

The complaint

L, a small business, complains that Revolut Ltd have unreasonably declined to refund them for two transactions they say they didn't agree to. They'd like the transactions refunded to them.

What happened

L holds an electronic money account with Revolut. In December 2022 one of the directors of L received a text message from Revolut with a one-time passcode (OTP). They say they subsequently received a call but did not enter into a conversation with the caller. They next received a text to confirm that their Revolut card had been added to a new Apple Pay wallet.

This device was used in a shop in London. Two transactions – one for £24,650 and one for £1,100 were completed before Revolut declined any further Apple Pay transactions. L reported these as unauthorised, and asked Revolut to refund them.

Revolut declined to do so, saying they could not successfully raise a chargeback under the scheme rules, as a valid Apple Pay wallet had been used.

L complained about this outcome, but Revolut stuck to their explanation. But they accepted their communication had been poor, and their response hadn't been sent within 15 days. They offered L £200 compensation for the service.

Unhappy with this, L referred their complaint to our service. One of our investigators looked into what happened. The director had by then left L. But they spoke to our investigator about what had happened. They said they were in a different area of the country to the transactions and cannot remember the nature of the conversation with the caller. But they said they didn't remember giving over the OTP.

The investigator thought it more likely than not that the director had shared the OTP with a fraudster, which allowed the new Apple Pay to be set up. They felt that under the relevant regulations the payments were unauthorised, but the director had been grossly negligent in handing over the code. This meant Revolut weren't liable to refund L.

But the investigator thought that as the first payment was so out of character for the account and had been made with the newly set up Apple Pay device, this should have given Revolut cause for concern. They felt the bank shouldn't have processed this transaction without confirming it with the L – and had they done so this would have prevented the loss. But they also thought that L's director had contributed to the loss by negligently handing over the OTP. They suggested Revolut refund 50% of the loss, plus 8% simple interest per annum from the date of payment to the date of settlement.

Revolut declined this, saying that from the moment that the OTP was shared then the payments should be considered authorised. They said that that L's account had handled much larger transactions than this, and it fell within the expected turnover of the business account. They also questioned that if the director had been grossly negligent, why they would be held liable for the transaction.

The investigator didn't think these points changed anything and still thought it reasonable that Revolut ought to have intervened before the first transaction.

As no agreement could be reached the complaint was passed to me to decide. On review I agreed with the investigator's outcome, although my reasoning was slightly different. I issued a provisional decision that said:

Authorisation and keeping security details safe

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. One of which is whether the user breached their obligations to the payments service provider with "gross negligence" – which is the test the investigator relied upon in their assessment.

L has said they didn't authorise the payments, although Revolut have argued that by sharing the code the payments are considered authorised.

At the time of their complaint, L had more than 10 employees, so would no longer be considered a "microenterprise". This is an enterprise with fewer than 10 employees and assets or turnover less than €2million.

In the terminology of the Revolut terms and conditions they would be considered a "large corporation" – simply that it is an enterprise that doesn't meet the definition of a microenterprise.

This distinction is important to this complaint as the PSRs allow the parties to disapply certain provisions, including Section 77. The Revolut terms explain this under the heading "Corporate Opt Out".

The relevant section of the Revolut terms at the time is 24 – What happens if someone steals from my account? For large corporations this says:

you must contact us within three months of the date the money was stolen from your account. We'll then refund the amount that was stolen 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.

The test whether L would be liable isn't whether they failed in their obligations with gross negligence – which I would take to mean proceeding with actions that show a significant disregard of an obvious risk. Instead, it's a test of whether the security details were kept safe. The Revolut terms say that "Security details include usernames, API Keys... and any passwords that allow access to the Revolut Dashboard." This doesn't specifically include the OTP, but I my reading of the terms is that this isn't intended to be an exhaustive list.

I'm satisfied the OTP would reasonably be considered part of the array of "security details", as it is a security feature intended to identify whether an instruction is legitimate.

We've spoken to the then director, who couldn't specifically remember giving over the OTP when they were called. However, I've been given no evidence to suggest they were involved in any fraud or deception here. And they've provided evidence that they were in a different area of the country to the disputed transactions. So, I'm satisfied that the transactions were likely carried out by an unknown third party fraudster – so in plain terms it was stolen.

It seems more likely than not that the director did give over the OTP to a fraudster, which then allowed the fraudster to add their card to an Apple Pay wallet. There doesn't seem to be any other reasonable explanation. If the fraudster was able to access the OTP by some other method, then they wouldn't have needed to speak to the director. I'm satisfied this means that the theft likely happened because they failed to keep their security details safe. So, under the relevant account terms Revolut would be within their rights to decline to refund L. I don't see it's unreasonable that they've done so.

This means any finding I'd make on whether the payments in dispute were authorised or unauthorised is irrelevant – in either eventuality Revolut can hold L liable for the transactions under the terms of the account. As such, I do not intend to make a finding on this point.

But I will note that this is only a conclusion on whether the regulations and terms or the account require Revolut to refund L. I have also gone on to consider whether there have been an errors or omissions by Revolut, or whether they could have done more to prevent the losses to L.

Could Revolut have done more to prevent the transactions?

Generally, under the PSRs Revolut will be expected to process payment requests – including those made by card or through Apple Pay – without intervention. But there is also a reasonable regulatory expectation for payment institutions to monitor accounts and payment activity for signs of financial crime or financial distress.

In this case, the terms of Revolut's contract with L modified the starting position from the PSRs, by – among other things – expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks" (section 22).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider

to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in December 2022 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMIs like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;¹
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So, it was open to Revolut to decline card payments where it suspected fraud.

¹ For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/

Overall, 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 December 2022 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 – (as in practice Revolut sometimes does); and
- 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.

And in practice I know Revolut declined any further transactions after the second payment, so I'm satisfied that at least some of these systems were in place at the time of the fraud.

Having taken this into account, I'm satisfied it would have been fair and reasonable for Revolut to decline the first payment instruction of £24,650.

Firstly, this payment is considerably more than had been made by card payment up to that point. I can see from the account history that there was a high volume of card payments, although the vast majority were for less than £1,000. There had been a few high value card payments in the month prior to this transaction – for example £6,241.24 in November 2022 and £3,522.48 in October 2022. But the first disputed transaction is several times larger than any previous card transaction the account had made previously.

I've considered what Revolut have said about the account being used for large payments before those in dispute. I can see in the weeks leading up to the disputed transaction that there was a payment of £22,066.40 to a supplier on the same day as £7,574.26 was paid to HMRC. These however were paid by bank transfer. I see that the payment method is relevant to consider here. The change in payment method indicates a significant change to the regular operation of the account, which is a factor that may indicate fraud or financial crime

The payment instrument used – the Apple Pay device – had also only been created that day. I'm not persuaded that the use of the OTP to set up this device mitigated the fact that it was rapidly used to make a very high value payment. The OTP would allow the device to make transactions without any additional authentication procedures from Revolut. So, I see that this ought reasonably to be seen as an increased risk.

I accept what Revolut have said about this being a business account, and it's turnover and use being different from that of a personal account, or even that of a microenterprise. This means payments can be unpredictable.

But I also bear in mind that Revolut did decline the third transaction attempted, which was for a lower value. They haven't been able to provide an explanation of why this was the point the device was blocked – so I'm not going to speculate on this. But it does tell me that the transactions triggered some concern within Revolut's systems.

Overall, I am minded that the first transaction of £24,650 stands out enough that it would have been reasonable for Revolut to decline it – in line with the terms of the account. Had they done so, I'm satisfied that it's likely the fraud would have come to light and L would not have suffered any losses. So, I intend to uphold L's complaint on this basis.

Should L accept some responsibility for the losses?

I've gone on to consider where L should accept some liability for the losses suffered – through any contributory negligence on their behalf.

As I've concluded earlier the most rational explanation I can see for the setting up on the Apple Pay device is that the director gave over the OTP to the fraudster.

The text of the OTP code makes it clear that it is for adding a card to a new Apple device, and not to enter it anywhere unless you want to add the card. The text also says not to share this with anyone, even if they claim they are from Revolut. This seems very clear to me what the code is for, and that it shouldn't be shared.

As the director hasn't given us a plausible explanation of why this was shared, or what they were told to make it seem like a reasonable thing to do, it's difficult for me to gauge the sophistication of the scam. But I think a director of a small business should have due regard to the warnings in the text. I can only reasonably conclude that the director was negligent in sharing this code.

We've also seen evidence that Revolut texted again to confirm the Apple Pay device was set up. The director has acknowledged seeing this message, but not taking any action.

I think a reasonable person on seeing their card added to a device they weren't expecting would act quite quickly to prevent any further use. But this doesn't appear to have happened. Again, I think this is a degree of negligence that contributed to L's losses.

How should the losses be split?

I've concluded that each party has failings here – the Apple Pay device was likely only set up because of the negligence of the director in sharing the OTP. But I'm also minded that it would have been reasonable for Revolut to decline the transactions.

I can't see that one party bears significantly more responsibility than the other. I'm minded that the fair way to apportion the losses is to split them equally – so in this scenario Revolut should repay L 50% of the losses.

I'm also satisfied it would be reasonable for Revolut to 8% simple interest per annum to this amount, from the date of loss to the date of settlement. This is to reflect the time spent without these funds.

Inconvenience caused to L

Revolut have accepted they didn't respond appropriately to L's claim or provide an answer within a reasonable timescale. They have already paid £200 for this. I'm minded this is a reasonable amount and in line with what I would have recommended.

I thought it reasonable Revolut:

- Refund 50% of the losses - £12,875

- Add 8% interest per annum to this amount from the date of payment to the date of settlement

Neither party responded to my provisional decision before the deadline. So, it now falls on me to issue my 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.

With no new evidence or points from either party to consider, I remain satisfied with the conclusions reached in the provisional decision.

- I do not need to reach a conclusion on whether the transactions would be considered authorised under the PSRs – in either eventuality the terms of Revolut's small business accounts allow them to hold L liable. I find it more likely than not the director of L shared the OTP with a fraudster, that allowed the Apply Pay device to be set up. In doing so they have failed in their obligations to keep their security credentials safe.
- I'm satisfied that at the time of the transactions Revolut would reasonably be expected to have in place systems and controls to monitor accounts, to detect potential fraud. Revolut's terms allow them to do this. That the third payment was stopped shows these systems were in place and active at the time.
- I'm satisfied that the first payment of £24,650 was so considerably outside the normal running of the account, with the added risk that it was a brand new payment instrument, that it would have been reasonable for Revolut to decline to process it. Had they done so I'm satisfied the fraud would have come to light and the losses would have been prevented.
- However, I'm also satisfied that it's reasonable L take some responsibility for the losses. By sharing the OTP the director of L has been negligent, which has contributed to the loss. And the director could have helped mitigate any losses by taking action when they received confirmation of the new payment device.
- Considering the faults of both sides, dividing the losses equally is a reasonable outcome. This means Revolut must now pay 50% of the outstanding losses – and add 8% simple interest per annum from the date of the loss to the date of settlement, to reflect L's loss of use of those funds in that period.

My final decision

My final decision is that I uphold this complaint and direct Revolut Ltd to:

- Refund L £12,875, which represented 50% of the losses
- Add 8% simple interest to this amount, from the date of payment to the date of settlement.

If Revolut consider that HMRC requires them to deduct tax from the interest award, they should provide L with a certificate showing how much has been deducted. L can then reclaim this directly from HMRC, if they are eligible.

Under the rules of the Financial Ombudsman Service, I'm required to ask L to accept or reject my decision before 2 December 2024.

Thom Bennett
Ombudsman