DRN-5462150

The complaint

Q, a limited company, complains that Revolut Limited have unreasonable declined to refund them for their losses from a scam. They'd like these funds returned to them.

What happened

The background to this complaint is well known to both parties, and largely not in dispute. So, I will cover them off only briefly here.

In February 2024 one of the directors of Q received a call from someone claiming to be from Revolut's fraud team, claiming that a fraudster was trying to access Q's account. At the same time Revolut sent genuine emails that confirmed attempts to login. The director was told that he would receive a one-time passcode (OTP), and that he needed to provide this to the caller to confirm his identity to lock down the account. The director gave over the code to the caller.

Unfortunately, the call wasn't from Revolut, and the director had been scammed. The code was used to set up a new payment device on Q's Revolut account – which led to six payments being sent in quick succession. This totalled £9,518.99.

The director contacted Revolut and told them what had happened. They in turn contacted the receiving bank but were told that no funds remained to return. Revolut declined to reimburse any of the losses, arguing that the director had beached the terms of the account by sharing security information with the scammer – including an email containing a link to confirm a new device. They felt by doing so the director had given authority to the scammer to carry out the transaction.

Unhappy with this answer Q referred their complaint to our service. One of our investigators looked into what happened. He concluded the director had shared the email and codes to set up the new device. He thought that under the terms of the account it was reasonable for Revolut to decline to refund the transactions. But he also thought that the pattern of transactions ought to have concerned Revolut enough that they shouldn't have processed the transactions and instead intervened to discuss the transactions with the director of Q – and this would likely have prevented any further losses.

He also thought the director of Q had contributed to the loss by sharing the codes. They suggested the loss be shared equally – and that Revolut should refund half the losses, plus 8% simple interest per annum for the period Q had been without the funds.

This was accepted by Q. Revolut did not respond. As such the complaint was passed to me to decide. Upon review I broadly agreed with the investigator's outcome, although my suggested redress was different. I issued my provisional decision that said:

Authorisation and keeping security details safe

The regulations relevant to this complaint are the Payment Services Regulations 2017 (PSRs). These outline the expectation on payment service providers (PSPs) in how to

process transactions – including when they'd be considered to be authorised. The key consideration here is whether the payer gives their consent to a payment using the "form and procedure" agreed with the PSP. Typically, this form and procedure will be outlined in the terms of the account.

The regulations also outline when a PSP will be liable for any unauthorised transactions. Generally, the PSP will be expected to refund any transactions a payer didn't agree to. Although there are certain caveats to that – such as whether they have kept their personalised security credentials secure, either intentionally or with gross negligence. These are outlined in Section 77 of the PSRs.

But the PSRs also make provision for payers who are not "consumers, micro-enterprises, or charities". For these payers it can be agreed with the PSP that certain sections do not apply – such as Section 77. In most cases this is agreed within the terms.

For the purposes of this decision, I should explain that a micro-enterprise is any enterprise that has a turnover and/or balance sheet below €2million, and fewer than 10 employees. But from what Q has told us, and based on publicly available information, they have more than 10 employees for the accounting period the transactions took place, and for the two years previously. For the PSRs' purpose Q wouldn't be considered a micro-enterprise.

In the terms of the Revolut account, Q is referred to as a "large corporation". The terms discuss "if a payment does not go as planned" and under "If someone steals from your business account" it explains what Revolut will do.

> *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.*

It seems accepted by Revolut that these transactions weren't carried out by Q, and that the payments were made by a malicious fraudster from a newly set up device. So, I'm satisfied that someone has stolen from Q's account, and this is the term that applies. There's no suggestion anyone at Q has acted fraudulently. So, the consideration for me to consider here is whether Q kept their security details safe.

The terms say that "security details" include usernames, API keys, passwords, PINs and "any other information you use to access your Revolut Business app". The director of Q has questioned how the scammer initially got hold of their details, and believes they may already have had the password to the app. I don't see that I can get to the bottom of those questions, but I should say I've seen nothing to suggest Revolut supplied it to them.

The director has accepted that they gave over at least one OTP to the scammer – the evidence suggests OTPs were needed to confirm a new login, set up the new payee, and reset the password on the account. And the evidence suggests that they forwarded the email with the link to set up a new device to the scammer as well. I appreciate this is in the context that the director thought they were taking steps to safeguard Q's account. But these were required for the new device to be set up to make payments.

Revolut have said that they would have required a selfie verification but haven't been able to supply any further information, and the director denies providing a photograph or similar information. I also note from the terms that this verification feature wasn't expressly part of the form and procedure for authorising payments. So, I'm not necessarily persuaded a selfie

verification took place – but I don't see this makes a difference to whether the transactions were authorised or not.

But overall, I think it is clear the director didn't keep the security details – the OTPs and the email – safe.

I consider that under the terms of the account, and the relevant regulations, then its reasonable for Revolut to decline to refund Q. But I've also gone on to consider what's fair and reasonable in the circumstances of the complaint.

Could Revolut have done more to prevent the scam?

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 PSRs 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 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 customers, when deciding whether to intervene.*

Here, I'm not persuaded that the first transaction ought to have prompted any particular intervention by Revolut. It was for a relatively low value of £59.99, and the records indicate there was an additional verification OTP sent as well. However, there was also a confirmation of payee mismatch – the account name entered didn't match the receiving bank name. But I'm not persuaded this is enough to prompt further action from Revolut.

But this was then followed rapidly by a conversion of a significant sum that was held as USD with Revolut to GBP. There was another transfer of £1,253 to the same account about a minute after, followed by a third of £2,142 only 13 seconds later – and at this point I see it would be reasonable for Revolut to have attempted a human intervention. There was now a newly added device making rapid transfers to a newly created payee, which is out of character for the account usage.

I recognise that Q's account had been used to make payments of this value previously, but not in such quick succession to a single new payee. And I'm minded that the newly added device and confirmation of payee mismatch should have prompted further concern as to the risk the account was falling victim to financial crime.

I see by the third payment attempt Revolut ought to have declined or delayed the payment requests until they'd been in touch with one of the signatories on the account. And had they been in touch with the director, I see it likely that the scam would have unravelled at this

point and there would have been no further losses. So, I think it would be reasonable to direct Revolut to refund the transactions from this point.

Should Q bear any responsibility for the losses?

I've gone on to consider whether Q should accept some liability for the losses suffered – through any contributory negligence on their behalf. As I concluded earlier the fraudster could only gain access to Q's account because the director had failed in their obligations to keep their security details safe – by sharing the initial email and the OTPs.

This was in the context of the director believing they were taking actions to prevent any losses to Q, and I see that this was quite a sophisticated scam. But I'm also minded that there should be a reasonable expectation for the director to be cautious about sharing information. So, I see that it would be reasonable for Q to bear some responsibility for the funds lost.

Customer service

The director of Q has highlighted to Revolut that they waited a long time for a response from Revolut. Looking through the chats I'm satisfied that the scam was reported promptly, but there was no outcome for over three weeks. There doesn't seem to be a clear explanation of why this was.

I can see how this would be disruptive to Q's business and take the director's time away from other matters. So, I think it's reasonable that Revolut pay a degree of compensation to reflect this.

Putting things right

I don't consider that either Q or Revolut bears significantly more responsibility than the other. I'm minded that the fair way to apportion the preventable losses is to split them equally. So, in this scenario this would mean asking Revolut to refund 50% of the losses from the third payment onwards – I make this out to be £4,103.

It would also be reasonable for Revolut to pay 8% simple interest per annum on this amount, from the date of payment to the date of settlement. This is to reflect the loss of use Q has had of these funds.

Revolut should also pay Q £200 compensation for the disruption caused by the delay in responding to the claim.

This was accepted by Q. Revolut did not respond before the deadline.

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.

In the absence of any new evidence or considerations from either party, I remain satisfied with the conclusions reached in the provisional decision.

I'm satisfied that under the terms of the account Revolut can hold Q responsible for the transactions, because Q is considered a "large corporate" business, and the director didn't keep their account details safe.

But I'm also minded that Revolut ought reasonably to have intervened to ask further questions on the third payment, as the account was now clearly showing signs of falling victim to financial harm. Any reasonable intervention would have prevented any further losses. It's fair for Revolut to accept some liability for Q's losses.

I'm satisfied though that Q has contributed to their own loss, so it's right that a deduction be made. And I don't see that one party bears significantly more than the other – so a 50% deduction is reasonable.

Lastly, I'm satisfied that the service provided by Revolut was not of the standard I'd expect to see. I'm satisfied this will have contributed to the inconvenience and disruption to Q's business. As such, it would be appropriate for Revolut to pay £200 compensation to Q.

Putting things right

To resolve this complaint Revolut must:

- Refund Q 50% of the losses from the third payment onwards – I make this to be £4,103.
- Add 8% simple interest per annum to this figure, from the date of payment to the date of settlement. If Revolut considers that HMRC requires them to deduct tax from this amount they should let Q know how much has been deducted, and provide a certificate showing this should Q ask for one.
- Pay Q £200 compensation.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Q to accept or reject my decision before 5 May 2025.

Thom Bennett
Ombudsman