DRN-5356892

The complaint

Mr E complains that Revolut Ltd won't refund money he lost when he fell victim to an employment scam.

Mr E is being represented by a claims management company in this complaint.

What happened

The full details of this complaint are well-known to both parties and have been previously set out by the investigator. Briefly, Mr E fell victim to an employment scam in the beginning of 2023. He was contacted by a recruiter (the scammer) through a popular instant messaging service and offered an online part-time job which involved completing product orders and increasing sales for merchants on an online marketplace in return for an income.

Mr E followed the scammer's instructions and set up a 'work account'. He understood that occasionally he needed to top up his account in cryptocurrency to complete some of the orders. He purchased cryptocurrency from a cryptocurrency platform using his Revolut card before sending it to a cryptocurrency wallet as instructed. At the time Mr E believed he was topping up his work account as the balance went up accordingly. However, unbeknownst to him, he was sending the cryptocurrency to wallets in the scammer's control.

Mr E made the following disputed payments using his Revolut debit card –

	Date	**Amount**
Payment 1	9 February 09:20	£100
Payment 2	17 February *11:55*	£160
Payment 3	21 February *09:43*	£950
Payment 4	28 February *20:51*	£100
Payment 5	8 March *12:20*	£60
Payment 6	8 March *14:19*	£100
Payment 7	8 March *14:33*	£300
Payment 8	8 March 14:48	£100
Payment 9	8 March *15:00*	£400
Payment 10	8 March *15:13*	£1,000
Payment 11	8 March *15:25*	£1,500
Payment 12	8 March *15:40*	£2,000
Payment 13	8 March *15:55*	£5,000
Payment 14	8 March *18:19*	£4,000
Payment 15	22 March *09:27*	£300*
Payment 16	23 March *17:02*	£200*
Payment 17	24 March *16:14*	£500*
Payment 18	26 March *08:07*	£150*
*disputed after complaint was referred to our service		

There were payments to the cryptocurrency platform before and after the above transactions, but Mr E has confirmed that they're not linked to the scam.

It was only when he was repeatedly asked to pay tax on his income before he could withdraw it that Mr E realised he'd fallen victim to a scam. He complained after Revolut refused to refund his loss. The matter was subsequently referred to our service.

Our investigator thought that a suspicious pattern began to emerge when Mr E attempted to make Payment 12 (see above table). They concluded that Revolut ought to have provided a warning about cryptocurrency scams, given the transactions were identifiably cryptocurrency related. The investigator also thought that by the time of Payment 13, Revolut should have gone beyond the provision of an automated scam warning and should have discussed the transaction with Mr E. Had it done so, the investigator was satisfied on balance that the scam would have unravelled, and Mr E's losses prevented.

The investigator recommended Revolut to refund Payments 12-14 (along with interest) but with a 50% deduction for contributory negligence on Mr E's part. Payments 15-18 weren't included in the investigator's consideration or recommendation as they had not been disputed or complained about at that stage.

Mr E accepted the investigator's recommendations, but Revolut didn't. In its appeal, it said the fraudulent activity didn't occur on its platform. Revolut also said that it doesn't owe a duty to prevent fraud or scams; and that it is bound by contract, applicable regulations, and the common law to execute valid payment instructions.

I issued my provisional decision last month. I gave reasons for why I intended upholding the complaint in part and making a different redress award. I said –

> *"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 Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.*
>
> *And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.*
>
> *In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:*
>
> - *The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.*
>
> - *At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.*

In this case, the terms of Revolut's contract with Mr E modified the starting position described in Philipp, 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 20).

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 (FCA)'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'm 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. In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I'm 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.

While 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 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, at the time of these payment, 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'm 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;*

[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_/

- *providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.*

For example, it is my understanding that in February 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I'm 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)[2].*

- *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 don't 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 October 2017, BSI Code[3], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).*

- *Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being*

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- *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, as indeed Revolut does in practice (see above).*

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 February 2023 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 (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.*

While I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in February 2023, Revolut should in any event have taken these steps.

<u>Should Revolut have recognised that Mr E was at risk of financial harm from fraud?</u>

It isn't in dispute that Mr E has fallen victim to a cruel scam here, nor that he authorised the card payments he made to the cryptocurrency platform (from where that cryptocurrency was subsequently transferred to the scammer).

I'm aware that cryptocurrency platforms generally stipulate that the card used to purchase cryptocurrency on their platform must be held in the name of the account

holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Mr E's name.

By February 2023, when these transactions happened, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[4]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service).

However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I'm satisfied that by the end of 2022, prior to the payments Mr E made in February 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact that the payments in this case were going to an account held in Mr E's own name should have led Revolut to believe there wasn't a risk of fraud.

So, I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr E might be at a heightened risk of fraud that merited its intervention.

Like the investigator, I don't think Revolut should reasonably have suspected that Payments 1-11, which were relatively low in value and spread across days, could be

---

[4] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

part of a scam. As I've also mentioned, Mr E's account activity shows previous payments to the same merchant.

But by the time Mr E attempted Payment 12, a pattern of increased cryptocurrency related spending in one day began to emerge. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led it to consider that Mr E was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Mr E?

Revolut didn't provide any scam warnings when Mr E authorised Payment 12, or subsequent payments.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Mr E attempted to make Payment 12, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a written warning that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr E by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

But I'm not persuaded that such a warning would have resonated with Mr E. This is because he wasn't sending payments in connection with an investment. He understood he was using the cryptocurrency platform to deposit funds into his account to complete orders for his 'employer'. So, I'm not satisfied that the kind of warning I would have expected at that time – setting out the typical hallmarks of cryptocurrency investment scams – would have stopped Mr E from going ahead with that payment.

Payment 13 was made 15 minutes after Payment 12. The value had increased by more than double, and by this point Mr E had already sent over £5,000 in cryptocurrency related activity in one day. With Payment 13, that amount doubled to just over £10,000.

In the circumstances – an increasing pattern of cryptocurrency-related spending with a combined daily value of £10,000 – I think a proportionate response to the risk stemming from Payment 13 would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mr E's account. I think it should have done this by, for example, directing Mr E to its in-app chat to discuss the payment further.

<u>If Revolut had attempted to establish the circumstances surrounding Payment 13, would the scam have come to light and would that have prevented the losses Mr E suffered from that point onwards?</u>

I've reviewed the chat correspondence between Mr E and the scammer, and I've found nothing within those conversations that suggests he was asked, or agreed, to mislead Revolut or disregard any warnings provided. I've also seen no indication that Mr E expressed mistrust of Revolut or financial firms in general.

Had Revolut asked Mr E a series of questions to establish the nature of his cryptocurrency transactions, on balance, I'm satisfied that he would have explained he was purchasing cryptocurrency to make payments to complete the job tasks he had been assigned. And I think Revolut would have been able to identify that Mr E was falling victim to a job scam. This type of scam had been on the rise by the suggested trigger point.

Overall, I consider that attempts to establish the circumstances surrounding Payment 13 followed by a scam warning specific to the risk identified would have given Mr E cause for concern. And, on balance, I think he's likely to have decided not to go ahead with the payment because of that intervention.

<u>Is it fair and reasonable for Revolut to be held responsible for Mr E's loss?</u>

In reaching my decision about what is fair and reasonable, I've taken into account that Mr E purchased cryptocurrency which credited a cryptocurrency wallet held in his own name, rather than making a payment directly to the scammer. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost.

I've carefully considered Revolut's view that it shouldn't be held responsible for losses that occurred on a third-party site. But as I've set out in some detail above, I think that Revolut still should have recognised that Mr E might have been at risk of financial harm from fraud when he made Payment 13, and in those circumstances, it should have taken additional steps before processing it. If it had taken those steps, I'm satisfied that it would have limited the losses that Mr E suffered.

The fact that the money wasn't lost at the point Mr E used his Revolut card to purchase cryptocurrency doesn't alter that fact and I think Revolut can fairly be held responsible for Mr E's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against the firm that is the point of loss.

I've also considered that Mr E has only complained against Revolut. I accept that it's possible that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr E could instead, or in addition, have sought to complain against those firms. But Mr E has not chosen to do that and ultimately, I can't compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded that it would be fair to reduce Mr E's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; hasn't complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I've set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mr E's loss from Payments 13 onwards, subject to a deduction for his role in what happened which I'll consider below.

Should Mr E bear any responsibility for his losses?

There's a general principle in law that consumers must take responsibility for their decisions. I recognise that there were relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent earnings and tasks. Reading the chat correspondence with the scammer, I understand that Mr E also seems to have been part of an instant messaging group with other people who claimed to be making money. I can imagine this would have given some validation to the scheme.

But, at its heart, the scam appears to have been fairly implausible. While I haven't seen and heard everything that Mr E saw, the scammer's explanation for how the scheme worked is quite baffling and I think Mr E ought reasonably to have questioned whether the activity he was tasked with carrying out (which doesn't appear to be particularly time-consuming or difficult) could really be capable of generating the returns promised.

So, given the overall implausibility of the scam and Mr E's own apparent recognition of the risk of being continuously asked to make deposits to cover the advance payments, I think he ought to have realised that the scheme wasn't genuine before going ahead with Payment 13. In the circumstances, I consider he should bear some responsibility for his losses.

Also, I note from Mr E's recent submissions that he engaged the services of a recovery firm to recover the money he lost to the scam. He's highlighted a payment he made to the firm in the beginning of April 2023. But having reviewed his account transactions, I can see that Mr E first paid that firm on 23 March 2023. This indicates that he would have realised he'd been scammed at the very latest by that date. But he proceeded with Payments 16-18 after paying a fee to the firm to help recover his losses. Having carefully thought about this, I've concluded that it would be fair to reduce Revolut's liability to zero for the last three payments.

Weighing the fault that I've found on both sides, I think Mr E should bear equal liability for Payments 13-15, and 100% liability for Payments 16-18.

Could Revolut have done anything else to recover Mr E's money?

These were card payments to purchase cryptocurrency. We know Mr E sent that cryptocurrency on to the scammer. Revolut wouldn't have been able to recover the cryptocurrency from the cryptocurrency provider.

Additionally, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency was provided. In other words, the services paid for were rendered by the merchant.

So, I don't think Revolut should have done anything more to try and recover Mr E's money."

I gave both parties an opportunity to provide any further information or evidence they wanted me to consider before finalising my decision.

Mr E's representative replied and questioned why Revolut was only expected to warn against investment scams (in relation to Payment 12) when not all cryptocurrency scams are investment related. The representative has argued that had a more specific and sufficient warning about common cryptocurrency scams including employment scams been provided, it would have stopped Mr E from going ahead with Payment 12. Therefore, Payment 12 should be included in the refund, given Revolut did have an opportunity to intervene at the time.

Revolut asked for an extension to the deadline I gave to review my provisional decision. But the date it requested the extension till has now passed and we haven't heard back. I'm satisfied that Revolut has had sufficient opportunity to consider and reply to my provisional decision. So, it is now appropriate for me to proceed to 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 thank Mr E's representative for their comments which I've carefully considered. But they don't persuade me to depart from the findings I made in my provisional decision.

I understand the point the representative is trying to make – employment scams involving cryptocurrency did exist around the time of Mr E's payments. However, at the time of his payments, the most prevalent type of scams involving cryptocurrency were investment scams.

So, while I think Revolut ought to have recognised that cryptocurrency related payments carried a heightened risk and therefore it should have provided a written scam warning to Mr E, I would only expect such a warning to have covered the typical features of the most prevalent type of scams involving cryptocurrency. I wouldn't have expected it to have narrowed down the risk even further when these payments were made.

New legislation came into force later in 2023 and it put an obligation on firms to avoid foreseeable harm to customers – including fraud and scam detection. Given the increasing variation in cryptocurrency scams, I'd expect the firm to establish the actual scam risk associated with cryptocurrency payments before providing a better automated warning. But

given Mr E's payments were prior to the legislation coming into force, Revolut wasn't expected to take these additional steps.

So, having considered the representative's response, I see no reason to depart from my provisional findings.

Putting things right

To put things right for Mr E, Revolut Ltd needs to refund Payments 13-15 (inclusive) making a 50% deduction for contributory negligence.

Revolut Ltd also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of refund.

If it considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, Revolut should tell Mr E how much it's taken off. It should also provide a tax deduction certificate if Mr E asks for one, so that the tax can be reclaimed from HM Revenue & Customs if appropriate.

My final decision

For the reasons given, my final decision is that I uphold this complaint in part. I intend requiring Revolut Ltd to put things right for Mr E as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 2 April 2025.

Gagandeep Singh
Ombudsman