DRN-5601170

The complaint

Miss A is complaining that Revolut Ltd didn't do enough to prevent her from making payments to a scam.

The complaint is brought on her behalf by a professional representative.

What happened

The circumstances of the complaint are well-known to both parties so I won't repeat them in detail here.

In short, in August 2023 Miss A fell victim to an employment scam after receiving a message about a job opportunity. As part of the scam she made the following payments to a cryptocurrency exchange, using her debit card (I've excluded a payment of £0.10 which was later refunded).

Payment number	Date of transaction	Amount
1	14 August 2023	£82.30
2	15 August 2023	£216.64
3	15 August 2023	£82.79
4	16 August 2023	£830.34
5	16 August 2023	£3,331.74
6	23 August 2023	£1,544.86

The order of Payments 1 to 4 differs from that set out in the Investigator's view as this was completed before we received details of the timings of the payments from Revolut, but this doesn't change the outcome of the complaint.

When Miss A was unable to withdraw any funds, she realised she'd been scammed. On 26 August 2023 she contacted Revolut to report the scam.

Revolut didn't refund the payments Miss A made, so she raised a complaint – and when Revolut didn't change its decision she brought the complaint to the Financial Ombudsman.

Our Investigator thought Miss A's complaint should be upheld. He thought Revolut ought to have intervened to warn Miss A about the scam when she made Payment 5. He asked Revolut to refund Payments 5 and 6 to Miss A – but with a 50% reduction to reflect Miss A's contribution to her loss.

Miss A accepted the Investigator's view. But Revolut didn't agree with the Investigator's view and asked for an Ombudsman to review Miss A's complaint. The complaint's now been passed to me for review and a 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.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Miss A modified the starting position described in *Philipp,* by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with Miss A and the Payment Services Regulations to carry out their 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 am 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 August 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 to 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 have 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 am 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 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 August 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 EMIs 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.

For example, it is my understanding that in August 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).

[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_/

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).
- 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 *"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[2], 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 Duty[3], 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 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

[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.

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

involving cryptocurrency[5] 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 August 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, 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 August 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?

It isn't in dispute that Miss A has fallen victim to a cruel scam here, nor that she authorised

[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.

the payments she made to a cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

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 much 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.

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.

By August 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.[6]

And by August 2023, when these payments took place, further restrictions were in place.[7]

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). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Miss A made in August 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.

---

[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

To be clear, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), 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 August 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 (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Miss A'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 A might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that Payments 1 to 4 were going to cryptocurrency providers, but they were relatively low in value, and I don't think Revolut should reasonably have suspected until Payment 5 that they might be part of a scam. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of these payments, I don't think Revolut ought to have been sufficiently concerned about them that it would be fair and reasonable to expect it to have provided warnings to Miss A at this point.

Payment 5 was also clearly going to a cryptocurrency provider. But its value was around four times higher than the largest of the previous payments Miss A had made to the cryptocurrency exchange as part of the scam.

At this point, looking at the frequency and escalation in value of the payments Miss A was making to cryptocurrency, I think a pattern was developing that should have caused Revolut to consider that Miss A was at heightened risk of financial farm from fraud. In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Miss A before this payment went ahead.

I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. 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 a warning.

For the reasons I've set out above I'm satisfied that by August 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud.

Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What kind of warning should Revolut have provided?

Looking at everything Revolut have said and provided, I can't see that it provided Miss A with any meaningful scam warning on any of the disputed payments.

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 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 August 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.

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 that by August 2023, on identifying a heightened scam risk, a firm such as Revolut should 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 5 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 am satisfied that, by August 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Miss A made Payment 5 Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Miss A was at risk from.

In this case, Miss A was falling victim to a 'job scam' – she believed she was making payments in order to receive an income.

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 A gave. I'd expect any such warning to have covered off key features of such a scam, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Miss A wouldn't have done so here.

I accept that there are a wide range of scams that could involve payments to cryptocurrency providers. I am also mindful that those scams will inevitably evolve over time (including in response to fraud prevention measures implemented by banks and EMI's), creating ongoing challenges for banks and EMI's.

In finding Revolut should have identified that Payment 5 presented a potential scam risk and that it ought to have taken steps to narrow down the nature of that risk, I do not suggest Revolut would, or should, have been able to identify every conceivable or possible type of scam that might impact its customers. I accept there may be scams which, due to their unusual nature, would not be easily identifiable through systems or processes designed to identify, as far as possible, the actual scam that might be taking place and then to provide tailored effective warnings relevant to that scam.

But I am not persuaded that 'job scams' would have been disproportionately difficult to identify through a series of automated questions (as demonstrated by Revolut's current warnings – which seek to do exactly that) or were not sufficiently prevalent at the time that it would be unreasonable for Revolut to have provided warnings about them, for example through an automated system.

I accept that under the relevant card scheme rules Revolut cannot delay a card payment, but in the circumstances of this case, I think it is fair and reasonable to conclude that Revolut ought to have initially declined Payment 5 in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Miss A attempted the payment again, should Revolut have made the payment.

I understand that Revolut did have systems in place by August 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time.

If *Revolut had provided a warning of the type described, would that have prevented the losses Miss A suffered from Payment 5?*

I think that a warning of the type I've described would have identified that Miss A's circumstances matched an increasingly common type of scam.

I've read the instant message conversation between Miss A and the fraudsters. I can see that before making Payment 5 Miss A appeared to have some concerns and doubts about the scheme but was persuaded to continue by the scammer. I think this indicates that it wouldn't have taken much persuasion (that a warning could have provided) to convince her that she was falling victim to a scam prior to making Payment 5.

I would add that the Investigator has contacted the businesses Miss A sent the funds to Revolut from, and they've told him they don't have a record of giving Miss A tailored scam warnings about any of the payments she made which were subsequently paid to the scam through her Revolut account.

Overall, I think that a warning provided by Revolut would have given the perspective Miss A needed, reinforcing her own concerns and she would more likely than not have concluded that the scheme was not genuine. In those circumstances I think, she's likely to have decided not to go ahead with Payments 5 and 6 had such a warning been given.

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

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision about what is fair and reasonable, I have taken into account that Miss A purchased cryptocurrency which would have credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

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 5 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 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 does not 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 Miss A'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 Payment 5 (subject to a deduction for Miss A's own contribution which I will consider below).

Should Miss A bear any responsibility for her losses?

I've thought about whether Miss A 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.

Miss A has accepted the Investigator's view on this point, so I won't go into great detail here.

But, I agree with the Investigator that there were some suspect elements to the scam that ought fairly and reasonably to have led Miss A to question the legitimacy of the job opportunity (although I appreciate some aspects of it may have looked sophisticated).

Miss A was approached out of the blue through receiving a message, and was offered a job opportunity which was apparently very highly paid for the amount of time and level of skill required, which didn't appear very plausible. As the Investigator's explained, she didn't receive an employment contract or any other paperwork. It would also be very unusual for a legitimate job opportunity to involve making payments to an employer, through cryptocurrency. And from her conversation with the scammer it does appear Miss A did rightly have some concerns about being asked to deposit more funds before she could make a withdrawal before she made Payment 5, but went ahead anyway. In these circumstances it would not be fair to require Revolut to compensate her for the full amount of her losses.

On balance, I think it's fair to reduce the amount Revolut pays Miss A because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

I do not think that the deduction made to the amount reimbursed to Miss A should be greater than 50% taking into account all the circumstances of this case. I recognise that Miss A 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 job 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 A 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.

Recovery of the funds

The payments were made by card to a cryptocurrency provider and Miss A sent that cryptocurrency to the scam. So, Revolut would not 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 cryptocurrency provider did provide cryptocurrency to Miss A which she subsequently sent to the scam.

My final decision

For the reasons given above, I uphold this complaint in part and require Revolut Ltd to pay Miss A:

• 50% of Payments 5 and 6 – which I've calculated to be £2,438.30; and

• 8% simple interest per annum from the date of the payments to the date of settlement (less any tax lawfully deductible) to reflect Miss A's loss of use of the funds.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss A to accept or reject my decision before 15 July 2025.

Helen Sutcliffe
Ombudsman