

The complaint

Ms R is unhappy that Revolut Ltd won't refund money she lost as a result of a scam.

What happened

Ms R was the victim of a job scam involving the following payments from her newly opened Revolut account, that she generally topped up from another bank account:

Payment Number	Date	Description	Amount
n/a	24 September 2023	Declined transfer to an individual 'A'	(£34)
n/a	25 September 2023	Payment received from an individual 'A'	+£133.00
1	26 September 2023	Payment to an individual 'I'	£83.05
2	26 September 2023	Payment to an individual 'I'	£20.56
3	26 September 2023	Card payment to Simplex, a cryptocurrency exchange	£102.00
4	26 September 2023	Card payment to Simplex	£10.00
n/a	26 September 2023	Declined card payment to Simplex	(£95.00)
5	26 September 2023	Payment to an individual 'O'	£96.00
n/a	27 September 2023	Reverted incoming payment from an individual 'V'	(£531.97)
6	28 September 2023	Card payment to Mercuryo, a cryptocurrency exchange	£120.00
n/a	28 September 2023	Reverted incoming payment from an individual 'A'	(£493.20)
7	29 September 2023	Card payment to Simplex	£820.00
8	29 September 2023	Card payment to Simplex	£1,650.00
n/a	29 September 2023	Five declined card payments to Simplex	(£3,400.00)
9	30 September 2023	Payment to GOAT Finance, a cryptocurrency exchange	£3,600.00
10	1 October 2023	Payment to GOAT Finance	£1,500.00
n/a	1 October 2023	Declined payment to GOAT Finance	(£13,400.00)

In summary, the fraudster told Ms R that the job involved her increasing ratings and reviews for products by completing tasks on an online platform that appeared to be connected to a genuine marketing company. Some of these tasks required her to deposit her own money on the platform, which she'd get back along with her earnings when she'd completed a certain number of tasks.

To deposit her money on the platform, Ms R sent money to her newly opened Revolut account. From there, she sent it to a number of crypto exchanges where it was exchanged to USDT, a cryptocurrency. Finally, she sent her funds to a wallet address the fraudsters gave her, believing it deposited funds on the online platform.

Ms R said she realised she was being scammed when she was asked to pay more and more to complete the tasks and access her earnings.

Revolut intervened several times with the payments. Of note:

- It declined several payments to Simplex between 26 and 29 September 2023. When Ms R asked about this via its in-app chat, she was told it wasn't possible to proceed given the risky nature of these transactions.
- On 30 September 2023, Ms R's transaction for £3,600 to GOAT (payment 9) was paused and she was asked a series of automated questions – she answered she was paying friends and family for a job, and they provided the details for the payment face-to-face. Following this, she was directed to Revolut's in-app chat where an agent asked whether the friend or family needed the money urgently. When Ms R said no, she was asked to carefully consider the information provided and consider whether she'd like to proceed.
- On 1 October 2023, a transaction for £13,500 to GOAT was paused and Ms R was again routed to Revolut's in app chat where she was asked questions over several days. She told them she created the account to avoid fees abroad, and that this transaction was to pay her family who did work on her home. She said she bought USDT so she could send money internationally without hefty fees. She also said she wasn't buying a cryptocurrency as she didn't know USDT was one.
- Revolut also spoke with Ms R over the phone about this payment, where they asked further questions. In summary, she said that she was paying her dad's cousin for a job, and the best way was to buy USDT via GOAT to avoid fees. She added that she also purchased some for herself, to exchange into dollars or pounds.
- After the call, Revolut told her they remained concerned she was falling victim to a scam. So they'd be closing her account and returning her money to her HSBC account.

On 17 October 2023, Ms R reported some of the transactions as a scam to Revolut, but it's not clear how this was taken forward. On 28 November 2023, Ms R raised a complaint with Revolut, via her professional representatives, that it failed to protect her from the scam. Revolut didn't uphold this, as it didn't receive the requested information to investigate.

Unhappy with the response, Ms R brought her complaint to us to investigate. I issued my provisional findings, upholding the complaint in part. Revolut responded to say it had nothing further to add; Ms R accepted my findings.

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.

Given that neither side has added anything further in response to my provisional decision, I see no reason to change my mind. For completeness, I've included my provisional findings below.

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 Ms R 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*”.

In this respect, section 20 of the terms and conditions said:

“20. When we will refuse or delay a payment

We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:

- *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 Ms R and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority’s “Consumer Duty”, which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in September 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.

So, Revolut’s standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the

payment. And, I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But 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 September 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 EMIs like Revolut do 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 August 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and

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/

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 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 *“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 Code², 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).
- Since 31 July 2023, under the FCA’s Consumer Duty³, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *“consumers becoming victims to scams relating to their financial products for example, due to a firm’s inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers”*⁴.

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

³ Prior to the Consumer Duty, FCA regulated firms were required to “pay due regard to the interests of its customers and treat them fairly.” (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

⁴ The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency⁵ 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.
- 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 September 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 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 September 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Ms R was at risk of financial harm from fraud?

It's clear that Revolut did recognise Ms R was at risk of financial harm from fraud here – it stepped in to ask further questions when she attempted to make payment 9 – a £3,600

⁵ 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.

transfer to GOAT, a crypto exchange. So the question for me is whether that was an appropriate point to intervene.

Overall, I'm satisfied it was – and I don't think Revolut acted unreasonably in not stepping in sooner. That's taking into account that the earlier payments were relatively low in value, and they were going to various merchants and individuals (it seems that Ms R sometimes used peer-to-peer services to purchase USDT). In contrast, payment 9 was the third, increasingly larger payment that day to a crypto exchange, and it followed several declined payments. So I think Revolut has cause to be concerned by these circumstances.

What did Revolut do to protect Ms R from financial harm and what should it have done?

For Payment 9, Revolut asked Ms R a series of automated questions, followed by further questions from a Revolut agent using its in-app chat. Given the risk of financial harm, I think the method used – having a conversation to understand the circumstances of the payment – was appropriate.

Accordingly, I must decide whether that conversation happened in the way I'd fairly expect – by asking open and probing questions and providing relevant context to establish Ms R's risk that she was being scammed.

Here, Revolut initially asked some automated questions about the payment – that established she was paying a family member for a job, and she'd got the details from them face-to-face. Following this, one of Revolut's agents asked whether she was told they needed the money urgently. When she said no, they told her she could now decide whether she wanted to continue with the transfer.

I'm not satisfied this conversation ought to have reassured Revolut – and I'd have reasonably have expected it to have gone further in its questioning. For example, her answers don't adequately explain why she'd need a cryptocurrency exchange to pay a family member or how she got these details face-to-face. Or, what the previous smaller payments were for. Similarly, it doesn't answer why, if the payments weren't urgent, there was a flurry of payments (including a number of declined payments), and why she was so keen to resolve the issue.

It follows that while I consider Revolut's method of intervention appropriate, I don't think the conversation happened in the way I'd reasonably expect in the circumstances. Instead, it ought to have probed Ms R further to establish that all was well.

If Revolut had intervened in the way I've described, would that have prevented the losses Ms R suffered from payment 9?

To answer whether a better intervention would've made a difference, I have considered that when Ms R was questioned about a later attempted payment, she was unable to reassure Revolut that all was well. And I can see why – Ms R had a cover story, but it didn't stand up to scrutiny. She couldn't clearly answer why she'd be paying for work done by family using cryptocurrency or why she was buying some cryptocurrency for herself (indeed, she said she didn't realise USDT was a cryptocurrency). There were also questions about why she was so keen to complete the transactions, and why, if they were for what she'd stated, she'd make them over several payments.

It follows that, had Revolut probed more in its earlier conversation, I think it's likely the result would've been similar – that Revolut wouldn't have made the payment.

I've considered whether that would've prevented Ms R's losses or, whether she'd have

continued making payments towards the scam via some other means. In deciding this, I've noted that when her money was returned to HSBC after the last attempted transaction, her statements indicate the money remained there – and wasn't further spent as part of the scam. I'm also mindful that for earlier payments, when she'd given less money to the scam, Ms R may not have been so taken in and desperate to act for the chance of accessing her supposed earnings and what she'd already paid.

Of course, I can't say for certain what would have happened. But, based on the evidence I have, I find it likely that a better intervention, earlier on, would've unravelled the scam and prevented further losses, in the same way Revolut's later intervention did.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Ms R purchased cryptocurrency which seemingly 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 carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss. In reaching my decision, I have considered that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at a regulated financial business. But as I've set out above, I think that Revolut still should have recognised that Ms R might have been at risk of financial harm from fraud when they made payment 9, and in those circumstances Revolut should have made better enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Ms R 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 Ms R's own account does not alter that fact and I think Revolut can fairly be held responsible for Ms R'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 Ms R 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 Ms R could instead, or in addition, have sought to complain against those firms. But Ms R has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Ms R'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 (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 Ms R's loss from payment 9

(subject to a deduction for Ms R's own contribution which I will consider below).

Should Ms R bear any responsibility for their 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 can see why Ms R taken in by the scam – the fraudsters appeared to be connected to a genuine company; she'd access to her account through a dedicated online platform; she went through 'training'; and there was a separate 'customer service' as well as a WhatsApp group with other 'colleagues'.

I've noted from the limited conversation records between Ms R and the fraudster that she was alive to the possibility of a scam – she asked the question when they explained she'd have to send her own money. While I can see how she was reassured by the other features of the scam I've described above, I'm mindful that Ms R was asked to pay increasingly higher amounts (something that's not typical for a job), and had to go through complicated means to make these payments, by using several crypto exchanges. Not only this, she was asked to repeatedly lie about what those payments were for.

Taking this into account, I think Ms R ought reasonably to have become more sceptical about whether this was legitimate by the time she made payment 9. It follows that I've reduced the award by 50% to reflect her contributory negligence.

My final decision

For the reasons I've explained, I uphold Ms R's complaint in part. Revolut Ltd must pay Ms R:

- The total of her losses from payments 9 and 10 less 50% for her contributory negligence. I understand this to be £2,550.
- Pay 8% simple interest per year on this amount, from the dates of the payments to the date of settlement (less any tax lawfully deductible)

.Under the rules of the Financial Ombudsman Service, I'm required to ask Ms R to accept or reject my decision before 17 July 2025.

Emma Szkolar
Ombudsman