

The complaint

Miss G complains that Revolut Ltd didn't do enough to protect her from a scam and hasn't refunded her since she reported it.

What happened

I issued a provisional decision (PD) for this complaint on 6 March 2025. In it set out the background and my provisional findings. I've included a copy of the PD at the end of this final decision so it can be easily referred to.

As I've included that copy, I won't repeat the same detail here. Instead, I'll explain what's happened since the PD.

Revolut didn't respond and the deadline for doing so has now passed. So there's no more evidence or information from it for me to consider.

Miss G did respond, and she accepted my findings.

As only one party has responded, it's now necessary for me to issue my final decision.

What I've decided – and why

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

I set out my reasons for upholding the complaint in my PD and these can be found within the attached copy.

There's been no new evidence or information supplied that I need to consider. The only response to the PD was Miss G's acceptance.

That being the case, there is no reason for me to depart from my original findings or to provide additional reasoning.

Revolut will now need to pay the redress set out in the PD and now confirmed in this final decision.

Putting things right

Revolut must, on Miss G's confirmed acceptance:

- Reimburse Miss G £1,000, that being 50% of the loss it ought to have prevented; *and*
- Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

My final decision

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss G to accept or reject my decision before 18 April 2025.

My provisional decision – issued 6 March 2025

I've considered the relevant information about this complaint.

[I'm issuing a provisional decision here as my findings differ slightly from those of the investigator, as does the amount of redress to be paid.

The deadline for both parties to provide any further comments or evidence for me to consider is 20 March 2025. Unless the information changes my mind, my final decision is likely to be along the following lines.

If Revolut Ltd accepts my provisional decision, it should let me know. If Miss G also accepts, I may arrange for the complaint to be closed as resolved at this stage without a final decision.

The complaint

Miss G complains that Revolut Ltd didn't do enough to protect her from a scam and hasn't refunded her since she reported it.

What happened

Miss G says her friend recommended an investment opportunity to her, though her friend hadn't used it herself. Miss G went on to look into the opportunity, which was said to use AI to carry out trading through a broker.

Miss G signed up to the service through what she's described as a professional looking website. She was then contacted by someone from the brokerage. Whilst all appeared genuine, it was actually a scam.

The scammers told Miss G that she could expect to make between £1,000 to £2,000 per week if she invested £5,000 and she decided to proceed on that basis. The scammers instructed her to download AnyDesk so they could assist with account opening and making the investments. She was also told to open an account with Revolut and two other firms, which she went on to do. She was also required to open cryptocurrency wallets so that funds could be transferred to them, and then on to the scammers.

Miss G made one successful card payment of £1,000 to her cryptocurrency wallet on 2 August 2023, although this was later returned to her on 10 August 2023. There were then multiple attempts to send more money to the scammers, but Revolut kept declining them. There was then one successful payment (£863.01) to a cryptocurrency platform, followed by a further decline. Miss G later tried to send money to someone else's personal account (£2,000), but the payment was declined by Revolut. Miss G attempted that same payment two days later and it went through.

During this time Miss G had sent more money to the scammers through her other accounts, held elsewhere.

Miss G could see the performance of her trading through the fake website of the scammers. All appeared to be going well and Miss G was encouraged to invest more over time. But, all of a sudden, her trading balance dropped to zero and this made Miss G realise she'd been scammed. She reported what happened to Revolut and the other firms involved.

One of Miss G's other account providers refunded her loss from the account held with it. Another two didn't as the money had been moved from those accounts to others in Miss G's name, and Miss G accepted those outcomes. There is an outstanding complaint against one other firm, for which the investigation is ongoing.

As for Revolut, it said it wouldn't reimburse Miss G's loss to the scam. It said Miss G had authorised the payments and there had been no reason for it not to follow Miss G's instructions, as it was obligated to do. It also said it wouldn't be fair for it to repay transactions that had gone to accounts/cryptocurrency wallets in Miss G's own name.

Miss G brought her complaint to our service as she was unhappy with Revolut's response. One of our investigator's considered it and recommended it be upheld. She said the account activity had been unusual enough so as to say Revolut ought to have suspected Miss G was at risk of financial harm through fraud. In particular, she referenced the multiple declined payments, that there were transactions which were identifiably for the purchase of cryptocurrency, and that the payments to the personal account had some concerning characteristics too.

She went on to say that Revolut ought to have questioned Miss G about what was happening with those transactions and to have warned against cryptocurrency investment scams. She was persuaded that, had it done so, the scam would have been revealed and Miss G's losses avoided. She said Revolut ought then to be held accountable for Miss G's losses.

Our investigator did also consider Miss G's action and how reasonable they were throughout. Broadly speaking, she felt Miss G ought to have done more to protect herself and that the investment proposition sounded unrealistic from the outset, especially considering the returns that were apparently on offer. So she said Miss G and Revolut ought to share responsibility for the loss equally.

Miss G accepted the investigator's findings, but Revolut did not. In summary, it said:

- The payments were 'self-to-self', meaning they went to an account or wallet in Miss G's own name. It says the point of loss was then from that account, and it's that firm which should consider reimbursing Miss G; *and*
- We ought to consider whether any of Miss G's other account providers intervened in any of the payments she was making, and how this might affect the outcome of her complaint against Revolut.

What I've provisionally 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.

Having done so I intend to uphold the complaint, although my findings differ slightly to those of our investigator. I'll explain further.

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 G 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 G 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 immediately¹. 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 August 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

¹ 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).

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;²
- 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 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).

² 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/>

³ BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

- Since 31 July 2023, under the FCA's Consumer Duty⁴, 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"*⁵.
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in August 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.

Should Revolut have recognised that Miss G was at risk of financial harm from fraud?

Our investigator found that Revolut ought to have stepped in to question the payment of £863.01 to the cryptocurrency platform. That was because there had been seven declined payments to the same or similar platforms in the previous eight days, with no intervention from Revolut. She also noted the payment was identifiably going to a cryptocurrency exchange, which carried a higher risk of being scam related than other types of payment.

⁴ 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.

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

She also didn't think the payment purpose selected by Miss G – 'goods and services' – matched up with the actual merchant types, and that Revolut ought to have recognised that.

I agree that Revolut needed to step in here, and for broadly the same reasons as set out by our investigator. Though I do have some further comments on what that intervention ought to have looked like, which I'll come on to shortly.

There is also the £2,000 payment to consider. And I'm satisfied Revolut ought fairly and reasonably to have questioned this payment too. It followed the earlier unusual activity on the account, albeit it was carried out some time later. Since that activity already referenced, there had then been a series of declined account top-ups, further demonstrating unusual account usage.

Furthermore, Miss G selected 'safe account' as the payment purpose. This ought to have given Revolut significant cause for concern. A safe account scam is a very common scam type and one that Revolut ought to be very much aware of. It's why it appears as a possible payment purpose, so that warnings might be given, and interventions might take place. When this payment purpose is selected, it is a significant red flag that a customer is at risk. I appreciate Miss G was not actually falling victim to a safe account scam, but there's no way Revolut could have known that at the time.

It also ought to have questioned the second – and this time successful – attempt at making this payment. It was only two days later, and the circumstances of the payment and the account overall hadn't changed.

What did Revolut do to warn Miss G?

For the £863.01 payment, Revolut did flag it as bearing some scam risk and so asked for the payment purpose. When Miss G selected 'goods and services' it went on to show a series of screens warning against scams involving the purchase of goods and services, the context being that there might be fake goods or merchants being promoted as genuine.

I can see Revolut looked to question the £2,000 payment too, when it was first attempted. And ultimately the transaction was declined by Revolut. It seems more likely than not Revolut stepped in to question the payment because Miss G selected 'safe account' from the payment purpose list, and I've described above why that was a big risk indicator.

Once the 'safe account' payment purpose was selected Revolut asked two further questions, which Miss G responded to. I've set out the questions followed by Miss G's answers below:

- *Have you been told that you've been the victim of fraud and rushed into making this payment?*
 - **Yes**
- *Have you been asked to ignore scam warnings during the making the payment?*
 - **No**

Miss G was then directed to the in-app chat and without prompting typed 'transfer to a friend'. Revolut then responded to say, in summary, the attempted payment was pending so further checks could be carried out.

I can't see there was any further conversation about the payment. There were no further questions asked or answered. And the payment appears to have then been declined by Revolut.

Revolut asked Miss G for the payment purpose again when she tried the transaction two days later. This time she chose 'something else'. She was then given some generic warnings about scams.

What kind of warning should Revolut have provided?

I can see why our investigator didn't think the warning for the £863.01 payment went far enough. Those reasons have already been set out above, so I'll not repeat them here. Whilst I do agree there was a lot of unusual activity on the account, and the payment did bear some risk, I'm not persuaded Revolut needed to do more than it did here. The payment value was quite low, in general terms, and so I wouldn't have expected Revolut to be particularly concerned by it. An automated warning, such as the one it gave, was enough. And I don't think it ought to have been immediately concerned by the 'goods and services' payment purpose being selected when the payment and its characteristics are looked at holistically.

This is where my findings differ from those of our investigator. As I'm satisfied Revolut acted fairly and reasonably up to this point, in respect of warnings and interventions.

I do, however, agree with our investigator where she's said Revolut didn't act fairly and reasonably regarding what happened next. It didn't go far enough to intervene in the attempted and then successful payment of £2,000.

It clearly recognised there was a risk here, but then didn't really take any steps to address that risk. A conversation was started but went nowhere. There was no exploration of the payment purpose, and so Revolut never got to understand what was happening. It just cancelled the payment. That could arguably have been enough at the time, as it is a fact the £2,000 wasn't lost at that point.

But Miss G then attempted the exact same transaction just two days later. And all the previous account activity ought to have factored into Revolut's decision on what to do with that payment instruction. It ought to have been on alert that Miss G was at risk of financial harm through fraud, given her earlier indication of 'safe account' as a payment purpose, alongside the other activity on the account.

But I can't see that Revolut then took sufficient steps to satisfy itself Miss G wasn't at risk of financial harm from fraud. The warning it gave at this point wasn't a proportionate response to the identifiable risk that was then presenting. Revolut ought to have directed Miss G to the in-app chat again, this time properly engaging her in a conversation to ascertain the true purpose of the payment, to identify the risks more specifically, and then to have given tailored scam warnings.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss G suffered from the £2,000 payment?

The scam Miss G fell victim to is sadly all too common. And the features of this particular scam bore many of the hallmarks of a cryptocurrency investment scam. I wouldn't expect Miss G to know and recognise those hallmarks, but I do find it's fair and reasonable to say Revolut should.

Had Miss G been directed to the in-app chat and had a detailed conversation taken place, I'm persuaded the scam would have been revealed and the loss prevented. Whilst Miss G had selected what might be described as 'incorrect' payment purposes, given she didn't say she was investing or purchasing cryptocurrency, I don't believe that indicates Miss G wouldn't have said what she was doing if asked openly. I've seen no evidence to suggest she was being heavily coached by the scammer or told to lie to Revolut.

I've also been able to consider interactions Miss G had with her other account providers. When asked directly, she did tell the firm that intervened that she was sending the money to Revolut for onward payment toward an investment. And so it follows she would have said the same to Revolut when asked. That would have been enough for Revolut to have started down the path of identifying the common features of a cryptocurrency scam.

I've seen no evidence to support that Miss G wouldn't have heeded Revolut's warnings once those features had been identified, with a tailored warning then being delivered. That being the case, the loss of the £2,000 could have been avoided.

Revolut said in its response to the investigator's findings that we ought to take account of any interventions that might have happened with other firms. That was an odd comment for it to make given the investigator's findings very clearly addressed that point directly. She directly commented on what happened with the other firms connected to the scam and highlighted there were no interventions or warnings that had any impact on the outcome. My finding on the matter is the same. Whilst other businesses did conduct some light touch intervention, there was nothing that educated Miss G about, or warned her against, the scam she was caught up in.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss G appears to have sent money to a friend which was then used to purchase cryptocurrency. I'm unclear as to whether that money then credited an e-wallet held in her own name or if it was a wallet in her friend's name. But it appears the payment didn't go directly to the fraudsters. So, the money wasn't completely out of Miss G's control or influence when she sent it from Revolut. It took further steps before the money was lost to the fraudsters.

It is important to note though that Revolut has been wrong to continue to claim that all payments were self to self. It's evident they were not. But this doesn't have an impact on the outcome overall.

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 taken into account that the £2,000 payment was made to another financial and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out above, I think that Revolut still should have recognised that Miss G might have been at risk of financial harm from fraud when she made the £2,000 payment, 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 Miss G suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred on by Miss G does not alter that fact and I think Revolut can fairly be held responsible for Miss G'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 G 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 G could instead, or in addition, have sought to complain against those firms. But Miss G 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 Miss G'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 Miss G's loss of the £2,000 (subject to a deduction for Miss G's own contribution which I will consider below).

Should Miss G 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.

Like our investigator, I find it would be fair and reasonable for Miss G to share responsibility for her loss, even where it's been found Revolut was at fault. Miss G accepted this position from the investigator's findings, and nothing has changed in terms of the principles applied now the case has been passed to me.

But, for the sake of clarity, I don't find that Miss G acted reasonably throughout and that there were signs this was not a genuine opportunity from the start. In summary, the key points of consideration here are:

- The investment proposal was too good to be true from the outset, with Miss G being promised returns of £1,000 to £2,000 a week on a £5,000 investment. That is an incredibly large return in a very short space of time and so I find it ought to have been viewed with a great deal of scepticism;
- There were online reviews about the broker which identified it as a scam. But Miss G doesn't appear to have sought to check the legitimacy of the broker or to have sought out such reviews;
- Miss G was instructed to open several different accounts and with little explanation as to why.

I have taken into account that Miss G had access to a professional website, complete with her own account and a convincing looking trading platform. I can see why that would have lent apparent legitimacy to the proposed investment. But I find the concerning elements of what was being proposed outweigh the positives ones, and Miss G ought to have been more cautious about sending her money to an unknown party.

Putting things right

My proposed outcome will be for Revolut to, on Miss G's acceptance:

- Reimburse Miss G £1,000, that being 50% of the loss it ought to have prevented; *and*

- Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

My provisional decision

I intend to uphold this complaint against Revolut Ltd.

Ben Murray

Ombudsman