DRN-5834241

The complaint

Mr S brings this complaint on behalf of Z, a limited company. Z complains Revolut Ltd hasn't reimbursed it for its loss after it was the victim of a scam.

What happened

On 20 February 2024, scammers contacted Mr S and the following events took place:

Time	Activity	Amount
14:43	A new device log in attempt email sent to registered email address	
14:49	Mr S forwarded the new device log in email to scammers	
15:06	New device created a virtual card (first activity carried out by new device)	
15:18	OTP 1 - Text message with one time passcode (OTP) to allow viewing of virtual card details sent to registered mobile number	
15:26	OTP 2 - Text message with OTP allowing a transfer of £11.10 sent to registered mobile number	
15:26	Payment 1 - transfer	£11.10
15:26	Payment 2 - transfer	£878
15:27	Payment 3 - transfer	£856
15:27	Payment 4 - transfer	£956
15:27	Payment 5 – transfer	£942
15:27	Payment 6 - transfer	£981
15:28	Payment 7 - transfer	£951
15:28	Payment 8 - transfer	£912
15:28	Payment 9 - transfer	£952

15:29	Payment 10 - card payment	£1,000

Mr S, who has authority to use Z's account, has told us:

- On 20 February 2024 he was contacted by scammers pretending to be Revolut. They told him Z's account had been accessed by a third party and he needed to follow their instructions in order to secure the account.

- He logged into Z's online banking account and could see a new device had been added. He tried to log it out immediately but got an error message and the new device wasn't removed. Seeing this new device persuaded him the call was genuine as it evidenced someone had accessed Z's account.

- Shortly after the call began, Mr S received an email confirming a log in attempt had been made and the scammers asked him to forward this to them, which he did. He then received several text messages containing OTPs which he also gave to the scammers believing it was helping remove the new device that had been added.

- Towards the end of the call, the scammers told Mr S to log out of his account and delete the Revolut application from his phone. He was told to wait for an update before logging back in while they continued to secure the account. Mr S became suspicious after noticing the text messages with the OTPs included the new device details and logged back in on another of his devices. He then discovered the transactions scammers had carried out and the call ended.

- Mr S said he didn't provide any log in details to the scammer and believes flaws in Revolut's security systems have allowed them to access Z's account. He also believes that errors with Revolut's systems showed a new device as being logged in before the two stage authentication had been completed and prevented him from logging out the device at the start of the scam. Had these errors not occurred, the scam would've been prevented.

Revolut has told us:

- It believes Mr S has acted with carelessness in allowing scammers to access Z's log in details and forwarding the email that allowed a new device to access the account. It also feels he was careless in sharing two OTPs with the scammers which allowed them to make the transfers and the card payments above. Because Mr S has acted carelessly it didn't think it was responsible for Z's loss.

- The new device added by scammers wouldn't have shown on the account until the two stage authentication process had been completed – which meant the email confirming the log in had to be sent and the link within the email clicked to confirm the log in.

- It has no record of any failed attempts to log out the new device that Mr S said was added by scammers, only a record the device was successfully removed by Mr S after it had been properly authenticated and the transactions had been made.

- Revolut had done what it could to recover the funds once the scam had been reported and it verified a scam had taken place, but no funds remained to return to Z.

I issued my provisional decision in December 2025 and said:

Did Z authorise the payments

In broad terms the starting position in law is that an account holder will normally only be responsible for the payments they've authorised.

Where a payment is authorised, that will often be because someone authorised to use the account has made the payment themselves. But there are other circumstances where a payment should fairly be considered authorised, such as where the account holder 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.

There's no suggestion in this case that Mr S, the only person authorised to use Z's account, made the payments himself. It appears scammers were able to access Z's account and make the transfers and card payment I've outlined above. However, I think in the case of 'Payment 1', the first transfer scammers made out of the account, Z authorised this, as Mr S gave permission for the payment to be made, even if he didn't understand the true circumstances surrounding it.

Mr S fell victim to what is known as a safe account scam. He was told by scammers Z's account had been accessed by a third party and that various actions needed to be taken in order to secure Z's account.

Scammers told Mr S that a third party had tried to make a payment of £11.10 to United Airlines the previous day but this had been stopped by Revolut. In order to secure the account, they said the payment had to be made. The scammers then attempted to transfer £11.10 to their account ('Payment 1') which prompted a text message with an OTP to be sent to the registered mobile number. The transfer could not be made without the OTP.

The text message Mr S received said:

> *"Confirm transfer of £11.10 to United Airlines. Device: [new device]… Use code: …Location: United Arab Emirates, Dubai…"*

Mr S gave scammers the OTP confirming this transfer could be made. So although he did so believing he was helping to secure the account, he gave his permission for the payment to be made. Because of this I think Revolut can fairly treat 'Payment 1' as authorised.

Gross negligence

Section 72 of the Payment Services Regulations (PSRs) set out the obligations of the payment service user in relation to payment instruments and personalised security credentials. It says:

> *"72. … (3) The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service"*

The PSRs set out that the payment service user is liable for all losses incurred in respect of an unauthorised payment transaction where the payment has acted with gross negligence. The PSRs don't define gross negligence but do set out that gross negligence means more than negligence, involving conduct exhibiting a significant degree of carelessness.

Reflecting this, the Financial Conduct Authority in its document setting out its role under the PSRs says "…we interpret "gross negligence" to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness."

So, whilst I have concluded all but 'Payment 1' of the transactions listed above were unauthorised, I have to consider whether Mr S failed with gross negligence to meet his obligations as a payment service user or to comply with the account terms and conditions in relation to the other payments.

Where it's not possible to know exactly what's happened, I need to decide what I think is more likely in the circumstances, on balance, based on the evidence available.

Mr S has said the scammers called him from a private number, not a spoofed Revolut number. He's said they had some personal details, but Z is a limited company. So its details, and details of those involved in the company (such as name, month and year of birth, and addresses) are publicly available. So it's not clear what information Mr S was initially provided by the scammers to persuade him he was talking to someone from Revolut.

Mr S has said at the start of the scam call he logged onto Z's internet banking account and could see the new device had already been added to the account. He says this gave everything the scammers subsequently said plausibility, because he could see someone was accessing his account.

But Revolut's records don't show this is the case. According to its records, Mr S logged into the account, seemingly from his own device, and checked the password several times. Shortly after this, a new device tried to log into the account which prompted an email to be sent to the registered email address as part of the two stage authentication process that allows a new device to be added. Mr S has confirmed he sent this email to scammers, but only after he spent some time trying to verify their identity further. And Revolut's records show the new device was added around 20 minutes after this email was sent, which aligns with Mr S's testimony that he discussed things with the scammer before forwarding it to them.

Mr S has said he didn't receive the new device log in email until some time after he'd logged into his account. He's also said he couldn't have logged into the account one second after Revolut's records show the email confirming the new device was sent. But the email was asking for confirmation of a new device, not the existing one. So Mr S logging in on his existing devices wouldn't have been prevented by the lack of response to the 'new device' email he hadn't yet sent to the scammers.

Given the two stage authentication process has to be followed, and given the very detailed records Revolut has of exactly when the log-in email was sent and when the new device was being used on the account, on balance, I don't think it's more likely the device was already showing when Mr S logged in from his existing advice at the start of the scam call. So it's not clear what information the scammers provided that persuaded him someone had accessed Z's account without his knowledge and that he should hand over the information he did.

Mr S has said as soon as he logged in he tried to remove the new device but Revolut's system showed him an error message. He's said if this error hadn't occurred the whole scam would've been prevented. As I've said I don't think the device likely was logged in at this point, and Revolut records don't show any error in trying to remove it.

I understand scammers are highly skilled at causing confusion and distracting victims so I think it's understandable that Mr S may not perfectly recall the sequence of events. Whilst I

have taken his testimony into account, I've had to balance this with the records Revolut has from the period in question. Overall I don't think the more likely scenario in this case is that the new device was showing as added before the authentication process was complete. I also don't think there is sufficient evidence to show Revolut failed to allow the device to be removed before it was later successfully removed.

Mr S has said he didn't give any of Z's log in details to the scammers. He's said they must've somehow obtained them elsewhere and overall he believes Revolut has flaws within its systems that have allowed the scam to take place.

In order to register a new device on Z's online banking account, the scammers needed to know the registered email address and a password or passcode. Z's individual log in details for its internet banking account wouldn't have been known by Revolut staff, so, it's not clear how scammers might've accessed this information if it wasn't disclosed by Mr S.

I understand Mr S has said this didn't happen. And I've considered his testimony carefully. I also accept that it would be unusual for anyone to hand over their banking log in details without recognising this was likely a scam. I'm aware there are other ways people might be tricked or persuaded to hand over their log in details. But Mr S hasn't provided any other plausible explanation as to how this information might've been obtained by scammers, such as any unusual websites or links he might've followed leading up to the scam. And I've noted that when Mr S logged in from his existing device, before the scammers new device was added, he seems to have viewed the account password.

I accept Mr S may not exactly recall how the scam happened or the sequence of events. But in the absence of any plausible point of compromise for Z's internet log in details it seems more likely than not this information was provided by Mr S.

As Mr S hasn't provided any information about why he might've provided this information to scammers it's difficult to establish why this might've happened. But I think even if he did think he was speaking to Revolut, a reasonable person would recognise a genuine bank wouldn't ask for these details and they shouldn't be handed over.

Knowing these details alone wasn't enough to give scammers access to the account. Once scammers tried to log into the account from the new device, using Z's individual log in details, an email was automatically sent to the registered email address linked to the account. Mr S has confirmed he received and then forwarded this email to the email address the scammers gave him. This email said:

> *"We got your login request. Before you confirm, take a moment to read the information below:*
>
> ***Before you click…***
>
> - *Did you make this request? If in doubt, **do not click below**. If someone is asking you to forward this email, **do not send it** to anyone…"*

Mr S forwarded this email to the scammers. He said he did have concerns about doing this and questioned why Revolut would need him to do this. He's said he also identified the domain name on the email address they gave him wasn't the usual Revolut domain name and asked the scammers about this.

To reassure him they were Revolut, the scammers sent Mr S a text message to prove it was them. He said he again questioned the message as it was different to the way Revolut texts usually appear. He said he was told it was different due to the account reset. Mr S has said

he was aware scammers could 'spoof' phone numbers and so the text message didn't prove anything, but despite this sent the email to the address provided. This allowed them to add a new device and access Z's online account.

Given the concerns Mr S said he had here, it's not clear what reassured him they were genuinely Revolut and that he should forward an email that sets out it shouldn't be forwarded. He had concerns about the email address he was using, and he also had concerns about the text message – which looked different to the usual messages received from Revolut. But despite this proceeded to send the email that allowed a new device to access the account.

After the scammers had access to Mr S's account from their own device, they first viewed the full card details of a virtual card on the account. Before they could do this a text message was sent to Mr S which said:

> *"Use code:… to confirm displaying card details in your Revolut Business app… Device: [new device]… Location: United Arab Emirates, Dubai…"*

Mr S's testimony is that he remembers providing 'one or two' OTPs to the scammers throughout the call. And the scammers were able to successfully view the card details that allowed them to later make a card payment. So it appears Mr S provided the OTPs in both messages to the scammers.

I don't think Mr S has explained why he thought he received the text message confirming someone was reviewing the virtual card details or why he thought Revolut staff securing his account would need to review the full card payment details. I can't see any plausible reason Revolut might've given to persuade Mr S it needed to do this when securing the account or setting up a new card or why it would need to send him an OTP in order to do so. The text message Mr S received about this activity also confirms the new device is carrying it out, which Mr S already knew belong to scammers, and shows the location as overseas. So it's not clear why he gave this information to the scammers.

In the case of the second OTP, which allowed scammers to transfer funds to a new payee and which subsequently allowed all subsequent transfers to be made, I think in isolation the circumstances were more persuasive as the scammers provided a specific reason the OTP should've been provided.

But at the point the scammers asked for the second genuine OTP I think the risk reasonably ought to have been obvious to Mr S. I think he'd likely provided Z's online banking log in details, had forwarded an email that allowed a new device to be added and provided an OTP that allowed them to view card payment details. Given all of this I think a reasonable person ought to have had serious doubts about whether they were genuinely talking to someone from their bank, and I think he ought to have recognised the serious risk in handing over another OTP which allowed a payment to be made.

Mr S likely provided Z's online log in details to scammers, forwarded an email that allowed them to add a new device and provided OTPs that allowed them to make payments. I think in providing this information to scammers Mr S hasn't taken all reasonable steps to keep safe Z's individual security credentials relating to a payment instrument or an account information service. Because of this I think Revolut is acting fairly in holding Z liable for its loss. However, I also need to consider Revolut's responsibility to Z.

<u>Should Revolut have done more to intervene when the payments were being made</u>

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what's fair and reasonable in this case.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably:

- *Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 banks 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, before it processed a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*

From 'Payment 2' onwards, all of the transfers and the card payment ('Payment 10') that formed part of this scam happened within seconds or minutes of the previous transfer. The transfers were all for similar amounts – between £800 and £1000 - and they were all being made to the same payee.

Whilst I don't think any single payment alone would've seemed unusual enough to have prompted intervention, I think by the time 'Payment 4' was made a pattern of repeated payments had emerged and Revolut ought to have recognised this pattern was indicative of a scam. Had it done so I would've expected it to have intervened and found out more about the transactions before allowing them to be made. And had it contacted Mr S to find out more about the transactions I think it's likely the scam would've been uncovered given he thought he'd already been speaking to Revolut. So I think Revolut missed an opportunity to prevent the payments being made from 'Payment 4' onwards.

Whilst I do think Revolut missed an opportunity to prevent some of the payments being made, for the reasons given I think Z's actions also contributed to its loss here. So I think Revolut should reimburse Z 50% of the payments from 'Payment 4' onwards.

Did Revolut do enough to recover the funds

Revolut didn't try and recall the funds as soon as Mr S reported the scam to it. It's said it needed some time to carry out further checks. Revolut is of course able to carry out whatever checks it feels best meet its obligations. But I consider it best practice that it tries to recall funds promptly when a scam is reported. It can of course choose not to do this, but it also takes on the risks associated with waiting.

In this case it waited around three days to contact the recipient's bank. And whilst most of the money had already been removed from the account by the time Mr S reported the scam, so Revolut delays didn't make a difference for the most part, it appears £39 did remain in the recipient account for several hours after the scam was reported. Had Revolut acted sooner, I can't see any reason this amount wouldn't have been returned to Z.

Because of this I think Revolut should pay Z the £39 it potentially prevented the recovery of.

Revolut responded and accepted the findings in my provisional decision. Z did not. Mr S responded on Z's behalf with a number of points and in summary said that:

- He had not provided any security information to the scammers that allowed them to access the account, and did not check his password when he logged on. He believes Revolut's systems had been accessed by the scammers which is how they obtained Z's log in information. He feels this is supported by the amount of Revolut accounts that are scammed generally.

- He reiterated the new device that carried out the disputed transactions was logged into Z's account when Mr S started speaking to the scammers which gave everything they told him credibility. Therefore, he didn't accept he hadn't taken reasonable steps to keep Z's account safe.

- He felt a number of the events shown in Revolut's records were incorrect and I should have requested more in-depth records that show exactly when the new device was logged in and when and why Revolut failed to allow Mr S to log the device out when he tried.

- An email informing Mr S of the new device log in attempt was not sent at 14:31 as I'd said in the provisional decision, it was sent at 14:43 and forwarded to scammers at 14:49. So Revolut's records were incorrect and this meant it had admitted a new device was logged in at 14:31 before the two stage authentication had been completed supporting his testimony.

- The email quoted in my provisional decision was not the email he'd received confirming a new device had attempted to log into the account and that he'd forwarded to scammers.

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 want to assure Mr S I have considered all Z's points very carefully and have considered the complaint in full, again. Whilst I have taken Mr S's response into account, I haven't responded to everything again here. Where I haven't responded to a specific point, I'm satisfied the reasoning and answer given in the provisional decision is sufficient and hasn't changed.

Having considered the complaint again in full, my findings remain broadly the same as set out in the provisional decision for the reasons given. But, there are some points in his response I'd like to address in order to clarify my findings.

The information provide by Revolut is insufficient

Much of Mr S's response relates to the evidence I've relied on. He's explained he doesn't believe Revolut's records are reliable and believes it should be able to provide more in-depth records of certain events and he knows this based on his personal expertise. I accept Mr S feels strongly about this, but our service is an informal one. My decision in based on what I think is more likely, on balance, based on the evidence available. If Z believes a more in-depth investigation of this situation would be appropriate, it may wish to consider what action it might be able to take outside of the service.

With regards to my investigation, I'm satisfied the evidence Revolut has provided is sufficient. I'd also note that a large part of what Mr S believes Revolut should provide more evidence of is evidence the new device wasn't logged in when he says it was, and evidence the device wasn't logged out when he requested it was. But this is asking Revolut to prove a negative which I don't think is reasonable to expect.

Instead, I've looked at the records Revolut has of the activities that it's recorded did take place and balanced this evidence with Mr S's testimony. Based on this, for the reasons given in my provisional decision, I don't think it's more likely the new device was already logged in when Mr S first logged in and started his call with the scammers. Apart from the fact the security process hadn't been followed that would allow this to happen, if the scammers had been able to add a device without any input from Mr S, it's not clear why they then would've required a further log in email to be sent, or why they would've needed to persuade Mr S to send it to them to allow the new device to log into the account. Any contact with Mr S increased the risk of scam being uncovered before any money was removed from the account. So it's not clear why this would've happened if it hadn't been necessary.

Whilst Mr S has said Revolut's systems must've been 'hacked' and that's how scammers obtained Z's log in details, I don't consider this the more likely scenario here. If scammers had been able to access Revolut's account to the extent they were able to gain full access to customers' accounts and log in details, again, it's not clear why they would need to contact the customers to discuss this. But, even if they somehow had been able to obtain Z's log in details without Mr S's input, they ultimately accessed the account and removed the funds because Mr S provided the log in email and two OTPs that allowed the scammers to use the account.

Overall, based on the evidence I've seen, I think it's more likely than not Mr S provided scammers with the details outlined in my provisional decision for the reasons given.

The email evidence I've relied on is incorrect

In my provisional decision, the table of events I provided said the new device log in attempt email sent to the registered email address was sent at 14:31. Mr S has the new device email was sent at 14:43. I accept what Mr S has said about this and I've amended the sequence of events and the table above to reflect this.

Whilst the records provided by Revolut start from 14:31 which Mr S has said the scam call started and he logged into Z's account, it has provided records which show the verification email was sent at 14:43 and was used at 14:49. Mr S has confirmed this when the new device email was received and then forwarded by him.

So I accept the new device log in attempt email was sent at 14:43, and not 14:31 as I'd mistakenly inferred. But I don't think this materially affects the outcome. Mr S has confirmed he did receive a log in email and he did send this to scammers which allowed them to

access the account, so this isn't in dispute. The difference of 12 minutes in when the email was received by him doesn't change my findings on this point.

And whilst Mr S has said he feels this proves that for around 13 minutes (between when the call with scammers started at 14:30 and the email was received at 14:43) he was spending time verifying the plausibility of having to forward the email to scammers which proves he was acting with a reasonable amount of care, I don't agree.

As I've highlighted in the provisional decision, Mr S has said when he was asked to forward this email he could see the domain name in the email address the scammers were asking him to use differed from Revolut's official domain name. He's said that upon questioning this they sent a text message to prove he was speaking to Revolut which he's said he could also see was different to usual Revolut contact and was aware Revolut's number could be 'spoofed'. He hasn't explained what happened after noticing these issues that persuaded him to forward an email allowing a new device to log in to Z's account. Especially given he's said he thought the new device listed in the email was already logged into his account and knew it belonged to scammers.

Mr S has also provided a copy of the new device log in email he received and says it doesn't contain the information I'd quoted in my provisional decision. It doesn't include any of the following:

> *"We got your login request. Before you confirm, take a moment to read the information below:*
>
> ***Before you click…***
>
> - *Did you make this request? If in doubt,* ***do not click below****. If someone is asking you to forward this email,* ***do not send it*** *to anyone…"*

He's said that Revolut has deliberately misled the service in providing this email. The email provided by Revolut is addressed to Mr S and contains the information above. So it appears it has been sent to Mr S at some point. However, I accept this isn't the new device log in email he received at 14:43 on 20 February 2024 and accept the email he's provided was the one he received. The email he's confirmed he received said:

> *"To confirm login, click the 'Confirm' button below*
> ***When:*** *20 February 2024*
> ***Where:*** *United Kingdom, [City], [Postcode] (Based on IP)*
> ***Device:*** *[New device]*
> ***IP:****…*
> ***Security information***
> - *This confirmation will only be valid for 10 minutes*
> - *If this wasn't you, change your passcode (mobile) and password (web), then contact us immediately…"*

It's clear this email was sent on the date the scammers accessed the account from the new device and it refers to the new device in the email. So I'm satisfied this is the email Mr S likely received and I've considered everything again in light of this information. But again, I don't think this materially changes the outcome here. Whilst the email Mr S actually received didn't contain the warning not to forward it, even without the warning, I don't think Mr S was acting with a reasonable amount of care in sending it to the scammers.

Given the content of the email, I think a reasonable person would understand that this type of email is a security measure and that it can be used to log the named device into the

account. The email clearly states what device was trying to log into the account and Mr S has told us he knew this device belonged to scammers. It also tells the recipient to contact Revolut immediately if they hadn't attempted a log in, which Mr S knew he hadn't. And whilst he's said he thought he was already talking to Revolut, the information in the email would've contradicted whatever he was being told by scammers.

So it's not clear why Mr S would forward a log in email to a third party which allowed a device he was aware belonged to scammers to log into Z's account. Especially when he already had suspicions about who he was sending it to. Mr S has said he didn't see the harm given he thought the device was already logged into the account. For the reasons given I don't think the new device likely was already logged in. But even so, I don't think Mr S has been able to explain what plausible or reasonable explanation he'd been given as to why allowing a scammer to log back into Z's account would allow Revolut to prevent scammers accessing the account.

I think Mr S reasonably should've recognised sending the email to a third party was a significant risk. For the reasons given in the provisional decision, and again above, I don't think I've seen sufficient evidence the scammers' story had enough credibility or plausibility from the outset to explain why Mr S reasonably believed Revolut would legitimately be asking Mr S to send it this email as well as the OTPs he provided. I'm also not persuaded it was reasonable for him to do so given his clear suspicions and the lack of explanation as to what allayed these suspicions.

In forwarding this new device log in email, even without any written warning not to, in addition to the other security information likely provided, I don't think Mr S was acting with a reasonable amount of care.

Mr S has also stated that the virtual card was not created at 15:06, but before the log in email was sent at 14:43. Based on the evidence I've seen I'm satisfied it was likely created at 15:06, after the new device had been logged into the account.

I've considered this case again, taking into account the additional information from Mr S and changing details in what happened where relevant. Having done so I think Mr S likely provided Z's online log in details to scammers, forwarded an email that allowed them to add a new device and provided OTPs that allowed them to make payments. I think in providing this information to scammers Mr S hasn't taken all reasonable steps to keep safe Z's individual security credentials relating to a payment instrument or an account information service. Because of this I think Revolut is acting fairly in holding Z partially liable for its loss. I do remain of the view Revolut is partially responsible for the reasons outlined in my provisional decision.

Putting things right

- Revolut should reimburse Z 50% of the payment from 'Payment 4' onwards (£3,347)
- It should apply 8% simple interest to this amount from the date the payments were made until the date of settlement
- It should reimburse a further £39 that likely could've been recovered from the receiving bank had it acted immediately when the scam was reported
- It should apply 8% simple interest to this amount from the date the payments were made until the date of settlement

My final decision

I uphold this complaint in part and direct Revolut Ltd to pay the settlement outlined above. Under the rules of the Financial Ombudsman Service, I'm required to ask Z to accept or reject my decision before 19 February 2026.

Faye Brownhill

Ombudsman