DRN-5577237

The complaint

Miss M is complaining that Revolut Ltd didn't do enough to prevent her from making payments to a scam, and didn't reimburse her after she reported the scam.

What happened

In 2023 Miss M fell victim to cryptocurrency investment scam. After clicking on an email link, Miss M was contacted by someone who claimed to be from an investment scheme. Miss M says she was persuaded to open a trading account by the scammer, who also told her to download an app which allowed him remote access to her mobile phone and desktop computer. The scammer told her to open a Revolut account, and an account with cryptocurrency exchange A, and to install the apps on her phone – which she did. She also shared her passport and driving licence details with the scammer.

The following payments were made to the scam, using Miss M's debit card. The payments were partly funded by two loans Miss M took out, which passed through her current account with her bank before being transferred to Revolut.

Payment number	Date of transaction	Payment destination	Amount
1	8 July 2023	Cryptocurrency exchange A	£950
2	8 July 2023	Cryptocurrency exchange A	£1,050
3	11 July 2023	Cryptocurrency exchange B	£10,000
4	11 July 2023	Cryptocurrency exchange B	£5,350
5	11 July 2023	Cryptocurrency exchange C	£4,650

Miss M says the scammer made the first two payments using the remote access they had to her device. After the first two payments were made, she could see a balance showing on the trading account. She then received two emails which she thought were from cryptocurrency exchange A and the Faster Payments service, which said she had to make further deposits to access the profits she'd made. The scammer told Miss M they would complete these deposits from her Revolut account and to facilitate this Miss M moved funds into her Revolut account from her bank account. Miss M says the scammer then went on to make payments 3 to 5 to cryptocurrency exchanges without her knowledge. Miss M says accounts in her name with these cryptocurrency exchanges had also been opened without her knowledge, using the identification details she'd shared with the scammer.

Miss M received an email asking for further funds on 13 July 2023 and said she became suspicious. She contacted Revolut via its in-app chat. Revolut investigated, but it concluded that Miss M had authorised the payments through its app. So, it didn't uphold her complaint.

When Revolut didn't uphold Miss M's complaint, she brought it to us. Our Investigator also didn't uphold her complaint. He thought that Miss M had authorised the payments to the scam. He thought Revolut should have done more to intervene, as it should have found the payments to be suspicious from payment 3. But he didn't think that would have uncovered the scam, because Miss M had said the scammer had told her to lie to her bank – and the Investigator thought Miss M wouldn't have been truthful with Revolut if it had intervened.

Miss M didn't agree. She reiterated that she hadn't authorised the payments to the scam, so she didn't think she should be held responsible for them.

Because Miss M didn't agree, the complaint was passed to me for review and a decision.

My provisional decision

I issued my provisional decision on 1 May 2025. This is what I said.

"*I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.*

Authorisation

The relevant law here is the Payment Services Regulations 2017 – these set out what is needed for a payment to be authorised and who has liability for disputed payments in different situations. With some exceptions, the starting point is that the consumer is responsible for authorised payments and the business is responsible for unauthorised payments. Miss M says she didn't authorise the payments, so I'll address this point first.

I've also taken into account the common law principle of apparent authority which protects the expectations of a third party who has reasonably relied on a representation by the principal that an agent has authority to act on their behalf.

The PSRs specify that authorisation depends on whether the payment transactions were authenticated correctly – and whether the account holder consented to them.

The PSRs go on to specify how consent is given. It must be in the form, and in accordance with the procedure, agreed between Miss M and Revolut. This will be laid out in the terms of Miss Ms's account. Broadly, in practical terms, that means Miss M consents to a payment if she completes the agreed payment steps. Or if someone else acts on her behalf and uses those agreed steps. If Miss M allowed someone else to use the payment steps, that individual would be treated as her agent and any payments they made would be considered authorised.

Miss M's explained that the scammer completed payments 1 and 2, with her knowledge. But she says payments 3 to 5 were completed without her knowledge. She says the scammer did this through the use of remote access software on her devices. She said she was unaware of the existence of the virtual debit card which was used to make the payments from Revolut to the cryptocurrency exchanges.

I'm conscious Miss M says she doesn't recall sharing her card details. But Revolut's app and desktop sites prevent access to sensitive information, including card details, via the remote access software the scammer was using, so it's difficult to see how the scammer could have

obtained these details if Miss M hadn't shared them herself.

Additionally, the card payments were authenticated via "3DS", which means they had to be approved in the app. Miss M says the scammer completed the steps to authenticate the payments in Revolut's app using remote access on her devices.

I've been provided with the screenshots to show what would have appeared in Revolut's app during the authentication steps. I can see that the screen would have displayed the name of the merchant and shown the payment amount. For the 3DS to be approved, it's likely they would have had to enter a passcode or use a biometric authentication to gain access to the app. So, I'm satisfied the payments were authenticated either by Miss M or someone to whom she gave the passcode to allow them to make payments. As such, I consider the card payments authorised.

Turning to the issue of consent, I'm satisfied Miss M consented to payments 1 and 2 as she says she was aware they were being made on her behalf, albeit by the scammer. Miss M has said she didn't make payments 3 to 5 herself and wasn't aware of them. But I'm satisfied that she was aware these payments were going to be made, because she took out loans and transferred the money from her bank account to Revolut in order to make them.

I understand Miss M thought the payments were being made to the companies that she thought had emailed her to ask for deposits to complete the withdrawals from her investment, rather than to the cryptocurrency exchanges they went to.

As, I've explained, a consumer can be bound by the acts of a third party which appear to have been made with the consumer's authority – this is called apparent authority. And I think that Miss M provided apparent authority to the scammer, by (most likely) sharing the details needed to allow him to complete the payment steps, either during their phone calls or by allowing the use of remote access to her devices to carry out the payments. So, even if she didn't know the true destination of the payments, they can be considered 'authorised.'

I would make it clear I understand the scammers gained this authority through deception. Overall, it appears to me Miss M likely completed steps, and shared details, to allow these payments to be made. So, it's reasonable to for Revolut to treat the payments as authorised.

Should Revolut have done anything else to prevent the payments to the scam?

I've concluded that the payments were authorised by Miss M, so I've gone on to consider if Revolut should have done anything else to prevent the payments she made to the scam.

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 M modified the starting position described in Philipp, by – among other things – expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks".

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

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

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

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

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

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

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

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

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

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

I am also mindful that:

- *Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].*
- *Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of 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 Code[3], 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*

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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 July 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.*

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

<u>Should Revolut have recognised that Miss M was at risk of financial harm from fraud?</u>

It isn't in dispute that Miss M has fallen victim to a cruel scam here.

Whilst I have set out the circumstances which led Miss M to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, 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 M might be the victim of a scam.

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 the payments would be credited to a cryptocurrency wallet held in Miss M's name.

By July 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. [4] And by July 2023, when these payments took place, further restrictions were in place.[5]

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.

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

To be clear, I'm not suggesting as Revolut argues that, as a general principle Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees.

As I've set out in some detail above, it is the specific risk associated with cryptocurrency in July 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 payments, in this case, going to an account held in Miss M's own name, should have led Revolut to believe there wasn't a risk of fraud.

---

[4] 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

[5] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

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

Miss M's account with Revolut had been opened as part of the scam, so it didn't have any account history to rely on to decide if the payments appeared unusual. Miss M had selected 17 reasons for opening the account – including making payments to cryptocurrency - so I don't think that information would have been particularly useful to Revolut in deciding whether the payments looked out of line with the account opening purpose.

I think Revolut should have identified that the payments 1 and 2 were going to a cryptocurrency provider but they were relatively low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

Payment 3 was also clearly going to a cryptocurrency provider and was significantly larger than the first two payments. Given the size of the payment, and what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Miss M 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 intervened before this payment went ahead.

To be clear, I do not suggest that Revolut should intervene in every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted an intervention.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. 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 July 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.

<u>What did Revolut do to warn Miss M and what kind of warning should Revolut have provided?</u>

Revolut has told us that it gave no warnings to Miss M, and didn't intervene in any other way.

Having thought carefully about the risk payment 3 presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Miss M's account. I think it should have done this by, for example, directing Miss M to its in-app chat to discuss the payment further.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Miss M suffered from payment 3?</u>

Had Miss M told Revolut that she was being asked to pay a deposit to a cryptocurrency exchange in order to access funds from a trading company she'd invested in, I think it would have been able to provide a clear warning that things were not as they appeared, and her loss would have been prevented. So, I've considered whether Miss M would have revealed the circumstances in which the payments were being made.

Given Miss M has told us the scammer was in control of her devices, there is a question mark around whether she would have seen and engaged with an intervention from Revolut. But as I've mentioned, I do think it's likely Miss M did retain control of her phone in order to complete the 3DS authentication of the payments. Any intervention from Revolut would have taken place within its-app chat, and I'm aware that from June 2023, Revolut's systems would have shown a blank screen instead of the in-app chat if remote access software was detected. So, I think it's unlikely the scammer would, for example, have been able to conduct the chat through remote access without Miss M's knowledge, or to have seen the chat via remote access in order to guide her through it.

Miss M has also told us that she wasn't told by the scammer to lie to Revolut if it had intervened – but she says the scammer told her to say the funds were for personal use if her bank contacted her about the payments when they were made to Revolut. And when Miss M's bank did intervene, she said the funds were for spending. I've listened to this call and there's no evidence of active guidance taking place at the time of the call, Miss M is confident in her answers and there's no hesitation which would suggest she's being told what to say by a third party.

I've thought carefully about what this means for any intervention Revolut may have carried out. I've reviewed the messages between Miss M and the scammer, and I can't see that she was given a cover story which would have been likely to have satisfied Revolut that she wasn't at risk of a scam had it intervened and asked her some questions about payment 3, but I also accept that because there was no real scrutiny of the transactions by Revolut, this may not have been required.

But ultimately, Revolut didn't question the payment. And I don't think there's compelling evidence that Miss M would have misled it about the purpose of the payments or the surrounding circumstances. I think if she had said the payments to cryptocurrency were for personal use, Revolut would have asked some probing questions about what the circumstances of the payments were which Miss M would have answered honestly. And I think Revolut could then have provided a very clear warning setting out the key features of cryptocurrency investment scams, such as the use of remote access, the existence of a convincing looking trading platform showing profits, and being encouraged to buy cryptocurrency to invest in the scheme. I think, on the balance of probabilities, such a warning would have resonated with Miss M, and further payments to the scam would have been prevented.

<u>Is it fair and reasonable for Revolut to be held responsible for Miss M's loss?</u>

In reaching my decision about what is fair and reasonable, I have taken into account that Miss M purchased cryptocurrency which credited a cryptocurrency wallet held in her own name, rather than making a payment directly to the scammer. So, there were further steps after the money leaving Revolut before it was lost.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss M might have been at risk of financial harm from fraud when she made payment 3 and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Miss M suffered. The fact that the money used to fund the scam came from elsewhere, and that it wasn't lost

at the point it was paid to the cryptocurrency exchange, does not alter that fact and I think Revolut can fairly be held responsible for Miss M's loss in such circumstances.

I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Miss M has only complained against Revolut. We know that Miss M's bank did intervene here when she transferred funds to Revolut from it, but she's not brought a complaint about her bank. 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 M could instead, or in addition, have sought to complain against those firms. But Miss M has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Miss M's compensation in circumstances where: she has only complained about one respondent from which she is entitled to recover her 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 M's loss from Payment 3 (subject to a deduction for Miss M's own contribution which I will consider below).

Should Miss M bear any responsibility for her losses?

So, the point that remains for me to decide here is whether Miss M should share responsibility for her loss under the principle of contributory negligence – that is, because her actions fell short of the standard of care that would be expected of a reasonable person in these circumstances.

I can understand how, at the outset, the investment scheme may have appeared legitimate - we know that these types of investment scams can be very sophisticated.

However, as Miss M's communications with the scammer went on, I think she should have started to have concerns about what he was asking her to do. For example, Miss M agreed quite early on in the communications with the scammer to allow remote access to her phone and to her desktop computer. I think giving a third party remote access to her devices showed that Miss M didn't exercise a reasonable degree of caution, because I think she should have had some concerns about why she was being asked to do this.

Miss M agreed, to some extent, to be guided by the scammer when speaking to her bank about making payments to Revolut, and I've not seen that the scammer gave her a plausible reason for why she shouldn't be open and honest with her bank about what she was doing, if the scheme she was investing in was genuine. So, I think this was also something that Miss M ought reasonably to have had some concerns about.

Miss M also took out two loans to pay the deposits she'd been asked for in order to access her funds – and she says she was encouraged to do so by the scammer. But when Miss M was still unable to withdraw from the scheme after the first deposit I'd have expected her to have had some questions and concerns about why a second deposit was needed before taking out another loan.

Miss M hasn't said whether she carried out any online investigation into the scheme before she started to invest. That said, I don't think she was obliged to carry out due diligence before investing and in the circumstances here, this in itself isn't sufficient reason to conclude she acted negligently. But given the concerns I've identified, I'd have expected her to have become more concerned about the legitimacy of the investment as time went on, and certainly by the time she made payment 3 - which should reasonably have prompted her to do some more research into the investment company. And if Miss M had have done some research, I can see there was quite a lot of information online at the time to suggest that this particular company may not be legitimate. So, I think if Miss M had carried out this research, the payments from payment 3 could have been prevented.

I do not think however, that the deduction made to the amount reimbursed to Miss M should be greater than 50% taking into account all the circumstances of this case. I recognise that Miss M did have a role to play in what happened, and it could be argued that she should have had greater awareness than she did that there may be something suspicious about the scam. But I have to balance that against the role that Revolut, an EMI subject to a range of regulatory and other standards, played in failing to intervene. Miss M was taken in by a cruel scam – she was tricked into a course of action by a fraudster and her actions must be seen in that light. I do not think it would be fair to suggest that she is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that she was at financial harm from fraud, and given the extent to which I am satisfied that a business in Revolut's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circumstances of the complaint.

I'm sorry to learn of the difficult circumstances Miss M was experiencing at the time of the scam, and I thank her for sharing them with us. But taking everything into account, I think it's fair for her to share liability for her loss with Revolut, to reflect the role she played in what happened here. And on balance, I consider a 50% deduction is fair and reasonable in all the circumstances of this case.

Could Revolut have done anything to recover the payments once the scam was reported?

These payments were made by card to a cryptocurrency provider, which was then sent on to the scam. So, Revolut would not have been able to recover the funds. And I don't consider that any chargeback claim would have had any prospect of success, as it's not in dispute that Miss M received the cryptocurrency she'd paid for, which she subsequently sent on to the scam.

Putting things right

I think Revolut should have intervened at payment 3, and if it had done so further payments to the scam would have been prevented.

So, to put things right, Revolut should refund 50% of payments 3 to 5 to Miss M, which I've calculated to be £10,000.

I've considered the loans Miss M took out here, and how they affect appropriate redress. As far as I can see from the most recent information Miss M has provided about her loans, she is still repaying one of the loans in line with her loan agreement. Miss M defaulted on the other loan in May 2024 and as such it doesn't appear interest is still being applied, but I've not seen anything to show that the outstanding balance has been reduced or otherwise written off, and Miss M was initially being charged interest on this loan at a very high rate. Overall, I think our usual approach of applying 8% simple interest for loss of use of funds,

from the date of the payment to the date of settlement, will result in broadly a fair outcome here.

My provisional decision is that I uphold this complaint in part. To put things right, Revolut Ltd should:

- *Refund £10,000 to Miss M, being 50% of payments 3, 4 and 5; and*

- *Pay interest on this amount at 8% simple per year from the date of the payment to the date of settlement (less any tax lawfully deductible.)"*

I asked Revolut and Miss M to reply by 19 May 2025 with anything else they wished to add.

Revolut said it had received my provisional decision, but it didn't reply with anything else it wished to add by the deadline.

Miss M replied to say, in summary:

- She only has a basic understanding of how to use computers and she assumed this was the reason the scammer asked for access to her computer and phone, and why she granted it;

- An investment savvy person would have researched the company before investing – but Miss M wasn't investment savvy and the whole fraud happened over a period of four days. She was under constant pressure and it was unlikely a reasonable person would have conducted research;

- The scammer told Miss M the banks were stopping people investing in cryptocurrency, so she should say it is for her personal use;

- Miss M didn't have control of the cryptocurrency accounts and wallets; and

- Miss M had been deceived and directed by the scammer and didn't have the requisite investment or computer knowledge to challenge him.

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 have considered what Miss M has said in response to my provisional decision, in relation to whether she should bear any responsibility for her losses. And what she's said doesn't change my decision. I'll explain why.

I appreciate that the payments to the scam took place over a relatively short period of time, and that Miss M was under pressure from the scammer. But even so, I think there would have been adequate time for Miss M to have looked further into what she was being asked to do here before making Payment 3. I don't think Miss M not being an experienced investor, or being experienced with computers, changes the fact that she could have completed a quick search of the company name to see what she was being guided to invest in in the time she had between Payments 1 and 2 and Payment 3. And even if Miss M didn't know much about computers, I think a third party asking to have access to her devices is still a red flag to be concerned about.

Miss M's told us that the scammer told her that the banks were stopping people investing in cryptocurrency – but I don't think this was necessarily a plausible reason to justify why she should not give accurate information to her bank. And I also think this could also reasonably have prompted further questions and concerns for Miss M about why this would be the case.

I've explained in my provisional decision why I don't think that Miss M was so under the spell of the scammer that an in-app chat intervention from Revolut *wouldn't* have prevented her from making the payments. I've thought about this point again in light of Miss M's response to my provisional decision, which does imply that she was being directed by the scammer, to see if that changes my overall decision.

But I'm also taking into account that it remains the case I've seen no evidence Miss M was given a cover story which would have stood up to probing questions from Revolut about why she was making substantial payments to cryptocurrency. I still think Miss M's lack of understanding about what she was investing in, and why, would have become apparent in an in-app intervention and would have led to the scam being uncovered, as I've explained. So, I'm not changing my decision on this point.

I'm sorry to disappoint Miss M – I do appreciate that she's been the victim of a scam and she'd like all her money to be returned. But I'm satisfied that the overall decision I've reached here is fair and reasonable, in all the circumstances.

My final decision

My final decision is that I uphold this complaint in part. To put things right, Revolut Ltd should:

- Refund £10,000 to Miss M, being 50% of payments 3, 4 and 5; and

- Pay interest on this amount at 8% simple per year from the date of the payment to the date of settlement (less any tax lawfully deductible.)

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 25 June 2025.

Helen Sutcliffe
Ombudsman