DRN-5334094

The complaint

Miss A has complained that Revolut Ltd ("Revolut") failed to protect her from falling victim to a scam.

What happened

I issued my provisional decision ("PD") in January 2025 explaining why I was minded to uphold Miss A's complaint. I gave both parties the opportunity to respond before making my final decision. Neither Miss A or Revolut responded by the deadline of 10 February 2025, nor had they responded by the time of writing this final decision.

I've included an extract of my PD below.

> **What happened**
>
> The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.
>
> Miss A has complained that she transferred £6,513 to an unknown party that she believed had offered her a task-based employment opportunity, in which she'd have to complete 40 "missions" per week in return for a salary of £35-£45 per hour, or £1,500 - £2,000 per week. She's explained that she was looking for a job at the time, so when she received a message allegedly from a well-known recruitment agency offering her the role, it didn't appear suspicious.
>
> Miss A explains that as the conversation with the scammer continued, she was pressured into purchasing cryptocurrency as an investment, and she was given access to what she now realises was a fraudulent website, allegedly showing the performance of her investments. She says she was constantly pressured to make further deposits, and to recruit other people to invest, and the scam was brought to a halt when her sister realised what was happening. She's explained that although the scam started as what appeared to be an employment opportunity and became an investment, she still thought she could make money so she continued.
>
> Miss A has also explained she was added to a group chat where other alleged investors discussed their investments, to give the impression that the investment was legitimate.
>
> The payments relevant to this scam are as follows:

	Date	Payment type	Amount
1	24 May 2023	Transfer to beneficiary 1	£20
2	25 May 2023	Transfer to beneficiary 1	£10
3	25 May 2023	Transfer to beneficiary 2	£75
4	25 May 2023	Transfer to beneficiary 3	£135
5	25 May 2023	Transfer to beneficiary 1	£562
6	25 May 2023	Debit card payment to crypto exchange	£1,030
7	26 May 2023	Debit card payment to crypto exchange	£1,262
8	26 May 2023	Debit card payment to crypto exchange	£2,000
9	26 May 2023	Transfer to beneficiary 2	£619
10	26 May 2023	Transfer to beneficiary 1	£800
-	11 July 2023	Fraud refund from Revolut	£64.62+
		Remaining loss	**£6,448.38**

Miss A says that as soon as she discovered she'd been scammed she reported it to the relevant authorities, as well as to Revolut. Revolut didn't refund what Miss A had lost, and it rejected her request to raise chargebacks for the debit card payments as it said it hadn't found evidence of fraudulent activity. It also said the debit card payments had been authorised using the Revolut app on Miss A's mobile phone.

Miss A made a complaint to Revolut. Revolut didn't uphold the complaint and in its response it said that it didn't have chargeback rights for the debit card payments, as they fell under the fraud chargeback category but Revolut had established that they weren't fraudulent. In relation to the mobile payments, Revolut said that it had shown Miss A a message related to the purpose of one of the payments, although it didn't specify which one. It also said it showed Miss A a series of educational screens related to a certain type of scam, although it again didn't specify which type. Revolut confirmed in the same letter that it had been able to recover £64.62 from one of the beneficiaries' accounts, which it credited to Miss A's Revolut account.

Miss A remained unhappy so she referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. He explained that there was no interaction between Miss A and Revolut at the time any of the payments were made, so there's no reason Revolut should've been suspicious of them, or on notice that Miss A might've been the victim of a scam. He also explained that although the payments weren't particularly large, Revolut showed a generic warning urging Miss A to ensure she was confident that she was making a payment to someone she knew and trusted. Finally, he didn't think the scam was particularly convincing, so he thought Miss A ought to have been more wary about who she was sending money to before making the payments.

As Miss A didn't accept the investigator's opinion, the case has been passed to me to make a decision.

What I've provisionally 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.

Having considered everything I'm currently intending to reach a different outcome to our investigator. I'll explain why.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Miss A authorised these payments from leaving her account. It's accepted by all parties that Miss A gave the instructions to Revolut and Revolut made the payments in line with those instructions, and in line with the terms and conditions of Miss A's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

I'd firstly like to say that having reviewed the chat transcripts between Miss A and the scammer I can understand how hard it must've been to deal with this situation. Not only did the scammer demand money, but unreasonable videos from Miss A, supposedly in return for allowing her to withdraw funds from what she'd earned.

Having reviewed the first seven payments Miss A made as part of this scam, I'm not persuaded that Revolut ought to have been on notice that they might've posed a risk to Miss A.

I say this because firstly, the values of the transactions are fairly modest, and not out of character when viewed alongside the other transactions on Miss A's account in the preceding months. Although there's a slight difference from her usual activity in that the majority were made as transfers, as opposed to Miss A's usual activity of primarily making debit card payments, I don't think Revolut ought to have deemed that as suspicious in itself.

I'm also mindful that by the time Miss A made slightly larger payments as part of the scam, in particular payments five, six and seven, Miss A had previously paid the same payees before. Whilst I understand this was likely a deliberate act by the scammers to circumvent any fraud detection systems, it does unfortunately mean that it's unlikely they'd have appeared suspicious, or would've at least appeared less suspicious, to Revolut. Finally, even when considering the cumulative values of the transactions Miss A made, although significant to Miss A, they were still fairly low in value when considering the broader landscape of payments Revolut processes, and for that reason, the general level of risk they presented.

With this in mind I don't think Revolut ought to have intervened when Miss A made the first seven transactions.

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 Miss A'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 A modified the starting position described in *Philipp,* by – among other things – expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*" (section 20).

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

Revolut says that all three of the debit card payments were verified using 3D Secure, or 3DS, which is an additional layer of security to prevent unauthorised payments. Whilst I accept this point, I haven't considered it any further, because there's no question that the payments were authorised by Miss A.

However I've considered whether – regardless of whether the card payments were authorised or not – Revolut ought to have realised they presented a risk of financial harm to Miss A. And if so, how it ought to have dealt with that risk.

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's fair and reasonable on the basis set out at DISP 3.6.4R, I consider that by May 2023 Revolut should've been on the lookout 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 lookout for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMIs like Revolut did in fact seek to take those steps, often by:

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

[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_/

- 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 May 2023, if it identified a scam risk associated with a card payment through its automated systems, Revolut 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'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)[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 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

[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"

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, regulator's 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 May 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 Miss As) and the different risks these can present to Miss As, 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 May 2023, Revolut should in any event have taken these steps.

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

Whilst I have set out in this decision the circumstances which led Miss A 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 less information available to it upon which to discern whether any of the payments presented an increased risk that Miss A might be the victim of a scam. That said, I think Revolut could and should have identified that the debit card payments were going to a cryptocurrency provider, as the merchant is well-known and the merchant category code (MCC) would've given Revolut and indication of this.

From January 2023 we expect that all firms ought to have been able to recognise that cryptocurrency-related transactions carried an elevated risk of the likelihood of the transaction being related to a fraud or scam. And by 1 January 2023, many leading firms had appreciated this risk and placed blocks or restrictions on cryptocurrency related transactions, and there had been widespread coverage in the media about the increase in losses to cryptocurrency scams, as well as regulator's warnings about the risks of cryptocurrency scams.

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 A's name. But by May 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 customers' ability to purchase cryptocurrency using their bank accounts, or had increased friction in relation to cryptocurrency-related payments, owing to the elevated risk associated with such transactions.

I don't think that Revolut ought to have warned Miss A or declined the first two debit card payments that she made. Although it was clear they were being made to a cryptocurrency platform, they were for fairly modest values, and I don't think Revolut would've had sufficient grounds to decline them based on that alone. I've therefore gone on to consider the position in relation to payment three, which was made to the same cryptocurrency platform.

Payment three was larger than the previous two card payments and was made on the same day as payment two. Whilst the individual values of both of those payments weren't particularly remarkable, the cumulative value by the time payment three was made ought to have roused Revolut's suspicion that Miss A might've been at risk of harm. The total value of the two payments, on the same day, was over £3,200 and as such I think Revolut ought to have taken steps to give Miss A a warning, tackling some of the key features relevant to cryptocurrency scams, before allowing the third payment to be made.

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). 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, and as is the case here.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Miss A made in May 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 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 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've 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 that the payments in this case were going to a cryptocurrency account held in Miss A's own name should have led Revolut to believe there wasn't a risk of fraud.

As I've already set out I'm also not suggesting that Revolut should provide a warning or an intervention for *every* payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of the third debit card payment which ought to have prompted a warning.

Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes, but would reduce the risk of financial harm from fraud and scams.

What did Revolut do to warn Miss A?

Revolut says that when Miss A created the new payees before making the payments, it gave her a general warning asking her to confirm that she knew the person she was paying and that she accepted the risks of sending funds to unknown individuals. IT also says that before she made the transfers it showed a warning screen which included the following: "Do you know and trust this payee? If you're unsure, don t pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment."

Revolut also says that for two of the payments – although it hasn't specific which two – it gave Miss A more specific warnings related to the payment purpose she'd selected, which was "something else". It has provided a copy of a series of educational warning screens that it says it showed.

The first screen shows a warning stating "This transfer could be a scam", to which Miss A would've had to select "Continue anyway" in order for the payments to proceed. The next screen is titled "Victims lose millions every year" and gives some further details about scam trends, and the following screen is titled "Fraudsters are professionals" and it gives some information on how fraudsters make their victims believe they are trustworthy.

Revolut says that authenticated the debit card payments using the 3D Secure system, but it didn't issue any scam-related warnings before any of them.

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

Taking that into account, in line with what I consider to have been good industry practice at the time, as well as what I consider to be fair and reasonable, Revolut ought to have provided a written warning which covered the key scam features of the payment in question, when Miss A made payment eight.

As the payments were being made to an identifiable cryptocurrency provider Revolut 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, promoted by a celebrity or public figure; 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 the features of either employment scams or cryptocurrency investment scams, both of which feature in Miss A's scenario. But I think a warning covering the key features of cryptocurrency investment scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented, would have been a proportionate and reasonable way for Revolut to have acted at the time these payments were made, to minimise the risk of financial harm to Miss A.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss A suffered from the third payment?

The circumstances of Miss A's case had many features that are common to both investment and employment scams. Miss A had been contacted out-of-the-blue by an alleged recruiter offering her work, and she'd been told to complete a set number of tasks in return for commission, whilst also making payments in order to earn that commission.

It's also clear she was persuaded to start by investing small amounts, and she's described how she was pressured to make further deposits into her alleged 'investment' and encouraged to recruit further investors into the scheme. All of these features are well-known traits of scams and, had Revolut told Miss A about that as party of a cryptocurrency investment warning, it would likely have resonated with her and prevented her from making the payments that were ultimately made.

I haven't seen anything to suggest that Miss A wouldn't have been receptive to a warning that bore resemblance to the features of the scam she was falling victim to, so I'm satisfied the losses would likely have been prevented if Revolut intervened before Miss A made payment eight.

As I think the scam would've been uncovered at that point, I also think Revolut could've prevented final two bank transfers Miss A made (payments nine and ten). Although they were made in a different way, had Revolut intervened and uncovered the scam when it should have, those payments also wouldn't have been made.

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

In reaching my decision about what's fair and reasonable, I have taken into account that Miss A funded her Revolut account using other accounts, and Revolut wasn't the point of ultimate loss – that happened when Miss A transferred the funds from her cryptocurrency account to the scammers.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss A might have been at risk of financial harm from fraud when she made payment eight, and in those circumstances it should have given a written warning covering the common features of cryptocurrency investment scams before allowing the payment to be made.

If Revolut had taken those steps, I am satisfied it would have prevented the losses Miss A 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 A's own account elsewhere doesn't alter that fact and I think Revolut can fairly be held responsible for Miss A'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 A has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Miss A could instead, or in addition,

have sought to complain against those firms. But Miss A has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Miss A's loss from the third debit card payment, subject to a deduction for Miss A's own contribution which I will consider below.

Should Miss A bear any responsibility for her losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I think that, as a layman with little investment experience, there were several features of the
scam that would have appeared convincing. Miss A was given access to an online investment platform, that a reasonable person might expect to be vetted in some way. And, while I haven't seen the specific investment platform Miss A used, I've seen many similar ones and they can appear to be very convincing.

But I do think that Miss A should have been more sceptical of both the employment offer and the investment opportunity at the time. I say this because she was contacted out of the blue, and she was told she'd need to pay to earn money in return, which isn't a realistic situation. I'm also not aware that Miss A received any correspondence or documentation in relation to either the alleged job opportunity or the investment, so this should've also been a cause for concern.

Finally, I'm mindful that Miss A was told she could earn salary of £35-£45 per hour, or £1,500 - £2,000 per week. This seems to be an unreasonably high offer for a job with no recruitment process, nor specialist knowledge required, so I again think this ought to have led Miss A to consider the legitimacy of what she was being told, or whether it was too good to be true.

With the above in mind and having considered the matter carefully, I think it's fair for the responsibility of Miss A's losses to be shared equally between Revolut and Miss A.

Recovery of the funds

As Miss A used her debit card for some of the payments that were part of the scam, the chargeback process is relevant to them. The chargeback scheme is a voluntary agreement between card providers and card issuers who set the scheme rules and is not enforced by law.

A chargeback isn't guaranteed to result in a refund, there needs to be a right to a chargeback under the scheme rules and under those rules the merchant or merchant acquirer can defend a chargeback if it doesn't agree with the request. Unfortunately, the chargeback rules don't cover scams.

I'd only expect Revolut to raise a chargeback if it was likely to be successful, but based

on the available evidence this doesn't look like a claim that would have been successful. Miss A paid a legitimate cryptocurrency exchange, and in return she received a service from
the cryptocurrency exchange whereby it exchanged her money into cryptocurrency, before Miss A sent it to the wallet address provided by the scammer.

Considering this, the cryptocurrency exchange provided the service it should have by providing the cryptocurrency, so Miss A's disagreement is with the scammer, not the cryptocurrency exchange. So Revolut was right to say it didn't have chargeback rights against the cryptocurrency exchange for these transactions. Revolut was also right to say that it didn't have chargeback rights under the fraud category – as those rights only apply where a third party makes unauthorised transactions without the cardholder's knowledge or consent, and that's not what happened in this case.

With regard to the other transactions, which were sent as electronic payments, I've seen evidence that Revolut attempted to recover them from the beneficiaries' accounts when Miss A made it aware of the scam. Revolut was able to recover £64.62 from the account of the recipient paid at payment ten, referred to as "Beneficiary 1" above, which it returned to Miss A, but it was told that no funds remained in the other recipients' accounts. Whilst this is disappointing, there's nothing more Revolut could've done here.

What I've decided – and why

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

As I've not received any comments or information to change my decision, I see no reason to depart from my provisional conclusions.

It therefore follows that I uphold Miss A's complaint for the reasons outlined in my provisional decision, which forms part of this final decision.

Putting things right

To put things right I require Revolut to:

- Refund 50% of Miss A's losses from (and including) payment eight, minus the £64.62 it has already returned and;
- Pay 8% simple interest on each amount, from the date each payment left Miss A's account until the date of settlement*.

*If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Miss A how much it's taken off. It should also give Miss A a tax deduction certificate if she asks for one.

My final decision

I uphold Miss A's complaint against Revolut Ltd and require it to put things right as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss A to accept or reject my decision before 17 March 2025.

Sam Wade
Ombudsman