

## The complaint

Mr J complains that Revolut Ltd won't reimburse him after he fell victim to a job scam.

Mr J is professionally represented in bringing his complaint, but for ease of reading, I'll refer to all submissions as being made by Mr J directly.

## What happened

On 19 May 2025, I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any more evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

*Mr J has explained that he was looking for work to supplement his income and was contacted via instant messaging by an individual purporting to be a recruiter, but who was in fact a fraudster. Mr J was asked whether he was interested in a role 'driving data value' by boosting sales of items for a known luxury fashion retailer. Mr J confirmed his interest and was passed to another individual, who he understood worked for the company.*

*This fraudster told Mr J that the role takes around 30 minutes per day and he could earn £90 - £450 per day, plus a further £500 for working five consecutive days. Mr J was shown how to navigate the scam platform and 'boost sales' on a training platform. Mr J was also told that he needed a cryptocurrency wallet as some tasks required funds to be added to the system before they could be actioned. Mr J was told the firm doesn't 'deal with banks' because it doesn't 'want misunderstanding with clients'.*

*After completing his training, Mr J began working his tasks on his own account. However, the cost of tasks he was required to pay kept increasing and when he finally completed the tasks, he was told he needed to pay £5,000 to withdraw his funds. After paying this fee and still being unable to withdraw, as well as the fraudster's contact number keep changing, Mr J realised he'd fallen victim to a scam and contacted Revolut to raise a claim.*

*In total, Mr J made the following payments towards the scam:*

<b>Payment number</b>	<b>Date and time</b>	<b>Payment type</b>	<b>Value</b>
1	6 April 2023 15:31	Card payment to cryptocurrency	£60
2	7 April 2023 16:57	Card payment to cryptocurrency	£292.72
3	8 April 2023 18:06	Card payment to cryptocurrency	£730
4	8 April 2023 18:19	Card payment to cryptocurrency	£580
5	8 April 2023 18:32	Card payment to cryptocurrency	£2,205.56
6	8 April 2023 19:18	Bank transfer for peer to peer lending	£3,300
7	10 April 2023 20:27	Bank transfer for peer to peer lending	£3,300
8	11 April 2023 16:00	Card payment to cryptocurrency	£680
9	29 May 2023 19:02	Card payment to cryptocurrency	£70
10	27 June 2023 19:09	Card payment to cryptocurrency	£500
11	24 September 2023 14:52	Card payment to cryptocurrency	£5,000

*Revolut investigated Mr J's claim but declined to reimburse him. It said that its role was to execute the payments in accordance with regulatory obligations and that it has transaction monitoring and prevention systems in place, based on multiple factors.*

*Mr J remained unhappy and referred his complaint to our service. An investigator considered the complaint and upheld it in part. He said that when Mr J made payment five, six and seven, Revolut ought to have provided warnings related to scams, but based on the prevalence of job scams at the time, he didn't consider it reasonable to have expected such warnings to have covered this specific scam. He therefore didn't think anything Revolut would've provided at this time would've uncovered the scam. However, he said that by the time Mr J made payment 11, which was following the inception of the Financial Conduct Authority's Consumer Duty, Revolut ought to have done more to question the specific purpose of the payment Mr J was making, including questions relating to job scams and had it done so, he considered the scam would've been uncovered at this point.*

*However the investigator also considered Mr J should be held responsible in part for his losses, as he thought there were red flags Mr J ought to have identified about the job offer. He therefore considered Revolut should reimburse 50% of Mr J's losses for this final payment, plus interest.*

*Mr J disagreed with the investigator's view. He thought that Revolut ought to have implemented human intervention when he made payment six, based on the number of payments made that day, many of which were going to cryptocurrency, and the increase in payment values. He considers that had it done so, the scam would've been uncovered at this point. He also didn't think it was fair to apply a deduction for his part in the scam. He said he was unfamiliar with remote work and assumed requests were in line with this form of employment. He was also reassured by initial returns he received and the platform he was using, which seemed professional.*

*Revolut also disagreed with the investigators view. To summarise some of the points it raised, it said:*

- *This was a self-to-self payment, where Mr J owned and controlled the account where*

*the majority of his funds were sent. So the fraudulent activity (and therefore the scam) did not occur on Mr J's Revolut account.*

- *Revolut is an Electronic Money Institute (EMI), which is typically opened to facilitate payments of a specific purpose. Therefore these payments were not out of character, nor unexpected.*
- *Other bank's interventions should be considered in tandem with this complaint and whether Mr J acted negligently in disregarding other warnings.*
- *Revolut is bound to execute valid payment instructions except in very limited circumstances, such as where a customer has asked Revolut to act unlawfully. The Payment Services Regulations 2017 impose obligations on Revolut to execute transactions promptly.*
- *Revolut recognizes its obligations to counter the risk that it may be used to further financial crime, but that duty is not absolute and does not go as far as to require Revolut to detect and prevent all fraud.*

*As Mr J and Revolut disagreed with the investigator's view, the complaint has been referred to me for a final decision.*

### **What I've provisionally decided – and why**

*Having done so I'm also partially upholding Mr J's complaint, but from a slightly earlier point than previously decided on by the investigator, as well as removing the recommended interest payment. I've explained my reasoning in detail below.*

*In broad terms, the starting position at law is that an 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 J 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'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.*

*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 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 April 2023 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 EMI's like Revolut do in fact seek to take those steps, often by:*

- using algorithms to identify transactions presenting an increased risk of fraud;<sup>1</sup>*
- 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.*

*For example, it is my understanding that in April 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 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*

---

<sup>1</sup> 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/](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/)

*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 October 2017, BSI Code<sup>2</sup>, 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<sup>3</sup> 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 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.*

*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 April 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;*

---

<sup>2</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

<sup>3</sup> Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

- *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.*

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

*Should Revolut have recognised that Mr J was at risk of financial harm from fraud?*

*It isn't in dispute that Mr J has fallen victim to a cruel scam here, nor that he authorised the payments he made by card to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer) and the payment transfers he made.*

*Whilst I have set out in this decision the circumstances which led Mr J to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr J might be the victim of a scam.*

*I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange 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 payments would be credited to a cryptocurrency wallet held in Mr J's name.*

*By April 2023, when these transactions took place, 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<sup>4</sup>.*

*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*

---

<sup>4</sup> 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.

*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 am satisfied that by the end of 2022, prior to the payments Mr J made in April 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.*

*To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.*

*In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks. So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr J might be at a heightened risk of fraud that merited its intervention.*

*I think Revolut should have identified that all card payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). Mr J only opened his Revolut account a few months before he began making scam payments – and the account opening purpose provided was 'vaults' – so while Revolut didn't have much customer data to rely on when determining Mr J's typical account use, it was aware that the account use didn't match what Mr J initially stated was his intention for the account.*

*By the time Mr J made payment six towards the scam, this was the fourth payment made in just over an hour that day, the three prior payments being to cryptocurrency and the fourth being a further notable uplift in payment value to a new payee.*

*Given what Revolut knew about the first three payments made that day, followed by a fourth large payment in quick succession, I think the overall circumstances should have led Revolut to consider that Mr J was at a heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr J before this payment went ahead.*

*To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment transfer request (combined with the cryptocurrency payments which came before it) which ought to have prompted a warning.*

*What did Revolut do to warn Mr J and should it have done more in the circumstances?*

*Revolut has confirmed that when making the payment transfer, Mr J was asked for the purpose of the payment he was making and he selected 'something else'. Mr J was shown a set of screens explaining that the payment he was making may be a scam, and providing some general scam advice.*

*I've thought carefully about what I consider would have been a proportionate warning in light of the risk presented 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 primary duty to make payments promptly.*

*Taking that into account, when Mr J attempted to make scam payment six, knowing that Mr J had already made three payments prior to this in just over an hour, all to crypto, and that payment value was generally increasing, I think Revolut ought to have spoken to Mr J via its in-app chat to better understand the payments he was making. While I accept it had asked Mr J the payment purpose for this transfer already, Mr J had selected 'something else' and been provided with general scam advice – so I don't think Revolut had gone far enough in mitigating potential risks associated with this additional transfer, or understanding the payment purpose in light of the potential risk.*

*During an in-app chat, I would expect Revolut to ask open ended questions to better understand the payments Mr J was making – for example asking who the payee was from this transfer, why Mr J had made multiple cryptocurrency payments that day, whether the money he has paid remains in his wallet, and if not, where it has been sent, has he been advised to make these payments, and by whom.*

*If Revolut had discussed these payments during an in-app chat, would that have prevented losses incurred by Mr J?*

*I've thought carefully about whether such a discussion with Mr J would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have.*

*I've seen nothing from Mr J's conversations with the fraudster that would lead me to believe he would've been dishonest with Revolut in an in-app chat about what he was doing. As this scam was funded by payments made to Mr J via friends and family, I've also not seen any evidence that Mr J bypassed warnings relating to this scam from other banking providers.*

*Had Mr J explained that he was making payments to his employer via peer to peer lending and cryptocurrency in order to complete tasks and earn commission, I think Revolut would have identified that Mr J had fallen victim to a scam and provided advice on this, which would have stopped Mr J making further payments.*

*Mr J realised he had fallen victim himself when the fraudster's phone number kept changing and he had difficulties withdrawing his 'commission' – so I don't think Mr J was so 'under the spell' of the fraudster that relevant scam advice wouldn't have resonated with him and caused him to further research what he was doing. I'm therefore satisfied that a timely warning from Revolut would likely have caused the scam here to be revealed and prevent further losses for Mr J.*

*Is it fair and reasonable for Revolut to be held responsible for Mr J's loss?*

*In reaching my decision about what is fair and reasonable, I have taken into account that for the majority of scam payments made, Mr J purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So the funds passed through an additional financial institution before losses were incurred.*

*I have carefully considered Revolut's view that in a multi-stage fraud, liability for any losses incurred should be split between all financial institutions involved.*



*But as I've set out in some detail above, I think that Revolut still should have recognised that Mr J might have been at risk of financial harm from fraud when he made the first payment towards the scam, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mr J suffered. The fact that the money wasn't lost at the point it was transferred to Mr J's own cryptocurrency account does not alter that fact and I think Revolut can fairly be held responsible for Mr J'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 either the firm that is the origin of the funds or the point of loss.*

*I've also considered that Mr J has only complained against Revolut about the money he lost from this account. 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 J could instead, or in addition, have sought to complain against those firms. But Mr J has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.*

*I'm also not persuaded it would be fair to reduce Mr J's compensation in circumstances where Mr J has chosen to only complain about Revolut 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 have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr J's loss from the sixth successful payment he made to the scam (subject to a deduction for Mr J's own contribution which I will consider below).*

#### *Should Mr J bear any responsibility for his losses?*

*In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.*

*I recognise that there were aspects to this scam that would have appeared convincing. Mr J has provided evidence that the fraudster provided him with an employment platform, which Mr J has said appeared legitimate in appearance. He also received several credits as 'commission' which would've reinforced that this was a genuine opportunity, as well as being added to a group chat which appeared to show many other employees achieving expected results. I can understand why Mr J would be reassured by these factors that this was a legitimate role.*

*I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr J to be reduced, but I think it should.*

*While I accept the above would have gone some way to reassure Mr J, I still think there were elements of this scam that ought reasonably to not have been overlooked by Mr J, prior to proceeding. For example, Mr J believed he was working for a luxury retailer – I think Mr J ought to have had concerns as to why such a firm would ask employees to, in essence, create inaccurate sales data to drive item's popularity, by making it appear purchases were being made when they weren't. In addition, the entire premise of making payments to an employer is a complete inversion of the typical employee/employer relationship that I think would strike most as unusual. I also don't think the reasons provided as to why such payments should be made in cryptocurrency (as the retailer 'doesn't want misunderstanding with clients') was sufficient or entirely plausible.*

*Mr J also began working without any form of interview process or contract, and the wage he was being offered for a 30 minute, unskilled role is, I consider, unrealistic. While Mr J has explained he was unfamiliar with remote work, I don't think this negates having accepted the role on face value with minimal research first into what he was signing up for.*

*I've therefore concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr J because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.*

#### *Could Revolut have done anything else to recover Mr J's money?*

*I've also thought about whether Revolut could have done more to recover the funds after Mr J reported the fraud.*

*The majority of payments were made by card to a cryptocurrency provider and that cryptocurrency was sent on to the fraudsters. So, Revolut would not have been able to recover the funds.*

*In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the cryptocurrency platform performed its given role in providing cryptocurrency in return for payment in sterling.*

*For the payment transfers Mr J made, these similarly were made for peer to peer lending – so Mr J received cryptocurrency in return for the payments and the recipients of his funds weren't necessarily involved in the scam in question. I therefore don't think Revolut had any prospects of recovering these funds either.*

*Overall I think a fair outcome in this complaint is for Mr J and Revolut to be equally liable for all losses Mr J incurred from his Revolut account from payment six onwards in the scam and for Revolut to reimburse him 50% of these losses.*

*All credits Mr J received as a result of the scam were prior to the point I think Revolut ought to have intervened and uncovered the scam – so I do not think it would be fair or reasonable for these credits to be deducted from Mr J's reimbursement. However, Mr J has confirmed that payments he made towards the scam were funded by family and friends – the majority of which he still owes back. As Mr J himself has therefore not been out of pocket for his losses, I don't consider it would be fair to apply any interest on top of his refund from Revolut.*

#### ***My provisional decision***

*My provisional decision is that I uphold Mr J's complaint against Revolut Ltd in part. I'm minded to direct Revolut Ltd to reimburse Mr J:*

- *50% of losses incurred from payment six of the scam onwards (50% of £12,850), totalling £6,425.*

*Mr J agreed with my provisional outcome. Revolut confirmed it had nothing to add and would await the 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.*

*As neither Mr J nor Revolut has provided any additional points for consideration, my opinion*

on this complaint remains the same as that set out in the provisional decision above.

### **My final decision**

My final decision is that I uphold Mr J's complaint against Revolut Ltd in part. I direct Revolut Ltd to reimburse Mr J:

- 50% of losses incurred from payment six of the scam onwards (50% of £12,850), totalling £6,425.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr J to accept or reject my decision before 7 July 2025.

Kirsty Upton  
**Ombudsman**