

The complaint

Mrs P has complained that Revolut Ltd won't refund money she says she lost to a scam.

What happened

Mrs P says she saw an advertisement for an investment opportunity on a social networking platform and it piqued her interest. Mrs P was under the impression the investment was legitimate as it had been advertised on social media, 'endorsed' by a celebrity and had a very sophisticated website. She says she did research the company and found countless positive reviews. So, she left her details for someone at the 'company' to contact her. The scammer contacted Mrs P, provided assurances, and helped her set up her trading account. Mrs P says the scammer told her to open an account with Revolut due to banks disliking cryptocurrency.

Between 25 February 2023 and 16 March 2023 Mrs P says she sent £18,410 to two new payees linked to cryptocurrency. Mrs P says she instantly saw her money being deposited into her trading account, in her mind, reinforcing the fact the company was legitimate.

Mrs P says the scammer pressurised her to take out several loans and it wasn't until she received a letter from one of the loan companies outlining suspicious activity on her account that she discovered she had been scammed. She feels Revolut didn't do enough to protect her and if they had provided an effective warning it would have prevented her financial loss. Revolut looked into Mrs P's complaint, but it didn't think it had done anything wrong. Mrs P remained unhappy and referred her complaint to our service. Our investigator looked into the complaint and recommended it be partially upheld. However, Revolut disagreed and so the complaint has been passed to me to consider.

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 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 P modified the starting position described in *Philipp*, by – among other things – 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*” (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in February 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMIs like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;¹

¹ For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/

- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in February 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with “due skill, care and diligence” (FCA Principle for Businesses 2), “integrity” (FCA Principle for Businesses 1) and a firm “must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems” (FCA Principle for Businesses 3)².
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut’s obligation to monitor its customer’s accounts and scrutinise transactions.
- The October 2017, BSI 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).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might

² 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 of this complaint pre-date the Consumer Duty and so it does not apply.

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

become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So, it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in February 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;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in February 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mrs P was at risk of financial harm from fraud?

It isn't in dispute that Mrs P has fallen victim to a cruel scam here, nor that she authorised the payments she made. I am mindful that Revolut has suggested it did not know what the 'typical' account usage was for Mrs P because the account was infrequently used at that time, so, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mrs P might be the victim of a scam. However, by February 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams

involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by February 2023, when these payments took place, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud. However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs P made in February 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in February 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Mrs P's own name should have led Revolut to believe there wasn't a risk of fraud.

I think Revolut should have identified that payment one, of £5,000 sent on 24 February 2023, was going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). And while Mrs P used her Revolut account infrequently, the payment was larger than any previous transactions (from the statements provided). Having considered the size of the payments, where they were going to and what Revolut would have reasonably known about it at the time, I think that the circumstances should have led Revolut to consider that

Mrs P was at heightened risk of financial harm from fraud. So, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment and the fact the payment went to a cryptocurrency provider which ought to have prompted a warning.

What kind of warning should Revolut have provided?

Revolut has confirmed that no warnings were provided to Mrs P.

I've thought carefully about what a proportionate warning 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. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think it would have been proportionate at that time for Revolut to have issued Mrs P with a written warning tailored to crypto investment scams given how prevalent they had become by the end of 2022. The written warning should have covered off the key features of a cryptocurrency investment scam. As the information which would have been available to Revolut at that time, is that the transactions were of a certain value being sent to a crypto exchange. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency investment scams, without significantly losing impact.

If Revolut had provided a warning of the type described, would that have prevented the losses Mrs P suffered.

I have considered what I think is most likely to have happened if Revolut had provided such a warning. And in doing so, I am persuaded that on balance I think it is likely it would have prevented Mrs P making further payments. I will explain why.

Having reviewed the scam evidence provided, it's apparent, prior to Mrs P making payment one, she had some concerns. She says:

"Hi money due to be paid in tomorrow, thinking about it I'm not ok with it, I transfer £5k and end up with a £5k loan to repay! Think I'll cancel and just have my money please. This doesn't feel safe"

Therefore, I am persuaded, if Mrs P had been provided with a written warning, specific to cryptocurrency investment scams, in line with the one I have highlighted above, I am satisfied it would have resonated with her own circumstances. This accompanied by the fact Mrs P already had concerns (as highlighted above) prior to sending payment one, I am persuaded it would have prevented any further loss occurring.

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

In reaching my decision about what is fair and reasonable, I have taken into account that some of Mrs P's transactions credited an account held in her own name, rather than making a payment directly to the scammers. 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 scammers.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs P might have been at risk of financial harm from fraud from payment one. And in those circumstances, it should have provided a written warning, which I am persuaded would have resonated with her. If it had taken those steps, I am satisfied it would have prevented the losses Mrs P suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mrs P's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs P'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 the point Revolut has raised regarding Mrs P only complaining 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 P could instead, or in addition, have sought to complain against those firms. But Mrs P 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 P'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 P's loss from Transaction one subject to a deduction for Mrs P's own contribution which I will consider below.

Should Mrs P bear any responsibility for her losses?

I've considered whether Mrs P should share any liability for the loss. 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. Overall, I do think it's fair to expect Mrs P to share liability equally with Revolut. I'll explain why.

I appreciate Mrs P says she had registered her interest on social media regarding the investment, so contact from the scammer wasn't unexpected. I also note she says the scammer came across as professional. But Mrs P has also said she was pressurised to take out a loan, and whilst I appreciate the scammer convinced her this was the normal process for this type of 'investment', a genuine investment company wouldn't pressurise a consumer to take out a loan to fund the investment. So, I think this ought to have alerted Mrs P to the fact something wasn't right.

I appreciate Mrs P did question the scammer about this (as explained above) demonstrating it had casted doubt in her mind, but at that point, I think it would have been prudent of her to have completed further research.

Mrs P has said she did carry out research prior to investing and had seen several good reviews. And while I don't doubt Mrs P's recollection of events, having completed a simple internet search, I found an FCA warning which gives a link to the FCA website. This confirms on 2 February 2023 (22 days before her first payment) that the company was an unauthorised firm and consumers should avoid dealing with the firm as it could be a scam.

I do accept that Mrs P has said she wasn't familiar with the FCA website and was an inexperienced investor. But I have also seen independent websites highlighting it was a potential scam, prior to when Mrs P invested. With that in mind, I think it's reasonable to conclude that there was evidence readily available to alert Mrs P to highlight it was a scam. I do accept that there may have been elements to the scam which appeared sophisticated. However, I do think there were some red flags Mrs P ought to have picked up on. For the avoidance of doubt, it is not my finding that Mrs P knew that she was likely falling victim to a scam and went ahead anyway. But I do think based on some of the information available to her that there was a possibility something wasn't right, or that she might not recover her money. In those circumstances it would not be fair to require Revolut to compensate her for the full amount of her losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mrs P because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything to recover Mrs P's money?

I have gone on to consider if Revolut took reasonable steps to try and recover the funds. As, Mrs P made the payments via debit card, the chargeback process is relevant here. The chargeback scheme is a voluntary agreement between card providers and card issuers who set the scheme rules and is not enforced by law. A chargeback isn't guaranteed to result in a refund, there needs to be a right to a chargeback under the scheme rules and under those rules the merchant or merchant acquirer can defend a chargeback if it doesn't agree with the request.

Unfortunately, the chargeback rules don't cover scams. So, Revolut would only be able to process chargeback claims against the merchant she paid. The merchant in this case was a genuine cryptocurrency exchange. The service provided by the cryptocurrency exchange would have been to convert or facilitate conversion of Mrs P's payments into cryptocurrency. Therefore, they provided the service that was requested.

I appreciate the cryptocurrency was later transferred to the scammer but that does not give rise to a valid chargeback claim against the merchant Mrs P paid. As the cryptocurrency exchange provided the requested service to Mrs P any chargeback attempt would have likely failed.

Compensation

I note that Mrs P has said that she wants £300 compensation for the distress and inconvenience caused and to cover her legal fees. As our investigator has highlighted, our service is free to use, and consumers can approach us without the use of legal representation. Whilst I don't dispute Mrs P would have felt distressed and inconvenienced by the scam she fell victim to, I haven't seen any evidence to persuade me that Revolut should pay Mrs P compensation as a result.

Putting things right

For the reasons I have explained above, I feel Revolut ought to have recognised that Mrs P might have been at risk of financial harm from fraud when she made Payment one, and in those circumstances, it should have provided a warning, and if it had done so it would have prevented Mrs P's losses.

So, it follows that I think it's reasonable Revolut should pay Mrs P:

- 50% of all payments from and including payment one.
- 8% interest on that amount (to reflect the loss of use of this money in the account) from the date the payment was paid to the date of settlement less any tax lawfully deductible.

My final decision

My final decision is that I uphold in part this complaint and require Revolut Ltd to pay Mrs P in line with the redress I have highlighted above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs P to accept or reject my decision before 2 July 2025.

Jade Rowe
Ombudsman