

The complaint

Miss H complains that Revolut Ltd is refusing to refund her the amount she lost as the result of a scam.

Miss H is being represented by a third party. To keep things simple, I will refer to Miss H throughout my decision.

What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Miss H received a message from a company I will call X. X offered Miss H a remote working job which involved completing multiple tasks before she would receive a commission.

Miss H was provided with training and access to X's platform where she had to make deposits via cryptocurrency to unlock tasks before she could complete them. Each time Miss H completed a task the amount required to unlock the next one increased.

The amount required to unlock the tasks continued to increase until they became unaffordable for Miss H. X told Miss H that the only way she could make a withdrawal from the platform would be to complete the set of tasks. As Miss H could not afford to make further payments she could not continue and later realised she had fallen victim to a scam.

Miss H made the following payments in relation to the scam:

Payment	Date	Payee	Payment Method	Amount
1	9 July 2023	Binance	Debit Card	£96.99
2	11 July 2023	Binance	Debit Card	£1,576.45
3	11 July 2023	Binance	Transfer	£3,364.52
	2 August 2023	Noble Trading PTY Ltd	Transfer - declined	£5,582.96
	2 August 2023	Noble Trading PTY Ltd	Transfer - declined	£5,582.96
4	2 August 2023	Noble Digital	Transfer	£5,582.96
5	8 August 2023	Binance	Debit Card	£80.67

Our Investigator considered Miss H's complaint and thought it should be upheld in part. Miss H and Revolut both disagreed.

In summary Miss H thought Revolut should have done more to protect her from being scammed and provided a stronger intervention earlier on. Miss H argues that had a proportionate intervention been provided early in the scam she would have taken notice and more of her loss could have been prevented. Miss H also argues that it is not reasonable to hold her partially responsible for her loss.

Revolut said in summary:

- The fraudulent activity did not take place on the Revolut platform, it was just an intermediary link between the consumer's own bank account and X. The payments from Miss H's Revolut account don't fit either the definition of an APP scam in the Dispute Resolution Rules ("DISP") or under the Lending Standards Board Contingent Reimbursement Model ("CRM Code") – of which it is not a signatory.
- the FOS appears to have decided as a matter of policy, that Revolut should be left "holding the baby" because, subsequent to the self-to-self transfer involving a Revolut account, customers have transferred funds to their own account with a third party. The FOS has concluded those third parties are outside its jurisdiction either because the relevant firm is not authorised, or because the relevant product is not regulated.

As an informal resolution could not be agreed this complaint has been passed to me to decide.

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 H 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 H 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 July - 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 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)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”.

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).

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_further_reduction_in_card_fraud_and_had_offers_from_banks/

³ 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 some of the circumstances of this complaint pre-date the Consumer Duty and so it does not apply to those.

- 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 customers' accounts and scrutinise transactions.
- The October 2017, BSI Code⁴, 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 Duty⁵, 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”⁶.
- 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 July - 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;

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

⁵ 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.

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

- from 31 July 2023, 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 H was at risk of financial harm from fraud?

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

Whilst I have set out in this decision the circumstances which led Miss H to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Miss H might be the victim of a scam.

The first two payments Miss H made in relation to the scam were clearly being made to a cryptocurrency exchange but given the relatively low value of the payments I don't think it was unreasonable that Revolut's fraud prevention systems were not triggered and that it did not intervene.

However, payment 3 was for a more significant value, and again it was clearly being made to a cryptocurrency exchange. Given the increased risk associated with this type of payment I think it should have caused Revolut to have concerns and it should have intervened and provided Miss H with a warning proportionate to that associated with the risk.

Considering the time payment 3 was made I think that a proportionate warning would have been for Revolut to provide a written warning that covered the risk of investing in cryptocurrency.

At the time Miss H was making payment 3 though, she was not investing in cryptocurrency, she was instead making payments in relation to a new job. So, I think it's unlikely such a warning would have raised any red flags with Miss H or uncovered the scam that was taking place.

When Miss H made payment 4 the value of the payment was much higher and not in keeping with how Miss H usually operated her account. With this in mind, I think Revolut should have had concerns that Miss H could have been at risk of financial harm and intervened.

What did Revolut do to warn Miss H and what should it have done?

From the information provided it doesn't appear that Revolut intervened when Miss H made any of the disputed payments.

As I have explained above, I think Revolut should have intervened when Miss H made payment 4. The payment was significantly higher in value, and Revolut had declined the

payment twice the same day for the reason of “suspicious activity”.

Given the risk associated with payment 4, and that Revolut had previously declined two payments for the same value to a similarly named payee on the same day, I think a proportionate intervention would have been for Revolut to have asked a series of questions about the payment Miss H was making in an attempt to narrow down the specific scam risk. Once that risk had been identified, Revolut should have provided a warning which covered off the key features of the scam risk identified. I think this warning should have included job scams.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss H suffered from payment 4?

I've thought carefully about whether a warning of the type I've described would have resonated with Miss H and prevented her from making payment 4. Having done so, I think it would. I'll explain why.

It's clear from the messages exchanged between Miss H and X that Miss H questioned the legitimacy of the job at times. As the scam Miss H was falling victim to had characteristics of common job scams and Miss H had no desire to lose her funds, I think it's most likely a warning tailored to the scam Miss H was experiencing would have been a red flag to her and it's likely she would have stopped making payments.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss H purchased cryptocurrency 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 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 final payment was made to another financial business (a cryptocurrency exchange) 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 H might have been at risk of financial harm from fraud when she made payment 4, 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 H 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 to Miss H's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss H'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 H 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 H could instead, or in addition, have

sought to complain against those firms. But Miss H 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 H'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 H's loss from payment 4 (subject to a deduction for consumer's own contribution which I will consider below).

Should Miss H 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.

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances, I do think it would be fair to reduce compensation by 50% on the basis that Miss H should share blame for what happened.

Miss H was contacted via a messaging service about a job opportunity. No formal interview was conducted, and she was required to make multiple payments in cryptocurrency before she could withdraw funds. I think this should have appeared unusual to Miss H and she should have been concerned.

I think it would have been reasonable for Miss H to carry out thorough due diligence before agreeing to part with significant amounts and had she done so it is likely she could also have prevented her loss.

Could Revolut have done anything to recover Miss H's money?

The payments Miss H made in relation to the scam were made to a cryptocurrency exchange and there is no dispute that Miss H received the cryptocurrency she purchased before forwarding it in relation to the scam.

As Miss H received the cryptocurrency Revolut would have no reasonable options available to it to recover the payments she made.

Putting things right

To put things right I require Revolut to:

- Refund 50% of the payments Miss H made into the scam from payment 4 onwards
- Add 8% simple interest per year to the amount it pays Miss H from the date of loss to the date the payment is made (less any lawfully deductible tax)

My final decision

I uphold this complaint and require Revolut Ltd to put things right by doing what I've outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss H to accept or reject my decision before 28 February 2025.

Terry Woodham
Ombudsman