DRN-5135047

The complaint

Miss L complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Miss L came across an online advert for a company which I'll refer to as "E", which was endorsed by a well-known celebrity. She did some basic research and noted generally positive reviews. She also checked the Financial Conduct Authority (FCA) website, noting the company wasn't listed because it was based overseas. She saw the company had mixed reviews, but felt was usual for legitimate businesses and reassured by the celebrity endorsement.

Miss L paid an initial fee of £233.59 using a credit card. This gave her access to an investment platform which I'll refer to as "F" and she was assigned an account manager, who I'll refer to as "the scammer". The scammer told her she could make returns of 10-15% by investing in cryptocurrency and that she could make withdrawals at any time.

He asked her to first purchase cryptocurrency through a cryptocurrency exchange company I'll refer to as "B", and then load it onto an online wallet. She transferred £23,000 into her Revolut account from Bank S, and £48,500 from Bank B. And between 31 January 2023 and 19 April 2023, she made sixteen transfers from Revolut to B totalling £71,500. On 3 March 2023, she received £1,124.39 from B.

Miss L made withdrawals at the end of January 2023 and February 2023, but the scammer said she'd have to pay an insurance fee and taxes before she could make any more withdrawals, at which point she realised she'd been scammed.

She complained to Revolut, but it refused to refund the money she'd lost. It said it was unable to raise a chargeback dispute because the payment was a money transfer, and the service was considered provided.

Miss L complained to this service with the assistance of a representative who argued that Revolut missed an opportunity to intervene because Miss L made large and frequent payments to a cryptocurrency merchant, which was unusual for the account. They said it should have asked probing questions including how she came across the investment, what returns she was promised, and what research she did. It should also have warned her about the risks associated with the investment, and had it done so she wouldn't have made any further payments.

Revolut further commented that Miss L said she'd researched the investment, but a simple google search showed results suggesting the investment company was a scam. It also said the payments were authorised by 3DS, so they couldn't have been completed without Miss

L’s permission, and they were made to cryptocurrency accounts in Miss L’s name, so the fraudulent activity didn’t occur on the Revolut platform.

It argued that the account was newly created, so there was no spending history to compare the payments with. Miss L had received funds back from B, which indicated there was an established relationship between the accounts. And there were multiple days between most of the payments, so she wasn’t rushed or coerced and had sufficient time to perform due diligence.

Revolut also cited the Supreme Court’s judgment in Philipp v Barclays Bank UK plc where the court held that in the context of APP fraud, where the validity of the instruction is not in doubt, no inquiries are needed to clarify or verify what the bank must do.

Finally, it said the payments were self-to-self- transactions and that its irrational to hold it liable for losses in circumstances where it is merely an intermediate link, and there are typically other authorised banks in the payment chain that had comparatively greater data on Miss L.

Our investigator recommended that the complaint should be upheld. He explained that, even though Miss L hadn’t used the account for a long time, Revolut ought to have been concerned because she was paying a high-risk cryptocurrency merchant, and that the payments didn’t match with the account opening purpose she gave, which was ‘transfers’. He also commented that funds were paid into and out of the account in quick succession, and the value of the payments was significant.

He thought Revolut ought to have intervened when Miss L made the first payment on 31 January 2023, and that a proportionate response would have been to provide a written warning covering off the key features of cryptocurrency investment scams such as false online articles mentioning celebrity endorsements, and unrealistic returns. It should also state that legitimate investment firms wouldn’t correspond via social media or WhatsApp and provide information about due diligence. He was satisfied a warning would have resonated with Miss L because the key features of the warning mirrored her situation, and so her loss would have been prevented.

Our investigator recommended that Revolut should refund Miss L’s loss from the first payment onwards, explaining that he didn’t think the settlement should be reduced for contributory negligence because she was an inexperienced investor, and we wouldn’t expect her to have known how to properly research the investment. He noted that she’d checked the FCA website and didn’t see any warnings, and that she’d been reassured by the celebrity endorsement, which he thought was reasonable.

Finally, he explained that the credit Miss L received on 3 March 2023 would be deducted from the settlement and that as he was also recommending that the complaint against Bank B should be upheld, liability for the funds that were sent from Bank B to Revolut should be shared between both parties.

Revolut has asked for the complaint to be reviewed by an Ombudsman. It has reiterated that this is a self-to-self scenario and the cryptocurrency platforms were the final stage before Miss L allegedly sent the funds to the scam, so the fraudulent activity didn’t occur on the Revolut platform.

It has explained that it is an Electronic Money Institute (“EMI”), and this type of account is typically opened and used to facilitate payments for a specific purpose and often not used as a main account. The payments weren’t out of character with the typical way in which an EMI account is used, especially since high street banks have started restricting customers from sending money to cryptocurrency exchanges.

Revolut has also stated that our recent reliance on R (on the application of Portal Financial Services LLP) is misconceived and amounts to a legal error. It has argued that the decision can't be relied on to allow us to abdicate responsibility for examining precisely what happened in a given case and completely ignoring the role of other parties and that we should consider the role of all of the other financial institutions involved and other bank interventions, which is relevant to whether Miss L acted negligently.

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 L 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 L 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[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 in January 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".*
- 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

[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_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.

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 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 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 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 January 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;
- 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 payments she made by transfers to third parties and to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in detail in this 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 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 L might be the victim of a scam.

I'm aware that cryptocurrency exchanges like B generally stipulate that the account used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Miss L's name.

By January 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 January 2023, when the first 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, 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 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 January 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 the payments in this case were going to an account held in Miss L's own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Miss L might be at a heightened risk of fraud that merited its intervention.

I've considered the nature of the payments in the context of whether they should have triggered Revolut's fraud systems, and I think they should have. Miss L was sending funds to a cryptocurrency account which she hadn't paid before, and the first payment was for £5,000, so given what it knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Miss L was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Miss L before the payment went ahead.

As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by January 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What kind of warning should Revolut have provided?

I think a proportionate response would have been to provide a written warning covering some of the key features of cryptocurrency-related investment scams, for example:

• Victims are usually targeted via social media or email.

• Scammers will utilise fake positive reviews from other individuals, or fake celebrity endorsements.

• Fake online trading platforms can appear professional and legitimate.

I've thought carefully about whether a warning tailored to cryptocurrency investment scams would have likely prevented any further loss in this case, and, on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present, such as finding the investment through an advertisement endorsed by a celebrity and being assisted by an 'account manager' or 'broker', and so I think Miss L would have realised the warning was relevant to the circumstances of the investment.

I haven't seen any evidence that she was asked, or agreed to disregard any warning provided by Revolut, neither have I seen any evidence that her relationship with the scammer was so close that Miss L wouldn't have listened to Revolut's advice. And I've seen no evidence that she was provided with warnings by other firms. Therefore, on the balance of probabilities, had Revolut provided Miss L with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her and she could have paused and looked more closely into the investment, which would have revealed the scam and prevented her losses.

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

As I've set out above, I think that Revolut still should have recognised that Miss L might have been at risk of financial harm from fraud when she made the first payment, and in those circumstances Revolut should have provided a written warning tailored to cryptocurrency investment scams before processing it. If it had done that, I am satisfied it would have prevented the losses she 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 L's own account does not alter that fact and I think Revolut can fairly be held responsible for the 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.

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 the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved, which I'm satisfied I have done.

Should Miss L bear any responsibility for her losses?

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for Miss L to have believed what she was told by the scammer in terms of the returns she was told were possible, notwithstanding the fact it was highly implausible.

Miss L hadn't invested in cryptocurrency before and so this was an area with which she was unfamiliar. She wouldn't have known the returns were unrealistic or how to check the information she'd been given. And she wouldn't have known the celebrity endorsement was a red flag without being alerted to this by Revolut. This unfamiliarity was compounded by the sophisticated nature of the scam, and the fact she trusted the scammer and believed the trading platform was genuine.

Revolut has argued that there was lots of information online about celebrity endorsements being related to scams, but as Miss L thought the endorsement was genuine, there would have been no reason for her to make these checks. And she has explained that she saw mixed reviews online but was satisfied this was normal and she thought E didn't need to be regulated by the FCA because it was based overseas. I don't think this is unreasonable and whilst there may be cases where a reduction for contributory negligence is appropriate, I don't think this is one of them.

Apportionment

As the parties are aware, Miss L has also complained about the actions of Bank B. Our service's ability to investigate complaints together and apportion the burden of redress between respondents is the subject of no specific rule and only limited guidance, which can be found in the FCA's Handbook at DISP 3.5.3G and DISP 3.6.3G, which say:

DISP 3.5.3G: *"Where two or more complaints from one complainant relate to connected circumstances, the Ombudsman may investigate them together, but will issue separate provisional assessments and determinations in respect of each respondent."*

DISP 3.6.3G: *"Where a complainant makes complaints about more than one respondent in respect of connected circumstances, the Ombudsman may determine that the respondents must contribute towards the overall award in the proportion that the Ombudsman considers appropriate."*

I've found there were failings not only by Revolut but also Bank B in what reasonably could've been expected of them. And with respect of £48,500, which was paid into Revolut from Bank B before being paid to B as part of the scam, I think it's fair to ask each of them to pay half the loss they could've prevented. Bank S isn't being held be responsible for any of the losses, so the £23,000 which was sent from Bank S to Revolut and on to B should be payable in full by Revolut.

I'm satisfied interest calculated at 8% simple per year is also appropriate to compensate Miss L for having been deprived of these funds.

Recovery

I don't think there was a realistic prospect of a successful recovery because Miss L paid an account in her own name and moved the funds onwards from there.

Compensation

The main cause for the upset was the scammer who persuaded Miss L to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think she is entitled to any compensation.

My final decision

My final decision is that Revolut Ltd should:

- refund 50% of £48,000.
- refund £23,000.
- 50% of £1,124.39 should be deducted from the settlement to reflect the credit Miss L received from B on 3 March 2023.
- pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Miss L with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms L to accept or reject my decision before 17 January 2025.

Carolyn Bonnell
Ombudsman