DRN-5215515

The complaint

Miss L is unhappy Revolut Ltd won't reimburse money she lost to a scam.

What happened

Around July 2022, Miss L came across a social media advert promoting a cryptocurrency investment which appeared to be endorsed by some well-known media personalities. She provided her contact details and received a call back from someone claiming to be part of an investment company, "Q". Unfortunately, Miss L was dealing with a scammer.

Miss L decided to invest and was assigned an account manager. She was given access to a trading platform, which appeared to show her payments being loaded then traded. To fund the trading account, Miss L was advised to set up an account with Revolut. She would send funds from Revolut to "B" and "W", cryptocurrency exchanges, to purchase cryptocurrency and send on to what she thought was her own account with Q. The scammer used remote access software to guide her through the process.

I've set out all the payments made, and received, in connection with the scam from Miss L's Revolut account below:

Payment number	Date and Time	Merchant	Type of payment	Amount
1	21 July 2022, 08:32	B	Debit card	£220
2	19 August 2022, 10:39	B	Debit card	£260
3	16 November 2022, 10:05	W	Debit card	£249.47
4	22 December 2022, 20:05	B	Debit card	£1,455
5	23 December 2022, 09:25	B	Debit card	£1,876
6	23 December 2022, 16:12	B	Debit card	£1,598
	13 January 2022, 13:26	*"C"*	*Credit*	*£490.72*
7	14 February 2023, 12:50	Recipient linked to B	Transfer	£38,500

Miss L has explained she didn't complete independent research into Q at the time of investing. She started by investing a smaller amount and paid in more after appearing to make a good return. In early 2023, having also received a small withdrawal from Q's platform, she was persuaded to take out loans to fund further trading – giving the loan purpose as 'home improvements' on the applications.

After making these payments from her Revolut account, Miss L set up a new account with a bank, and used this to send around £20,000 more on to the scam (again, sending the funds on via her cryptocurrency wallets).

Following this, in April 2023 Miss L enquired about withdrawing funds from Q. Her account manager stopped replying, and she found she could no longer access her trading account. Realising she had been scammed, she contacted Revolut. When it wouldn't agree to refund her, she referred the matter on to our service.

In its submissions to our service, Revolut argued all the payments had been authorised by Miss L. It said she hadn't sought proper investment advice or done enough to look into Q before investing. It also said the first six scam payments hadn't appeared concerning, bearing in mind the account was newly opened. And it had intervened on payment 7 – but Miss L had ignored its scam warnings. It denied liability for Miss L's loss.

One of our investigators upheld Miss L's complaint. They thought Revolut should have warned/questioned Miss L further when she made payment 7. And that, if it had done so, the scam would have come to light – preventing Miss L's further losses.

The investigator also thought Miss L bore some responsibility for those losses. They thought she should have been concerned about being told to say the loans were for home improvements when she was using the money to invest. They also thought she should have looked into Q further – and that doing so would have revealed further concerns. The investigator thought a fair deduction for the amount reimbursed would be 50%.

Miss L accepted this outcome. Revolut didn't agree. In summary, it said:

- When it intervened, it warned Miss L about the risk that scammers can pretend to be an exciting investment opportunity (amongst other things). As she proceeded following its warnings, it was obliged to proceed with her request.
- It does not owe a duty to prevent fraud and scams. Rather, it has a duty to execute valid payment instructions.
- No reimbursement codes apply to the payments Miss L made.

I then issued my provisional decision in November 2024 explaining why I was minded to agree with the investigator's overall conclusions about how the complaint should be resolved. I invited both parties to provide any further comments or evidence for me to consider. Miss L responded to confirm her acceptance of my provisional findings. Despite several chasers, Revolut hasn't responded.

In line with the Dispute Resolution ("DISP") rules our service follows, specifically DISP rule 3.5.14, as Revolut has failed to comply with the deadline set in my provisional decision (and the extended deadline given in further chaser messages), I'm now proceeding with my consideration of this complaint.

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.

As I have not received anything further to consider in response to my provisional decision, I see no reason to depart from it. I therefore uphold this complaint for the following reasons – as previously set out in my provisional findings.

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 the 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 L modified the starting position described in *Philipp,* by expressly requiring it 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 L and the Payment Services Regulations to carry out her 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[1]. 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 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) at the time of Miss L's scam payments.

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 do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]

---

[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).

- 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:

- EMIs 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"*.
- 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 here, but I nevertheless consider these requirements to be relevant to the consideration of a firm's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017 BSI Code[4], 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 Code 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] 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.

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

- 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 the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably have been doing the following at the time Miss L made these scam payments:

- 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.

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

It isn't in dispute that Miss L has fallen victim to a cruel scam here, nor that she authorised the scam payments to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

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

Miss L's Revolut account was newly opened for the scam, so Revolut had no prior sense of what typical account activity for her was. It would have seen that the merchants she sent the initial scam payments to appeared to be genuine cryptocurrency exchanges. It is also common that such exchanges stipulate the card used to purchase cryptocurrency must be held in the name of the account holder. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed the card payments would be credited to cryptocurrency wallets held in Miss L's name.

However, I'm also conscious that, by July 2022 – so at the time of the first scam payment – 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 have continued to increase since – reaching record levels in 2022.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think the destination of payments 1-6 should have led Revolut to believe Miss L *wasn't* at risk from fraud. But, looking more widely at how the account was being used, I'm not persuaded it ought to have seen those transactions as carrying a significantly heightened fraud risk.

Payments 1-3 were for modest amounts, and were spread out – with gaps of weeks, and months, in between. While payments 4-6 occurred in quicker succession (over two days in December 2022), and were for higher amounts, I don't consider this to be such a significant escalation that Revolut ought to have been concerned about fraud. By that point, Miss L had already paid B previously in July and August 2022. So the merchant, and nature of the transaction, seemed fairly consistent with how Miss L had been using the account.

However, when Miss L made payment 7, I think Revolut should have recognised she was at risk of financial harm from fraud. I don't think it would have been apparent to Revolut from the outset that this payment was linked to cryptocurrency. But it was a significantly large payment, and was out of keeping with Miss L's account history – at more than twenty times the size of the next largest payment. I think this made the fraud risk apparent.

What did Revolut do to warn Miss L and was this sufficient?

When Miss L added the payee for payment 7, Revolut showed her the following warning:

> *"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. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."*

This was a very general scam warning, so I don't think it would have struck Miss L as relevant to what she was doing. But Revolut went on to ask her for the purpose of the payment. She selected "payment for goods and services". It then asked the following questions:

- *"Does the offer seem too good to be true?"*
- *"Have you been asked to pay via bank transfer instead of the payment method recommended by the marketplace?"*
- *"Was the product or service you are paying for advertised on a social media platform or has a small number of reviews?"*

After this, Revolut says Miss L had the option to cancel the payment or to chat to one of its agents. She selected the latter. In the chat, Revolut then displayed the following warnings – asking Miss L if this, or something similar, was the reason for her payment:

"…please be aware that scammers are using increasingly sophisticated techniques to gather personal information and convince customers to transfer funds in complex scams. They can pretend to be a financial institution, government institutions, trusted online merchants, an exciting investment opportunity or even people you know. They may even contact you by phone or SMS from a number that appears to belong to a trusted source, such as Revolut or another bank. Revolut will NEVER contact you over the phone without verifying ourselves first via the in-app chat. We will also NEVER contact you by SMS to verify ourselves."

"We have noticed an emerging fraud trend and so we want to check some further details with you before you transfer your money. If you have been called by any bank claiming that your account is not safe and you need to move your money to another account, stop. They may claim that they have created a new 'safe' account for you to move your money into or they may claim that this is part of a special police / internal fraud investigation. This is a lie and is a tactic which scammers are using to scare you."

"Be aware that they are able to make it appear that they are calling you from a genuine bank phone number to convince you that they are from that bank. Remember, if you continue to transfer your money to the account details you have been provided, we cannot guarantee that we will be able to recover your money and you risk losing it."

Miss L confirmed she was still happy with the payment. She then confirmed she hadn't been contacted by anyone asking her to move money to another account. Revolut then said,

"I can see that you have advised that this transfer is for goods and services. If you have been told to select this option but you are not making a purchase stop, this is a scam. Have you been asked to ignore scam warnings during making the payment?"

Miss L said she hadn't been. She explained she was transferring money *"to an exchange to [buy] digital currencies for myself".* Revolut then displayed the following warning – after which she was able to proceed with the payment:

"Please be aware that scammers will typically offer a price below market value to attract your attention. Social media has also become an easy way for scammers to advertise their goods and services. Please do your research on the seller and try to verify if they are a genuine seller. You should check if the seller has reviews from previous customers before proceeding. If you have any concerns then do not proceed with the purchase. After this chat has ended, please return to the Revolut app where you can review the details of this transfer, consider the information provided and decide if you would like to continue with the transfer."

Given the significant size of the payment, and how different it was to the previous account activity, I think it as reasonable for Revolut to speak to Miss L directly through its in-app chat to try establish the circumstances surrounding the payment. But the warnings it gave were not very relevant to the features of the scam Miss L fell victim to. I don't think its response was proportionate in light of what Miss L had disclosed about the purpose of the payment. Namely, that she was purchasing digital currency.

What kind of warning should Revolut have provided?

Revolut argues it showed the warnings it did because Miss L selected the payment purpose as "goods and services" rather than "investment". However, it's clear from her chat response that she wasn't trying to disguise what she was doing – as when asked, she told Revolut she was purchasing digital currency.

Once Revolut was on notice that Miss L was sending a payment of almost £40,000 to purchase digital currency, I think it should have warned Miss L about the risks of cryptocurrency scams – given their prevalence at the time.

I think Revolut should have highlighted the key features of common cryptocurrency investment scams. While it could not cover off every eventuality, key points it could have flagged include: the use of social media adverts, seemingly promoted by a celebrity or public figure; the use of an 'account manager', 'broker' or ''trader' acting on their behalf; the use of remote access software; being encouraged to make smaller initial deposit which quickly increases in value; and being able to make a small withdrawal to induce them to pay in more.

If Revolut had intervened proportionately, would that have prevented the losses Miss L suffered from payment 7?

I've thought carefully about whether further contact and warnings from Revolut about the risks of cryptocurrency scams would have dissuaded Miss L from proceeding. On balance, I'm persuaded it would have done.

I'm mindful Miss L did disclose that she was purchasing digital currency. So, it seems to me she wasn't given a strict cover story to follow by the scammers in the event of being questioned about the payment.

This also fits with what I've found when looking at Miss L's interaction with the other bank from whom she sent payments to the scam. In March 2023, the bank flagged one of the scam payments (for around £10,000), and asked Miss L for more detail about what she was doing. Similar to what she told Revolut, she disclosed that she was investing in cryptocurrency – and that this was something she was new to.

The bank asked whether the account she was paying was within her control, which Miss L confirmed it was. She also confirmed only she had access to it. I think this seems consistent with Miss L's understanding of the account she was paying – particularly bearing in mind she was sending funds via her own wallets. I think this further demonstrates she wasn't trying to conceal what she was doing – so would have responded honestly to further questioning from Revolut.

I do accept there are some signs from the contact records that the scammers were trying to exert influence over Miss L. For example, at one point (not connected to Revolut's intervention) they say not to allow her bank to ask questions like she is a "*terrorist",* and to be *"bossy"* with them. But equally, it's clear from both interactions that Miss L did disclose the main reason for the payments when asked. She says she received some guidance from the scammers, but wasn't given a cover story. I consider that both plausible and likely, given what I have seen about how she interacted with her account providers when questioned about scam payments.

The bank warned Miss L cryptocurrency was a target for fraud and scams. It said if she was being pressured, or the investment was too good to be true, it was probably a scam. It appears Miss L was alive to this warning, and had some concerns – as she initially said she wanted to do some more research before deciding whether to proceed. That suggests she was open to heeding such warnings from her account providers.

Despite this hesitation, Miss L did ultimately decide to proceed with the payment. However, I'm conscious the warning did not cover many of the key features of cryptocurrency scams – such as those I have set out above when explaining what I thought Revolut's warning should have covered. Such as the use of remote access software and an account manager – both of which were relevant to the scam Miss L fell victim to.

If Revolut had covered the key features of cryptocurrency scams in more detail, I'm therefore persuaded Miss L would have realised this was relevant to her. I think she would have been persuaded not to proceed immediately. If she had then been prompted to look into Q further, it's likely she would have found public information, readily available online, raising serious concerns about them. Such as a warning issued by the FCA about Q in late 2022.

In those circumstances, I'm therefore persuaded that proportionate intervention by Revolut would have uncovered the scam and prevented Miss L from going ahead with payment 7.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss L purchased cryptocurrency which credited a wallet in her name, rather than making a payment directly to the scammer. 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 scam.

But as I've set out above, I think Revolut should still have recognised that Miss L might have been at risk of financial harm from fraud when she made payment 7, and in those circumstances should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the further loss Miss L 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 Miss L's own (cryptocurrency) account, does not alter that fact and I think Revolut can fairly be held responsible for her 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 L has only complained against Revolut in relation to the loss suffered from these payments. 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 L could instead, or in addition, have sought to complain against those firms. But she 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 L 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 L's loss from payment 7 (subject to a deduction for her own contribution which I will consider below).

Should Miss L 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. Having carefully considered this matter, I think there should be a 50% deduction to the refund I'm proposing for payment 7.

I can see why, as someone new to cryptocurrency investing, there were several features of the scam that seemed convincing. Such as the use of manipulated software to make it appear to Miss L that her Q account was being used for genuine trading.

However, I do think Miss L should have been more sceptical of some of the returns she was told she could make. For example, I've seen she was told in December 2022 that, if she made a relatively modest investment, she could expect to almost double her profit by the following month.

I also think Miss L should have been further concerned when Q directed her to take out a substantial amount of lending to fund further trading. If the investment had been legitimate, the funds would still have been at risk – so I think Miss L should have been concerned that Q was encouraging her to take on the risk of substantial debt. Particularly as it told her to declare the purpose of the loans as 'home improvements' – when she knew that wasn't how she would be using the funds.

I think, by this point at the latest, Miss L should have been concerned about Q's legitimacy. As mentioned above, if she had therefore undertaken independent research into Q, she would likely have discovered information online raising concerns about its operations.

Overall, I therefore think it would be fair for the loss stemming from payment 7 to be shared. Revolut should have prevented this loss – but Miss L should also have been aware of the warning signs Q might not be legitimate.

My final decision

For the reasons given above, my final decision is that I uphold this complaint and direct Revolut Ltd to pay Miss L 50% of payment 7 (a total of £19,250), plus 8% simple interest per year on that amount from the date of payment to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss L to accept or reject my decision before 3 February 2025.

Rachel Loughlin
Ombudsman