77 of the PSRs.

C didn't authorise the payments, nor can I see that they held out the scammer as their agent to Revolut, such that they would be considered "apparently authorised".

But based on what they've told us, and the publicly available information, at the time of their complaint, C had more than 10 employees. So, C would not be considered a "microenterprise". This is an enterprise with fewer than 10 employees and assets or turnover less than €2million.

This distinction is important to this complaint as the PSRs allow the parties to disapply certain provisions, including Section 77 to enterprises that are not consumers, microenterprises or charities. And I can see in the terminology of the Revolut terms and conditions in place at the time C would be considered a "large corporation" – simply that it is an enterprise that doesn't meet the definition of a microenterprise.

In the Revolut terms it explains under the heading "When a payment does not go as planned" it says when someone steals from your Business Account:

> *We may pay the money back and restore your Account to the state it would have been in if the amount had not been stolen. We won't provide a refund if the theft happened because you didn't keep your security details safe or evidence suggests that you acted fraudulently. We'll treat any payment instruction given using the*

Revolut card or the Open API as evidence that you authorised the payment or didn't keep your security details safe.

There's no suggestion anyone at C has acted fraudulent. So, the question to consider is whether C kept their security details safe. Here, the director of C has shared an email with a link to validate a new login, along with the OTPs. Because these are security features used by Revolut to ensure requests are genuine, I'm satisfied that the email and OTPs are considered security details. And I'm satisfied that by sharing these with the scammer, albeit under false pretences, the director has failed to keep the security details safe.

C has highlighted that Revolut had initially said that a selfie check and a QR code verification were passed, and that these didn't happen. Revolut have now accepted they don't have the record of these checks taking place, and it's unclear why this was relied upon in their response to C. But I don't see that this changes the underlying finding that the director of C had failed to keep the security credentials safe.

Under the terms of the account then, it's reasonable for Revolut to decline to refund C. But I have gone on to consider whether there may have been errors or omissions by Revolut, and whether they could have done more to prevent any losses to C.

Could Revolut have done more to prevent the transactions?

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.

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 February 2024 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 and the different risks these can present to consumers, when deciding whether to intervene.

Revolut accepted the investigator's opinion that they should have intervened to prevent the first transaction. While this was for a relatively small amount compared to what was later taken, it was set up on a new device and the payee name didn't match the recipient account. And I see that it's accepted that any proportionate intervention would likely have prevented the losses to C – both from the transfers out of the account, and the fees for converting currencies as well.

Should C accept some responsibility for the losses?

I see that the primary remaining dispute here is whether C should accept a degree of liability for the losses suffered. This is down to the concept of contributory negligence – where

someone has suffered losses, that may have in part contributed to these losses themselves. In these scenarios I may consider it fair to make a deduction in any award to reflect this.

A key principle here is that the director of C would be expected to act in the best interests of the company. And the starting point for my consideration of contributory negligence is what a reasonable person would do in the circumstances, and whether their actions fell below this.

In my view, this was a sophisticated scam – the scammer was obviously familiar with Revolut's authorisation processes. And the recollection from the director, as well as the chat history with Revolut, make it clear that the scammer was convincing and persuasive. They were creating new payees with names that matched existing payments – so that when the director saw the notifications it created some familiarity. So, I can see how they were convinced to hand over the OTPs.

But while they were no doubt convincing, I'm not persuaded the overall story was plausible. A financial business wouldn't require codes from a payer to confirm payments that had been made several days previously. The OTPs also referred to payments being made from a device which I understand isn't the device the director used – which ought reasonably to have prompted some concern. They also refer to "transfers" when the previous payments had been card payments.

The email with the link to confirm a new login was forwarded to an email address that mentions Revolut but isn't the genuine Revolut domain. But I note there is no warning on the email not to forward it on. But it does say that if it wasn't done by the recipient to change the account password immediately. It's likely that it was this email that gave the scammer's access to C's account.

Individually, these may not seem compelling. But together these ought reasonably to have given the director of C pause. I see that there is enough to say that there would have been reasonable grounds for the director to attempt verify what the scammer was telling them on the phone – such as contacting Revolut through the app, as the OTPs suggested. Had they done so, it's likely the scam would have come to light.

With that in mind, I'm satisfied that it would be appropriate for me to make a deduction for contributory negligence.

What is fair redress in the circumstances?

I've concluded each party has failings here – that C has failed to keep their security details secure, which has allowed the payments to be set up. But also, that Revolut ought reasonably to have declined the payment transactions.

I have considered carefully what C has said in response to the investigator's opinion, about their belief that Revolut's failings were greater. They've pointed out that Revolut ought to have intervened, which would have prevented any subsequent losses. But I see that the initial point of compromise is the sharing of the email that allowed the scammers access to C's account. There are failings from both parties are before any loss occurred.

As such, I don't see that one party bears significantly more responsibility than the other. I'm satisfied that the fair way to apportion the losses is to split them equally – so in this scenario Revolut should pay C 50% of the remaining losses to the balance of the account. I understand since the investigator's opinion an amount may have been recovered from the receiving bank. So, the award is based on the remaining losses, after the funds recovered.

I'm also satisfied that it would be reasonable for Revolut to apply 8% simple interest per annum to the refund, from the date of loss to the date of settlement. This is to reflect the time spent without these funds. Revolut should also refund any currency transactions fees or charges.

If Revolut considers that it's required by HMRC to deduct tax from the above interest award, they should tell C how much has been deducted. They should also provide a certificate showing this, should C ask for one.

My final decision

My final decision is that I uphold this complaint, and direct Revolut Ltd to settle it as outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask C to accept or reject my decision before 27 March 2025.

Thom Bennett
Ombudsman