

The complaint

Miss B complains that Revolut Ltd won't refund money she lost when she fell victim to a cryptocurrency investment scam.

What happened

Miss B says that in the autumn of 2023 someone online mentioned that they had used and made some money from an investment trading broker "X". This prompted Miss B to review X's website which she says looked professional. She also read an article about it on a website providing financial news, data, as well as commentary and analysis. It said that many people had made money through X. Miss B also saw videos relating to X on a video sharing platform. And she found that X held events in different cities around the world. After registering her interest, Miss B was contacted by someone who claimed to be a representative of X. They talked her through the investment opportunity – she was told she could double her investment in 29 days and was promised 2.5% compound interest in whatever she invested. Encouraged by this, Miss B decided to open a trading account with X.

Under the instructions of her 'account manager', Miss B opened an account with a cryptocurrency exchange as well as an e-money account with Revolut. She states she was told X preferred its clients to use the services of Revolut, which was an affiliate. To make deposits into her trading account, Miss B first transferred funds from her bank account to her e-money account with Revolut. She then made debit card payments to purchase cryptocurrency from the cryptocurrency exchange, before sending it on to wallets as instructed. At the time, she believed the cryptocurrency was being deposited into her account with X, given its balance increased by the corresponding amount.

When she asked to make a withdrawal, Miss B was told there were issues with the withdrawal being processed. Subsequently, X cut off all communication with her. It was at that point that Miss B realised she had been scammed.

The following debit card transactions, all in 2023, are relevant to this complaint –

	Date	Amount
Payment 1	11 October	£500
Payment 2	21 October	£500
Payment 3	24 October	£500
Payment 4	31 October	£500
Payment 5	31 October	£190
Payment 6	1 November	£200
Payment 7	20 November	£1,000
Payment 8	20 November	£200
Payment 9	20 November	£100
Payment 10	20 November	£2,500
Payment 11	20 November	£100
Payment 12	20 November	£100

	Total loss	£6,390

Miss B reported the scam to Revolut through its in-app chat function on 29 November. The agent instructed her to order a new card and submit a chargeback for the disputed transaction. Miss B asked for the agent's help in selecting the appropriate chargeback reason as scam wasn't on the list. The agent told her to choose "someone else made this payment" to allow the system to complete the submission.

Three days later, Miss B contacted Revolut again and asked to speak to an agent to discuss the matter again. She explained she was sold a dream to get rid of her family debts but instead all her savings were gone. Miss B mentioned she suffered from depression and was distressed about what had happened. The agent asked Miss B if she wanted to continue communicating via chat correspondence or if she wanted to request a phone call. She initially asked for a phone call but agreed to continue over chat as she didn't want to wait.

The agent went over some of the details before advising Miss B that they would need to transfer her to the appropriate team. Shortly afterwards, Miss B was informed by an agent from that team that her claim wasn't valid given Revolut had not found any evidence of fraudulent activity on her account – Miss B was familiar with the transactions.

Miss B explained that she had been scammed into thinking it was an investment. The agent informed her that if she didn't agree with Revolut's outcome and was sure that she was a victim of fraud, she'd need to file a police report if she hadn't already done so. Miss B told the agent she'd contacted Action Fraud. But the agent said there wasn't anything more Revolut could do about the situation.

Miss B asked if she could raise a complaint and have a manager call her back. After chasing the agent for a response, she was told that it wasn't possible. Miss B reiterated her request and the agent offered to schedule a call between its call support team's operational hours. Miss B provided a time slot for the following day and the agent confirmed that a request had been raised and the team would reach out to her.

The next day, 4 December, when she didn't get a call-back, Miss B contacted Revolut through its in-app chat. She was advised that the call might have been delayed due to an overwhelming number of requests. The agent reassured her that the team would reach out to her soon. Miss B contacted Revolut again the following day and said she hadn't heard back. She was informed that she would get a call soon. Miss B asked if the agent could help her over the chat and explained the situation again, but they told her to wait for the call which she would receive soon.

On 6 December, Miss B asked to raise a complaint with a manager as she still hadn't had received a call from Revolut. The agent said they believed they could help Miss B with her case and asked for some time to review the information. Moments later, they said the case had already been finalised and so there would be no change. The agent provided Miss B with a link to filling out a complaint form.

Later that day, Miss B contacted Revolut again and asked why it was refusing her claim when she had received a crime reference from Action Fraud and had been asked to contact Revolut. She asked why other banks were refunding customers, but Revolut had refused to. Miss B also told the agent that she'd already raised a complaint a few days earlier but wanted to speak to someone over the phone about the matter as she was getting distressed. The following day, she was informed that the phone support team was unable to call her due to a large number of requests it was getting.

On 16 December, Miss B contacted Revolut again and forwarded a complaint she said she'd already made. In the complaint, she raised concerns about the customer service she had received from Revolut in relation to reporting the scam, including the difficulties she had when reporting the scam and being asked to complete a chargeback dispute. Miss B explained that she was disabled and had a learning difficulty and suffered from mental health issues. She said she was disappointed that no one had called her back despite requesting this on several occasions.

The agent told Miss B that the complaints team would respond to her complaint by email. They also asked her if she wanted to arrange a phone call to discuss the matter over the phone. Miss B said yes and was informed that Revolut would call her on 18 December. On 18 December, Miss B was notified via chat that the final outcome of the dispute couldn't be influenced. She could submit a police report but the dispute couldn't be challenged as per the card scheme's rules.

Miss B asked about the call-back, and she was told that Revolut was unable to fulfil her request at that time. She asked why and the agent said this was due to overwhelming requests. Miss B explained the call wasn't just in relation to the transactions but also the poor customer service. The agent informed Miss B that the manager on duty was busy and although they could transfer her shortly, the results couldn't be influenced by the manager. Two minutes later, the agent told Miss B that a manager could only assist in chat and a call request couldn't be completed.

Miss B was informed by the manager that her complaint would be responded to within 15 working days and that Revolut wouldn't be able to fulfil her request for a phone call at that moment. Miss B asked if the manager could add her communication preference to the complaint so that the complaint response would be discussed over the phone. Shortly afterwards, the manager advised Miss B that her complaint had already been responded to on 12 December. Miss B told the manager that her complaint about the poor service hadn't been addressed and she wanted a call back to discuss that. She was informed that a phone call wasn't possible at the time. Miss B requested a phone call a few more times after that date but was told this wasn't possible.

In its final response, Revolut declined to refund any of the disputed payments, saying that Miss B had authorised them.

Unhappy with this, Miss B referred her complaint to our service. Our investigator didn't think the payments were unusual such that Revolut ought to have taken additional steps when they were made. Miss B disagreed with the investigator's outcome and another investigator considered her complaint. But they also reached the same conclusion.

I issued my provisional decision on this complaint in September 2024. I gave reasons for why I intended upholding it. I said:

"In deciding what's fair and reasonable, I'm 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 B 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".

In this respect, section 20 of the terms and conditions said:

"20. When we will refuse or delay a payment

We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:

- 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 B and the Payment Services Regulations to carry out her instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I'm satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in October 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in Philipp.

I've taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I'm also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But the basis on which I'm 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 October 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'm mindful that in practice all banks and EMLs like Revolut do in fact seek to take those steps, often by:

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

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/

For example, it is my understanding that from October 2023, Revolut operated a process whereby if it identified a scam risk associated with a card payment through its automated systems, it might initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat). If Revolut was satisfied with the response to those questions and/or it provided a relevant warning, the consumer could use the card again to instruct the same payment and Revolut would then make the payment.

I'm 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 customer’s accounts and scrutinise transactions.*
- The October 2017, BSI Code², which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).*
- Since 31 July 2023, under the FCA’s Consumer Duty³, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable*

² BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

³ Prior to the Consumer Duty, FCA regulated firms were required to “pay due regard to the interests of its customers and treat them fairly.” (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was “consumers becoming victims to scams relating to their financial products for example, due to a firm’s inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers”⁴.

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency⁵ 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.*
- 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 October 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;*
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;*
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings,*

⁴ The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

⁵ Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

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.*

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

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

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

I'm aware that cryptocurrency exchanges generally stipulate that the card 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 all of the disputed payments would be credited to a cryptocurrency wallet held in Miss B's name.

By October 2023, when these transactions started, 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 transactions⁶. And by October 2023, when these payments took place, further restrictions were in place⁷. 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 (as Revolut has told our service).

⁶ See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

⁷ In March 2023, both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

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'm satisfied that by the end of 2022, prior to the payments Miss B made in October 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.

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 B'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 B might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all the payments were going to a cryptocurrency provider (the merchant is a cryptocurrency provider). The first nine payments were relatively low in value, and spread across several days, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

But by the time Miss B made Payment 10, I consider that a pattern of increased spending on cryptocurrency had emerged. The payment in question was significantly larger than any other payments that had debited Miss B's account, and it was the fourth cryptocurrency related payment in one day. I think that the circumstances should have led Revolut to consider that Miss B was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Miss B?

Revolut says the disputed transactions were not deemed out of character for Miss B's account activity. It says the payments didn't take place in rapid succession, which is common for many scams. For the later transactions, Revolut says the merchant was no longer a new payee and so didn't warrant an intervention.

What kind of warning should Revolut have provided?

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 primary duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by October 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. As I explained earlier in this decision, I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider a firm should by October 2023, on identifying a heightened scam risk, have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that Payment 10 was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation, and investment scams.

Taking that into account, I'm satisfied that, by October 2023, fairly and reasonably, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Miss B made Payment 10, Revolut should – for example by asking a series of questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely cryptocurrency related scam Miss M was at risk from.

In this case, Miss B was falling victim to an investment scam – she believed she was making payments in order to deposit funds into her trading account. As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Miss B gave.

The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media; promises of returns that are too good to be true; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Miss B by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss B suffered from Payment 10 onwards?

I've thought carefully about whether a specific warning covering off the key features of 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 in the circumstances of Miss B's payments, such as finding out about the opportunity through someone she'd met online, being assisted by a broker who assisted her in making deposits to her trading account, being promised returns that were unrealistic (double in 29 days and compounded interest), etc.

We've asked her and Miss B no longer has the text conversation between her and the scammer – she's unable to recover it either. As such, I haven't seen anything that indicates that Miss B expressed mistrust of Revolut or financial firms in general. I've also taken into account that Miss B hadn't received any returns at the point of the suggested intervention. So, I'm not persuaded that she was so taken in by the scammer that she wouldn't have paid attention to Revolut's warning. I've also seen no evidence that Miss B was provided with warnings by the firm from which the funds used for the scam originated.

Therefore, on the balance of probabilities, had Revolut provided Miss B 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. She could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Miss B from Revolut would very likely have caused her to pause and take additional steps to verify the legitimacy of the investment opportunity – revealing the scam and preventing her further losses.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Miss B purchased cryptocurrency which credited an e-wallet held in her own 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 further steps were required before the money was lost to the scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss B might have been at risk of financial harm from fraud when she made Payment 10, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I'm satisfied it would have prevented the losses Miss B 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 B's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss B'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 point of loss.

I've also considered that Miss B has only complained to us about Revolut. I accept that it's possible that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Miss B could instead, or

in addition, have sought to complain against those firms. But Miss B has not chosen to do that and ultimately, I can't 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 B'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'm satisfied that it would be fair to hold Revolut responsible for Miss B's loss from Payment 10 onwards (subject to a deduction for Miss B's own contribution which I will consider below).

Should Miss B bear any responsibility for her losses?

I've thought about whether Miss B should bear any responsibility for her loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

I recognise that, as a layperson who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Miss B was introduced to X through someone she knew online. And she read a positive article about it on gains customers were making, although I haven't seen this particular article as the link no longer works. I've also taken into account the provision of the trading platform (which, I understand, used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I can imagine this would have given some validation to the investment opportunity.

But other than reviewing the firm's website and the said article, Miss B doesn't appear to have done any other research into X. Having carried out a backdated search on the internet (to the time just prior to Miss B's payments), I can see several results on the first page itself which are quite concerning. For instance, there's an article about X being removed from a popular mobile app store just a month prior over concerns about it being a ponzi scheme. Another result links to a community forum on the topic of X being too good to be true, with several users posting comments about it being a pyramid or ponzi scheme and to steer clear of it.

This hearsay is not in itself sufficient evidence of fraud. But, considered in conjunction with what Miss B has said about what she was told about guaranteed returns, it may fairly and reasonably be regarded as circumstantial evidence that helps build an overall picture of scammers dishonestly seeking gains at the expense of others. I'm concerned by the promise of doubling investment in 29 days, and interest being compounded. Some of the articles I found from the time suggest X offered a daily return of between 2 and 4%. I think Miss B should have recognised that the returns being promised were simply too good to be true. I think this should, despite the overall plausibility of the scam, have put her on notice that the scheme might not be genuine.

Having carefully thought about this, I consider it would be fair for the reimbursement due to Miss B to be reduced 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 Miss B's money?

These were card payments to a cryptocurrency provider. Miss B sent that cryptocurrency to the scammer. So, Revolut wouldn't have been able to recover the funds.

In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the exchange provided cryptocurrency to Miss B, which she subsequently sent to the scammer.

So, I don't think Revolut should have done anything more to try and recover Miss B's money.

Customer service

I've also considered the service Revolut provided Miss B after she reported the scam. I've mentioned key events when setting out the background to this complaint. It's clear from those messages that she was quite frustrated with Revolut initially offering to arrange to speak to her about her claim, and arranging a time, to later not phoning her as agreed.

I appreciate that Revolut primarily corresponds with its customers through its in-app chat. But in this instance, it offered to phone Miss B on multiple occasions but then failed to deliver on its promise each time.

In that time, Miss B was left to worry about the outcome of the investigation, and later worry about Revolut not understanding her claim given she'd been told to select a chargeback reason which didn't apply to her circumstances.

I acknowledge that Revolut didn't know about Miss B's circumstances – particularly around her health – at the outset. But she did mention it a few times in her subsequent chat messages with Revolut's agents. While it's reasons for rejecting the chargeback wasn't incorrect, at a time when she was already feeling vulnerable as the victim of a scam, I think Revolut's refusal to provide the accessibility support that Miss B requested (which it initially offered) would have been even more upsetting for her.

Having reviewed the in-app messages and her concerns about how it handled the matter, I think that the poor customer service Revolut provided at such a critical time caused Miss B a lot of unnecessary worry and frustration. In recognition of this impact, I consider that Revolut should pay Miss B £150 for the distress and inconvenience caused."

I invited further comments from both parties before finalising my decision.

Miss B replied and said she should receive a full refund. In summary, she's said Revolut has a responsibility to protect consumers from scam. The fact that scammers directed her to use Revolut indicates a concerning lack of security and vigilance. Miss B states that had Revolut provided her with a warning from the outset, it may have prompted her to reconsider her actions and avoid sending the money. She also states that it's crucial that accounts are

made more accessible for individuals with disabilities, including the implementation of extra verification checks. Such measures would have supported her and reduced her vulnerability.

Revolut didn't respond by the deadline given. It has had a further two weeks to reply since then. I'm satisfied Revolut has had an opportunity to provide any final comments for my consideration and that it's now appropriate for me to progress matters to a final 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.

I thank Miss B for her comments which I've carefully considered. But they don't persuade me to change the outcome reached. This is because I've already considered and addressed most of the points raised in my provisional decision. In that decision, I set out in detail why I consider 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 also gave reasons for why I didn't consider the first nine payments to have appeared suspicious or unusual to Revolut such that I think it should have provided her a scam warning. A payment service provider's primary duty is to execute the customer's payment instruction. There's a balance to be struck between identifying payments that could potentially be fraudulent – and then responding appropriately to any concerns – and ensuring minimal disruption to legitimate payments. While I appreciate that Miss B feels Revolut ought to have provided her a warning from the outset, and that extra verification checks should be implemented, I remain satisfied that it didn't need to intervene until Payment 10.

In relation to the payments that I do think Revolut could have prevented, Miss B hasn't put forward any reasons for why she doesn't believe a deduction for contributory negligence should apply. So, I remain persuaded that Revolut can make a deduction of 50% when refunding Payments 10-12.

Putting things right

Revolut Ltd needs to refund Miss B Payments 10-12, making a 50% deduction for contributory negligence. It also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of refund.

Revolut Ltd also needs to pay Miss B £150 for the distress and inconvenience caused by its customer service failings.

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require Revolut Ltd to put things right for Miss B as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 27 November 2024.

Gagandeep Singh
Ombudsman