

The complaint

Miss D complains Revolut didn't do enough to protect her when she fell victim to a job scam.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In early 2023 Miss D was looking for opportunities to earn extra money and had registered her CV with a number of recruitment agencies. In April 2023 Miss D received a call from someone purporting to be a representative from a recruitment agency ('the scammer'). Miss D said she was offered a position to work for an advertising agency, which I'll refer to as "BR". She was told the work involved *"optimizing apps and boosting them on various app stores"*. She would need to complete 40 tasks a day and would then receive commission payments.

The scammer directed Miss D to open an account with BR, and was directed to a platform where she could complete the work tasks. Miss D said the account had an opening balance, that had been pre-funded by BR, she used this balance to carry out tasks for a couple of days and saw her commission increase. When the initial balance was exhausted, the scammer advised Miss D to top it up herself. She was instructed to open accounts with Revolut and a crypto exchange, which I'll refer to as "B". Miss D then purchased crypto using B's peer to peer (P2P) exchange, before transferring the crypto to wallet addresses provided by the scammer. Miss D said she saw the funds credit the work platform.

In total, Miss D made two payments from her Revolut account – £2,311 on 25 May 2023 and £2,918 on 26 May 2023. Miss D had also made payments from accounts she held with other banks prior to 25 May 2023, but these do not form part of this complaint although provide further context to the complaint.

Miss D said she realised she'd been scammed when the price of tasks continued to increase and she was asked for further funds. She said she tried to contact the scammer but they stopped responding. She reported the matter to Revolut on 29 May 2023 and asked for help recovering the funds. Revolut didn't uphold her complaint stating that it was not liable for the authorised transactions. It noted that it had provided Miss D with scam warnings when she instructed the payments and it had made attempts to recover the funds when she reported the scam.

Unhappy with Revolut's response, Miss D referred her complaint to the Financial Ombudsman with the help of a professional representative. Our Investigator upheld the complaint. He noted that when making the second payment Miss D had selected she was transferring funds to a safe account. Our Investigator said that while Miss D was not in fact falling victim to a safe account scam, Revolut should have made further enquiries before releasing the payment. He concluded that had it done so the scam would have come to light and Miss D's loss could have been avoided. But he considered that Miss D should share responsibility for the loss as she hadn't taken reasonable care to protect herself even though aspects of the job scam ought to have given her serious cause for concern.

Miss D accepted our Investigator's opinion. Revolut disagreed, and set out the following points:

- The Financial Ombudsman had erred in law by suggesting Revolut owed a duty to its customers who had have been victims of scams;
- It does not owe a duty to prevent fraud or scams, but does have a contractual, regulatory and common law regulatory duty to execute valid payment instructions, which is set out in its terms and conditions;
- It has systems and controls in place to counter the risk of financial crime, but it does not have a duty to detect and prevent all fraud;
- The Supreme Court's judgement in Phillip v Barclays set out that a payment service provider need not assess the wisdom or potential for financial loss of a proposed transaction;
- It is not a signatory of the voluntary Contingent Reimbursement Model (CRM) code, and so those rules do not apply to it;
- Miss D acted with gross negligence as Revolut presented her with dynamic educational story messages that warned about the risks associated with the transfers that she negligently ignored. After being presented with the warnings Miss D selected "Pay Anyway" rather than selecting the more prominent option of "Cancel Payment".
- Miss D's payments were made to a crypto merchant (which I'll refer to as "N"). At the time of making the payments there were negative reviews of N that Miss D ought to have checked and realised it was a scam;
- There's evidence from the chats Miss D was having with the scammers that she was suspicious before she made payments, but that she went ahead with the payments anyway. It therefore questioned whether any intervention from Revolut would have made a difference to Miss D's decision making.

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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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 Miss D modified the starting position described in Philipp, by 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"*.

So Revolut was required by the implied terms of its contract with Miss D and the Payment Services Regulations to carry out her instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should, in May 2023, fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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;
- 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

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

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut’s obligation to monitor its customer’s accounts and scrutinise transactions.
- The October 2017, BSI Code, 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 crypto 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 crypto 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 crypto 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 May 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

- 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 crypto accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Revolut have recognised that Miss D was at a heightened risk of financial harm from fraud?

It isn't in dispute that Miss D has fallen victim to a cruel scam here, nor that she authorised the disputed payments she made because of the scam.

Whilst I have briefly set out the circumstances that led Miss D to make the payments, I'm aware that Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Miss D might be the victim of a scam.

As Miss D set the Revolut account up for the purposes of the scam, Revolut didn't have any knowledge of her usual account usage to be able to identify if the scam payments were out of character. But that's not to say it was unable to identify if the transactions highlighted that Miss D may be at risk of financial harm.

For the first payment on 25 May 2023, Revolut knew that Miss D had opened the account that day and had selected "*gain expose to financial assets*" as the reason for her opening the account. It also knew she was making a payment of £2,311 to a new payee, using funds she had recently loaded on the account from a third party bank account. It also knew her payment purpose was "cryptocurrency".

I am aware that Revolut accounts are often utilised for the purposes of purchasing crypto and given Miss D's selected account opening purpose I don't think Revolut ought to have been particularly concerned about Miss D's initial payment.

But when Miss D instructed the second payment on 26 May 2023, for £2,918, she selected that the payment purpose was "*Transfer to a Safe Account*".

While I would not necessarily have expected Revolut to have been particularly concerned about the value or destination of this payment, I think it ought to have been concerned that this payment could relate to a safe account scam, which Revolut would have been aware were (and continue to be) prevalent at the time.

What did Revolut do to warn Miss D?

Revolut has demonstrated that it did present Miss D with a series of educational story screens which warned her about the risks of safe account scams, it also asked her "*Are you being scammed?*" and advised that financial institutions wouldn't ask her to move money to a safe account, download software, access or view her device or ask her to ignore warnings.

In the circumstances, given the heightened risk of significant financial harm associated with safe account scams, I don't consider Revolut's intervention was proportionate to the risk identified.

While Miss D was not in fact falling victim to a safe account scam, Revolut would not have known this at the time. I consider it should therefore have made further enquiries with her before processing the payment to understand what the payment related to, and it shouldn't have let the payment through unless it was able to completely satisfy itself that the payment reason was selected in error.

Overall, I can't agree that the warning Revolut provided was proportionate to the risk the payment presented. While I accept that Revolut has attempted some steps to prevent harm from fraud, the warnings it provided were not impactful enough.

Having thought carefully about the risk the second payment presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Miss D's account. I think it should have done this by, for example, directing Miss D to its in-app chat to discuss the payment further.

If Revolut had attempted to establish the circumstances surrounding the payment, would the scam have come to light and Miss D's loss been prevented?

It's impossible to know for certain what would have happened had Revolut have intervened as I'd expect it to do, as that intervention never took place. So, I have had to consider all the circumstances, to determine what I think would most likely have happened.

Taking into account everything I know; I think it's most likely Miss D would have been honest in responding to Revolut's questions. I say this as I'm aware that Miss D did speak with another bank when making an earlier payment related to the scam she answered its questions honestly – revealing that she was transferring money to a crypto exchange.

Having carefully reviewed Miss D's interactions with the scammers, while it's clear Miss D had built up a close and trusting relationship with the scammer, I have seen no evidence that the scammer had sought to coach Miss D on how to interact with her bank or what answers she should give. This is the case even when Miss D informed the scammer her bank had stopped one of her earlier payments.

I have also considered the fact that Miss D selected what appears to be an inaccurate payment purpose, by selecting "*Transfer to a Safe Account*", when this wasn't what she was doing. When we asked Miss D why she selected this payment purpose she said she could not recall why she selected that option, but she was distressed and under emotional pressure to get her money back at the time. I have seen no evidence that Miss D was told by the scammer what to select as the payment purpose, and I can't say that she intentionally selected the wrong purpose to deceive or distract Revolut. Given that it was the first option in a list of payment purposes (none of which accurately matched what Miss D was doing), I think it was most likely selected for speed.

In view of this, had Revolut asked Miss D about the payment I think it's mostly likely she would have revealed that she was purchasing crypto. Had Revolut asked for more detail about the reason for the payment and what she was planning to do with the crypto, as I would have expected it to, I think Miss D would likely have revealed that she was making a payment as part of a job, and that she needed to make further payments to release commission she had earned. I consider that this ought to have been enough to put Revolut on notice that Miss D was likely falling victim to a job scam. It should then have provided her with a clear warning that highlighted the risks of a job scam. I think this would have resonated with Miss D, particularly as the evidence shows she had her own suspicions about the plausibility of the job at the outset. Given Miss D was worried about losing money, I think a clear, strong warning from Revolut would have been the tipping point to confirm her

suspensions. So, I think it's most likely she would have decided not to go ahead with the final payment, and this loss would have been prevented.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss D purchased crypto which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I have also taken into account that the money that funded the scam was transferred into Miss D's Revolut account from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss D might have been at risk of financial harm from fraud when she made the second payment, and in those circumstances it should have made further enquiries before processing her payment. If it had taken those steps, I am satisfied it would have prevented the losses Miss D suffered.

The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was initially transferred does not alter that fact and I think Revolut can fairly be held responsible for Miss D'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 Miss D 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 Miss D could instead, or in addition, have sought to complain against those firms. But Miss D has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm(s) (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 Miss D's loss from the second payment (subject to a deduction for Miss D's own contribution which I will consider below).

Should Miss D bear any responsibility for her losses?

I have thought carefully about whether Miss D should bear some responsibility for her loss by way of contributory negligence (which might justify a reduction in compensation). 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. Having done so, I consider that Miss D should bear equal responsibility for her loss.

When considering whether a consumer has contributed to their own loss, I must consider whether their actions showed a lack of care that goes beyond what we would expect from a reasonable person. I must also be satisfied that the lack of care directly contributed to the individual's losses.

I accept that this was a sophisticated and well-orchestrated scam. I can understand how certain aspects of the scam may have made the scheme appear legitimate – for example the existence of an online platform where Miss D could complete her tasks, and the fact the scammers cloned legitimate recruitment and digital marketing companies.

But I cannot ignore that there were also aspects of the scam that were highly implausible – for example the expected commission in comparison to the work completed (Miss D was told she could earn up to 500USDT commission a day plus 500USDT base salary every 5 days, but that the work would take an hour or two per day), the fact that Miss D would be paid in crypto, and that she needed to pay money to enable her to release her commission.

But most significantly, I note that Miss D had herself questioned the legitimacy of the scheme from the outset. In messages to the scammer while they were discussing the premise of the job, Miss D said *“Okay be honest, does this actually work?”*; *“I’m suspicious to be honest lol you have to be nowadays”* and *“That’s it? You just click and submit? Must be joking lol”*. But despite Miss D’s reasonable suspicions she took no steps to check if what she was doing was legitimate, which I think she could have done for example by researching the legitimacy of these types of jobs online or by making direct contact with the recruitment agency or marketing company the scammers were cloning. Had she done so the scam could have been uncovered.

I have also considered Revolut’s concern that there were scam warnings about N at the time Miss D made her payments. But while I have considered the negative information Revolut has highlighted, it seems from the circumstances of the case that Miss D was not dealing with N directly. Miss D has explained that she used B’s crypto exchange, and then purchased crypto via its P2P service, which credited her crypto wallet, and was then transferred to the scammer’s crypto wallet. As such, I do not consider Miss D ought to have reasonably conducted any research into N.

Having considered the overall circumstances of what happened, I’m not persuaded Miss D took reasonable care to protect herself from the risk of financial harm. I consider that a reasonable person would have had enough reason to question the legitimacy of what was going on and would ultimately not have made the payments.

As such, I think it is fair in the circumstances that Revolut and Miss D share equal responsibility for the loss she suffered on 26 May 2023.

Putting things right

As both Revolut and Miss D could have prevented the loss from the second payment, it is fair that Revolut should refund 50% of that payment. It should also add 8% interest to the payment to compensate Miss D for her loss of the use of that money ever since.

Your text here

My final decision

For the reasons I’ve explained, I uphold this complaint about Revolut Ltd and instruct it to pay Miss D:

- £1,459 (50% of the payment made on 26 May 2023), plus

- 8% simple interest per year on that amount from the date of payment to the date of settlement (less any tax properly deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 22 November 2024.

Lisa De Noronha
Ombudsman