

## The complaint

Mrs B complains that Revolut Ltd won't refund money she lost to a scam.

## What happened

Mrs B fell victim to a fake job scam after she replied to an advert about a job opportunity on social media. She was contacted on a messaging app and told she would be paid for completing a number of tasks. She was advised that she would be paid in cryptocurrency but would be able to withdraw her earnings at any time. Mrs B was told to open an account with the company she believed she was working for, and could see her earnings on the platform. However, after completing some tasks she began to receive 'bonus' tasks which required her to pay in funds before she could earn any more profit. But as she was told any money she paid into the scheme would be returned to her, Mrs B agreed to make the necessary payments. Over around a week, Mrs B received several of these bonus tasks and so made a series of payments totalling over £2,700 to sellers of cryptocurrency and received cryptocurrency into her cryptocurrency account, before sending that to the fraudsters. As well as the successful payments, there were also various unsuccessful payments that Mrs B attempted during this period. I've set the payments out below.

	Date	Time	Payee	Amount (plus fees)
Payment 1	27/07/2023	11:50	Payee 1	£158.11
Payment 2	27/07/2023	12:27	Payee 1	£288.23
Failed payment	27/07/2023	13:12	Payee 2	£543.13
Failed payment	27/07/2023	13:25	Payee 3	£560.67
Payment 3	27/07/2023	15:29	Payee 4	£533
11 failed payments	27/07/2023	16:40 to 18:47	Payees 4, 5, 6, 7	Amounts between £500 and £969.60
Payment 4	27/07/2023	18:57	Payee 7	£500
7 failed payments	27/07/2023	19:00 to 19:37	Payee 7	£464.60 for each attempted payment
Payment 5	27/07/2023	19:42	Payee 7	£202
4 failed payments	27/07/2023	19:43 to 19:46	Payee 7	Amounts between £202 and £260.58
Payment 6	27/07/2023	19:47	Payee 7	£101
Payment 7	27/07/2023	19:47	Payee 7	£101
Payment 8	27/07/2023	20:14	Payee 7	£65.65
5 declined payments	01/08/2023	11:16 to 11:24	Payee 2	Amounts between £201.40 and £805.60
Payment 9	01/08/2023	11:29	Payee 8	£805.60

Mrs B was becoming increasingly concerned as the scam progressed and she had to pay increasingly large amounts to the scheme. When she made the final payment set out above and was told she'd still need to pay in more funds, she realised she had been scammed.

Mrs B told Revolut what had happened but it didn't consider it had any responsibility for Mrs B's loss. It said it had provided her with appropriate warnings but that Mrs B nonetheless decided to go ahead with the payments.

Our Investigator upheld the complaint in part. They thought that Revolut ought to have questioned Mrs B in more detail about the third payment she made to the scam. The investigator thought that, had that happened, the scam would likely have been stopped. So, the investigator said that Revolut should refund the money Mrs B had lost from this payment onwards, less a deduction of 50% in recognition of Mrs B's own contributory negligence.

Revolut disagreed, it said it did not have a duty to prevent scams. It also maintains that the payments were not unusual enough to have been flagged as suspicious, and that nonetheless Mrs B was given appropriate warnings, and directed to the in-app chat to discuss some of the payments, but was not honest about what the payments were for. So Revolut says that any further intervention on its part would not have uncovered the scam or prevented Mrs B from making further payments. As no agreement could be reached, the matter has been escalated to me to determine.

### **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 Mrs B 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 Mrs B and the Payment Services Regulations to carry out their 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<sup>1</sup>. 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 July 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;<sup>2</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.

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)<sup>3</sup>.

---

<sup>1</sup> The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

<sup>2</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/>

<sup>3</sup> 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

- 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>4</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).
- Since 31 July 2023, under the FCA’s Consumer Duty<sup>5</sup>, 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”*<sup>6</sup>. However, in this case, the majority of the payments Mrs B made to the scam were prior to the inception of the Consumer Duty, so it does not apply to all but the final payment she made to the scam.

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 July 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

---

of this complaint largely pre-date the Consumer Duty and so it does not apply to all but the last payment Mrs B made.

<sup>4</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

<sup>5</sup> 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.

<sup>6</sup> The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

### What did Revolut do to protect Mrs B, and what should it have done?

Mrs B's Revolut account was opened for the purposes of this scam, so there was no account history against which Revolut could compare new transactions. But nonetheless, it's clear that Revolut did have concerns about the payments Mrs B was making from an early stage. The first payment Mrs B made to the scam – for £158.11 – was flagged by Revolut and Mrs B was asked to select what the payment was for, she chose 'cryptocurrency', and then was shown some education screens with information about scams involving cryptocurrency. However, these warnings were fairly generic, and did not address any of the features of the particular scam Mrs B was falling victim to, so I can see why this warning did not have any impact on Mrs B's decision to make the payment. But at this early stage of the scam, and given the low amount of the payment, I don't think that any further intervention was warranted from Revolut.

However, I do consider that by the time of the third successful payment Mrs B made to the scam Revolut should have been on notice that something potentially untoward was going on, and so intervened further. I say this as by this stage Mrs B had made or attempted payments to four new payees in only a few hours, and Mrs B had indicated that at least one of these payments was for cryptocurrency, which Revolut would have understood to be an additional indicator that these payments could be a risk to Mrs B, given its knowledge of cryptocurrency scams by this time. Payment 3 was also preceded by two failed payments. I think this pattern of spending was unusual, and evidently Revolut also felt that on some level as it did directly intervene in Payment 3. Initially, it asked Mrs B what the payment was for, she chose 'something else' as the payment purpose, it then showed her some educational warning screens, which again did not contain any information particularly relevant to the scam. At this stage Revolut directed Mrs B to its in-app chat feature, so it could ask some questions about the payment she was making. But while I think it was right for Revolut to have stepped in at this point, given the points set out above, to try to establish the circumstances surrounding this payment, I don't consider that these questions went far enough to uncover what Mrs B was actually doing.

Revolut asked Mrs B questions around whether she'd been called by anyone claiming to work for a bank and telling her to move money to a safe account to protect it, or by a friend or family member saying they needed her to make a payment to help them. It also asked whether she'd been called unexpectedly by someone telling her to move her money, whether she had received any recent text messages or emails where she'd entered personal information, and whether she'd downloaded any remote access software like AnyDesk or TeamViewer. In addition, Revolut noted that no bank or institution should be guiding her on what to say in response to questions she was being asked.

But what Revolut failed to do, and what I think it should have done given the risk it had identified, is ask Mrs B what the payment was for or who she was paying. When asked to select a payment purpose for Payment 3 Mrs B had said it was for 'something else', so Revolut had no clear idea of why Mrs B was making this payment, and the questions it asked did not clear this up. Given its concerns, I'd have expected Revolut to have asked a series of simple questions in order to establish the risk the payment presented. And, once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Mrs B gave. By the end of July 2023 I'd have expected Revolut to be aware of the key features of this kind of scam, so I'd expect any such warning to have covered off its key features, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Mrs B wouldn't have done so here.

Mrs B had already identified that the first payment to the scam was for cryptocurrency, so I don't think she was trying to conceal this fact. I note that Mrs B selected various different reasons for the payments she was making, but I don't think this was as a result of any dishonesty, given that she appears to have been making payments to individuals for peer-to-peer cryptocurrency purchase I can see why it wouldn't have been entirely clear to her which payment purpose was most relevant. I think it is likely that if Revolut had asked Mrs B what the payment she was making was for she would have explained it was for crypto currency as part of a job promoting businesses online, and that she was making payments to unlock tasks she had to complete before she could access her profits. And given that this is not a standard way that one would expect a job to operate and matched the features of what was, by this point, a reasonably well-known scam, I think that would have been a clear red flag to Revolut that Mrs B was at risk of financial harm, and it would have been able to explain this risk to Mrs B.

I've read the instant message conversation between Mrs B and the fraudsters. That conversation suggests that she already had some concerns about the scheme from quite early on in the scam – she appears to have been concerned about being asked to pay individuals to buy cryptocurrency, and about repeatedly being assigned bonus tasks. And I think this indicates that it wouldn't have taken much persuasion (that a warning could have provided) to convince her that she was falling victim to a scam if Revolut had intervened at the time of Payment 3.

In deciding this I've also thought about whether any other financial business involved in the payments Mrs B made might have provided warnings that she should have taken notice of. But I understand that the bank she made payments to her Revolut account from to fund the scam payments did not intervene to question her about those payments or to provide any warnings.

Overall, I think that a warning provided by Revolut would have given the perspective Mrs B needed, reinforcing her own developing concerns and she would more likely than not have concluded that the scheme was not genuine. In those circumstances I think she's likely to have decided not to go ahead with Payment 3.

So, in summary, I consider that if Revolut had intervened more appropriately at the time of Payment 3 then it could have prevented Mrs B's loss from that point onwards.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs B transferred her funds to Revolut from her main bank account provider, before using the funds to buy cryptocurrency which was passed on to the scammer.

But as I've set out above, I think that Revolut still should have recognised that Mrs B might have been at risk of financial harm from fraud when she made the third successful payment to the scam, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mrs B suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred out of Mrs B's Revolut account does not alter that fact and I think Revolut can fairly be held responsible for Mrs B'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 Mrs B 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 Mrs B could instead, or in addition, have sought to complain against those firms. But Mrs B 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 Mrs B'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 Mrs B's loss from the third successful payment she made to the scam (subject to a deduction for Mrs B's own contribution which I will consider below).

#### *Should Mrs B bear any responsibility for her 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.

And, having thought carefully about this, I do think Mrs B could have done more to protect herself from this scam. While there were some convincing elements of the scam – such as being given access to a task platform which looked professional – I think she ought reasonably to have had concerns about the legitimacy of the job offered, once she became aware of the requirement to send funds before she could earn any profits. And it's clear from Mrs B's conversations with the scammer that this element of the scam had caused her concern, as did being asked to pay individuals to purchase cryptocurrency. I also think the returns offered did seem too good to be true given the work she thought she was doing. Mrs B says she thought she could make as much as £3,000 in 30 days, and while this is not an exceptionally large amount, given that she thought she would only be working for less than an hour a day, I think this should have given Mrs B pause for thought and so led to her looking more deeply into this job she was apparently being offered.

But it's clear from Mrs B's chat with the scammer that she had apparently asked for very little information about the person she was dealing with or the company she was supposedly working for, it wasn't until late in her conversation with the scammer, after she had already

made several payments, that she appears to have asked the scammers name and started to look more into the company she believed she was working for. Because of this, I think it would be fair and reasonable to make a 50% reduction in the award based on contributory negligence in the circumstances of this complaint.

I've also thought about whether Revolut could have done anything to recover the payments Mrs B made to the scam, But given that the payments were to third party cryptocurrency sellers, who had provided the service they'd been asked to provide – the sale of cryptocurrency – I don't consider that Revolut could have done anything to recover those funds once it had been advised of the scam.

### **Putting things right**

To resolve this complaint Revolut should:

- Refund to Mrs B 50% of her loss from Payment 3 to the scam onwards.
- Pay 8% interest on this refund from the date of each payment to the date of settlement.

### **My final decision**

I uphold this complaint. Revolut Ltd should put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 26 September 2024.

Sophie Mitchell  
**Ombudsman**