

Complaint

Mr A complains that Revolut Ltd has refused to refund him the money he lost to a scam.

Background

In May 2023, Mr A was contacted via a social messaging platform and offered what he believed to be a part-time job. Unfortunately, this wasn't a genuine job but a scam.

He was told that he would be asked to complete tasks on an online platform on behalf of the employer and that he would earn commission for each completed task. He was given a fairly opaque explanation as to the purpose of the work. The scammers explained it in the following terms:

"Our position is data generator, we need to help merchant's app on [platform] to generate real traffic, joint platform's AI system to generate good reviews for the app, and finally complete the process of optimizing the app."

Mr A conducted a brief search on the purported employer and concluded, mistakenly, that the opportunity appeared legitimate. With hindsight, it appears that the fraudsters had chosen to imitate the name and corporate styling of another genuine company.

The fraudsters went on to fabricate reasons that Mr A needed to make payments to complete tasks. He made these payments thinking that he would get that money back once he received the commission payments he believed he'd earned. He was directed to use his Revolut account to make card payments to an account on a third-party cryptocurrency platform ("B"). Once transferred, the funds were converted into cryptocurrency and moved to an e-wallet controlled by the fraudsters.

He used his Revolut account to make the following payments:

#	Date	Value
1	29-May-23	£160
2	01-Jun-23	£224.85
3	01-Jun-23	£670
4	01-Jun-23	€ 1,640.76
5	01-Jun-23	€ 2,606.65
6	01-Jun-23	€ 1,155
7	01-Jun-23	€ 696
8	01-Jun-23	£250
9	02-Jun-23	€ 1,247.93
10	02-Jun-23	€ 4,796
11	02-Jun-23	€ 1,887.77
12	02-Jun-23	€ 2,900
13	02-Jun-23	€ 500

14	02-Jun-23	£1,250.14
15	02-Jun-23	£359
16	03-Jun-23	€ 4,400
17	06-Jun-23	€ 90
18	06-Jun-23	€ 70
19	11-Jun-23	€ 90
20	11-Jun-23	£17
21	12-Jun-23	£240
22	12-Jun-23	£434.25
23	13-Jun-23	£25.06
24	17-Jun-23	£2,455.65
25	19-Jun-23	£47.41
26	20-Jun-23	£89.84
27	21-Jun-23	£172.04
28	05-Jul-23	£15
29	06-Jul-23	£123.53
30	06-Jul-23	£112.70
31	06-Jul-23	£41.07
32	08-Jul-23	£16.31
33	08-Jul-23	£61.14

Once he realised that he'd fallen victim to a scam, he notified Revolut. It didn't agree to reimburse his losses. It said it didn't treat the payments as suspicious because Mr A had made payments to B in the past and he'd told it that purchasing cryptocurrency was one of his reasons for opening the account. It also said that it didn't think Mr A had done adequate due diligence before agreeing to go ahead with the payments.

Mr A wasn't happy with the response from Revolut and so he referred his complaint to this service. It was reviewed by an Investigator, who upheld it in part. The Investigator concluded that Revolut should have intervened on 2 June 2023 when Mr A made a €4,796 payment – payment 10 in the table above. He found that the pattern of transactions by that date ought to have raised concerns about the risk of fraud. Revolut disagreed, arguing that the payments were consistent with Mr A's stated account purposes and historic pattern of use. They also noted that they were made to an account in his own name, and so no loss had occurred at the point Mr A used his Revolut account to transfer funds.

As Revolut disagreed with the Investigator's opinion, the complaint has been passed to me to consider and come to a final decision.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

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 customer'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 A 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 must also 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 June 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or undertaken additional checks, before processing payments in some circumstances.

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

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

For example, it is my understanding that in June 2023, Revolut, where 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 function).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with “*due skill, care and diligence*” (FCA Principle for Businesses 2), “*integrity*” (FCA Principle for Businesses 1) and a firm “*must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems*” (FCA Principle for Businesses 3)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 “*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 Code³, 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

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/>

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”

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.

- 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 June 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 undertaken 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 June 2023, Revolut should in any event have taken these steps.

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

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 the payment identified by the Investigator would be credited to an e-wallet held in Mr A's name.

By June 2023, when this transaction 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. 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 am satisfied that by the end of 2022, prior to the payments Mr A made in June 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.

The Investigator said that Revolut should've intervened at payment 10. I'd agree with his conclusion on that. Mr A was making frequent card payments of a significant value to a payee with a known associated fraud risk. The day before, he transferred over €6,000 in four separate transactions. The aggregated value of those transactions ought to have been cause for concern. Nonetheless, I'm mindful of the fact that Mr A had made payments in the past to B, and he had told Revolut that cryptocurrency was one of the reasons he opened up his account. On balance, I wouldn't have expected Revolut to intervene at that point.

However, Mr A's rapid spending continued apace the following day in which he transferred over €11,000 in five separate transactions. One of those payments was payment 10 - the €4,796 one mentioned above. There was a clear pattern here that suggested the risk of one of a handful of different potential scam types. Revolut should've been concerned about that and shouldn't have processed that payment without taking some steps to warn Mr A about the risks of proceeding.

I've thought carefully about what a proportionate response 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 the risk was sufficiently clear that this required a human intervention. The payment should've been paused, and Mr A directed to interact with an employee of Revolut via the chat function in its app. There is no evidence that Mr A was instructed to mislead Revolut if questioned. The bank from which he made payments to his Revolut account has confirmed that it didn't query them or provide him with any warning, so I

can't draw any conclusions from that as to how he'd have responded if an intervention had taken place. On balance, I find it likely that he would have been forthcoming about the nature of the payments. With appropriate questioning, a Revolut employee could have identified that Mr A was engaging with fraudsters.

I recognise that this was an emerging scam type at the point Mr A made his payments. While "job scams" may not have been a readily identifiable scam category, a discussion of the purported job would, in my view, have revealed its implausible nature. The explanation provided by the fraudsters was too vague, the requirement for Mr A to make payments to perform tasks inverted the typical employer-employee relationship and the fact that the "employer" expected to be paid in cryptocurrency made the proposal even more suspicious.

I think an employee of Revolut would've recognised that this opportunity was a dubious one. They could've warned Mr A about the risks of proceeding and recommended he conduct further checks. I'm not persuaded that there's a good reason to doubt whether he would have acted on such a warning and ceased further payments.

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

In reaching my decision about what is fair and reasonable, I have taken into account that this payment was made to an account in Mr A's own name and that, at the point the funds left his Revolut account, he hadn't experienced any financial loss. But as I've set out in some detail above, I think that Revolut still should have recognised that he might have been at risk of financial harm from fraud when he made that payment, and in those circumstances it should have intervened. If it had taken those steps, I am satisfied it would have prevented the losses he suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr A's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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 A 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 he could instead, or in addition, have sought to complain against those firms. But he's 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 his compensation in circumstances where: he has only complained about one respondent from which he is entitled to recover his losses in full; has not 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 have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr A's loss from the payment specified above (subject to a deduction for his own contribution which I will consider below).

Should Mr A bear any responsibility for his losses?

I've also considered whether it would be fair and reasonable for Mr A to be considered partially responsible for his own losses here. In doing so, I've taken into account what the law says about contributory negligence while keeping in mind that I need to decide this case based on what I consider to be fair and reasonable in all the circumstances.

Having done so, I'm satisfied that Mr A's actions contributed to his loss here. He accepted a job without formalities. While I wouldn't necessarily have expected Mr A to have signed a written document, there was no point at which the terms of his employment were explained to him, other than through the informal messages sent via the messaging platform. The fraudsters didn't provide him with a coherent explanation regarding the work or the reason he was being paid to do it. Furthermore, the arrangement was in contrast with the usual employer-employee dynamic in that Mr A was required to make payments to perform work rather than being paid to do so. These factors should have prompted Mr A to proceed more cautiously than he did.

I don't say any of this to downplay or diminish the fact that Mr A has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for him and the position he's found himself in. However, my role is limited to looking at the actions and inactions of Revolut and I'm satisfied that this is a fair way to resolve this complaint.

Final decision

For the reasons I've set out above, I uphold this complaint.

If Mr A accepts my final decision, Revolut Ltd should refund 50% of all of the payments he made in connection with the scam from payment 10 onwards (the 2nd June payment of €4,796). It should also add 8% simple interest per annum to those payments calculated to run from the dates the payments left his account until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 20 January 2025.

James Kimmitt
Ombudsman