

## **The complaint**

Ms H complains that Revolut Ltd (“Revolut”) won’t refund the money she lost as part of a scam.

## **What happened**

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

In 2021, Ms H saw an advert for company that purported to be a crypto investment firm that I will call B. Ms H completed an enquiry form and was contact by a representative of B.

Subsequently, Ms H made a series of transfers and card payments between October 2021 and June 2022 to an account that she held with a different provider and to crypto exchanges. These transactions totalled over £240,000.

Ms H realised that she had been scammed when her “trading account” showed that there was a zero balance in November 2022.

She made a complaint via a representative to Revolut and requested that the above transactions be refunded. It declined to do this.

One of our investigators looked into this matter and she thought that Revolut should have intervened during transaction 4 and had it done so, it would have prevented the loss Ms H suffered and that it should therefore refund all of the above payments. She did though say that there should be a deduction of 50% as she believed that Ms H was equally liable for her loss. Revolut did not agree and therefore this complaint has been passed to me to issue a 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.

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 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 Ms 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 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 2021 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>

---

<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/>

- 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 customers’ accounts and scrutinise transactions.
- The October 2017 BSI Code<sup>3</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. So I think 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).

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 2021 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

---

<sup>3</sup> BSI: PAS 17271: 2017 *“Protecting customers from financial harm as result of fraud or financial abuse”*

- 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;
- 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).

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

I don't think that payment 1-3 ought to have concerned Revolut. Ms H's account was not a new one and therefore Revolut did have a payment history to compare this transaction to. But the size of these transactions on their own were not sufficient to have prompted an intervention and I don't think that a pattern had emerged that ought to have concerned Revolut.

I do however think payment 4, ought to have warranted an intervention from Revolut. It represented 4 payments to a new payee in ever increasing amounts, in a relatively short space of time. The payment itself was £10,000 and was larger than the payments Ms H usually made.

Considering all of those factors together, I think that the payment carried an elevated risk of financial harm from fraud and I'd have expected Revolut to have provided a warning that was proportionate to the risk that the payment presented.

I've gone onto consider whether the warnings that Revolut did give were proportionate to the risk the payment presented. But I don't think they were. I'll explain why.

Revolut says it provided a warning to Ms H. The warning would have been displayed when Ms H was creating a new payee, it read:

"Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back"

When the first payment was made Revolut provided a general warning. But by payment 4 I don't think that this was sufficient.

**What kind of intervention should Revolut have provided?**

I've thought carefully about what a proportionate intervention in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine.

When Ms H attempted to make Payment 4, I think Revolut, in line with what I consider to have been good industry practice at the time, as well as what I consider to be fair and reasonable, ought to have asked about the purpose of the payment via a human intervention such as in its in app chat.

Ms H's case had many features that are common to this type of scam. Ms H had seen an advert for an unregulated investment company. She'd been given access to a trading platform and a broker and had made initial deposits which appeared to be growing in value. She was sending money in order to purchase crypto which she was going to send to B.

She was being offered guaranteed returns and a number of risk-free crypto trades. She had been asked to instal remote access software - which no legitimate trading company would ask someone to do. So I think Revolut would have been able to point out that what she was doing was likely a scam.

In addition, Ms H did not receive any cryptocurrency investment related specific warnings from Revolut or any of the banks from which the money originated – so there's no evidence she ignored a specific and tailored warning. There was a phone intervention between Ms H and her other bank, but no specific warning was given and Ms H did not, in my view, mislead the bank with the very limited questions that were asked. So I think that Ms H would have been honest with Revolut and this would have allowed it to provide a warning and Ms H would have acted on any specific crypto warning given.

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

In reaching my decision about what is fair and reasonable, I have taken into account that the funds sent to Revolut went came from accounts that Ms H held with other providers

But as I've set out in some detail above, I think that Revolut still should have recognised that Ms H might have been at risk of financial harm from fraud when she made payment 4, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses the consumer suffered. The fact that the money used to fund the scam came from elsewhere does not alter that fact and I think Revolut can fairly be held responsible for Ms 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 Ms H has only complained against Revolut in relation to the payments that were sent to the scammer. But. In these circumstances therefore I can only make an award against Revolut for the payments in question.

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

I'm also not persuaded it would be fair to reduce Ms 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 for all the payments that relate to the scam 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 H's loss from payment 4 - subject to a deduction for Ms H's own contribution, which I will address below.

### **Should Ms 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.

In this instance, when Ms H started sending money to the scammer there were no credible warnings about B online. So I don't think that any initial research into B would have made Ms H aware that B was not a legitimate company. I also accept that adverts such as the one that persuaded Ms H to invest with B can be realistic and persuasive. So I don't think that Ms H was negligent at the start of the scam.

That said, being offered risk free crypto trades for a fee is not realistic. I also note that Ms H was offered at one point a 50% matching bonus which really should have raised questions. The language used by the scammer was unprofessional. Additionally, I think being asked to install remote access software, which no legitimate trading company would ask to do, Should have been a red flag for Ms H.

So overall and having considered everything I think that Ms H did contribute to her own loss and given this I think that there should be a 50% reduction to the redress due.

I've considered whether Revolut could have recovered any of Ms H's payments. But given the timescales involved and that the funds were sent on from the account she sent them to as part of the scam, I don't think that there would be any funds to recover. In relation to the Contingent Reimbursement Model, it does not apply in this instance as Revolut are not part of that scheme.

In relation to the card payments, I don't think that a chargeback would have been successful due to the timescales involved and given that there is not enough evidence to show that the goods or service purchased i.e. the crypto currencies were not received.

### **Putting things right**

Because of the reasons given above, Revolut Ltd should do the following to put matters right.

- Refund the money Ms H lost during the scam from and including, transaction 4 minus any credit received. There should then be a deduction of 50%.
- It should also pay 8% simple interest, per year, on the above amounts, calculated from the date of each payment, to the date of settlement (less any lawfully deductible tax).

### **My final decision**

My decision is that I uphold this complaint in part and instruct Revolut Ltd to pay the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 31 March 2025.

Charlie Newton  
**Ombudsman**