DRN-4443022

The complaint

Ms N has complained about Revolut Ltd not refunding several payments she says she made and lost to a scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. In summary, Ms N fell victim to a fake job scam after she was contacted on a messaging app by a scammer. The scammer told Ms N that she would be paid for completing a number of tasks, but she would also have to pay in funds to the task platform periodically, using cryptocurrency via an exchange I will call 'B', to unlock more tasks and to receive her payment. She was initially able to withdraw circa £14 as part of the demonstration by the scammer on 24 April 2023. The scammer also appears to have 'loaned' Ms N 50 USDT during the scam. After using her own funds, Ms N borrowed money from her sister without telling her what she was using it for. Ms N realised she had been scammed when the scammer continued to pressure her to pay more, without allowing her to withdraw any funds.

The relevant transaction history from Ms N's account statements are as follows:

Transaction	Date	Time	Type of Transaction	Amount
1	24 April 2023	20:18:25	Debit card payment to B	£50
2	25 April 2023	09:13:58	Debit card payment to B	£64.03
3	25 April 2023	10:01:20	Debit card payment to B	£40.31
4	26 April 2023	11:25:55	Debit card payment to B	£250
5	26 April 2023	12:15.22	Debit card payment to B	£190
6	26 April 2023	12:29:52	Debit card payment to B	£50
7	27 April 2023	09:40:23	Debit card payment to B	£200
8	27 April 2023	09:59:34	Debit card payment to B	£300
9	27 April 2023	10:01:45	Debit card payment to B	£50
10	27 April 2023	10:17:32	Debit card payment to B	£624.48
11	27 April 2023	10:28:56	Debit card payment to B	£1,060
12	27 April 2023	11:55:04	Debit card payment to B	£2,691
13	27 April 2023	12:10:09	Debit card payment to B	£25
14	27 April 2023	14:15:25	Debit card payment to B	£5,000
15	27 April 2023	14:21:44	Debit card payment to B	£970

Revolut didn't reimburse Ms N's lost funds and so she referred her complaint to us. Our Investigator looked into things and recommended the complaint be upheld. They weren't persuaded, on balance, that Revolut did enough to prevent Ms N from falling victim to the scam. Our Investigator thought Revolut should have intervened during payment 12 as, amongst other things, it ought to have known the payment was going to a cryptocurrency provider, which carried a higher risk of being associated with fraud. Our Investigator believed

Revolut should have provided Ms N with a warning that was specific to the main cryptocurrency scam risk at the time, cryptocurrency investment scams.

However, Revolut disagreed and in summary responded saying:

- It has no legal duty to detect and prevent all fraud.
- It must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the commercial wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25.
- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment ("APP") fraud. By suggesting that it does need to reimburse customers, it says our service is erring in law.
- Our service appears to be treating Revolut as if it were a signatory to the Contingent Reimbursement Model code.

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.

Earlier on this month I issued a provisional decision in which I said the following:

> *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 Ms N 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 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 April 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]
- *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 April 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated

[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_/

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 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.*

---

[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"

- *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 April 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 April 2023, Revolut should in any event have taken these steps.

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

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

Whilst I have set out in detail in this decision the circumstances which led Ms N 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 Ms N might be the victim of a scam.

I'm aware that cryptocurrency exchanges like B 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 Ms N made would be credited to a cryptocurrency wallet held in her own name.

By April 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 April 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.

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 Ms N made in April 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 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 April 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.

---

[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.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

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

Revolut should have identified that these payments were going to a cryptocurrency exchange as the merchant is a well-known cryptocurrency provider. However, I do not think the values of payments 1 to 11 were remarkable enough to have caused Revolut any concern. Nor do I consider enough of a pattern formed here to suggest Ms N might be at a heightened risk of financial harm due to fraud or a scam. Although the payments were identifiably going to a cryptocurrency provider that doesn't mean they all should automatically be treated as suspicious; particularly when there are no other concerning factors about the payments.

I think by payment 12 a pattern was emerging which was indicative of Ms N being scammed. Payment 12 was the sixth payment made in the same day and whilst individually the preceding payments were small in nature, multiple payments made to a cryptocurrency exchange on the same day is commonly a sign of someone potentially being scammed. Therefore, it would have been appropriate during payment 12 for Revolut to have given Ms N a written warning.

At this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scams, without significantly losing impact. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Ms N by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, 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.

That said, I am not persuaded a warning setting out the common features of a cryptocurrency scam would have stopped Ms N's loss at this point. I say this because such a cryptocurrency scam warning at this time would not have addressed fake job scams, which were not as well known in April 2023.

Similarly to payments 1 to 11 I do not think payment 13 ought to have been of any concern to Revolut. However, as the payments continued, I think that Revolut should have then intervened during payment 14. This was the eighth payment in

one day and was of a higher value compared with the proceeding payments. Having thought carefully about the potential risk payment 14 presented, I think a proportionate response would have been for Revolut to have attempted to establish the circumstances surrounding this payment before allowing it. I think, for example, it should have done this by directing Ms N to its in-app chat to discuss the payment further.

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

What did Revolut do to warn Ms N?

My understanding is that no warnings were provided by Revolut.

If Revolut had intervened, would that have prevented the losses Ms N suffered from payment 14?

If Revolut had questioned Ms N about these payments I am persuaded that she would have been honest about what they were for and how she had come across this job opportunity. I say this because when her other bank had questioned her on her recent account activity she was forthcoming with the details. This allowed it to inform her that she was the victim of a scam. Following this realisation she sent no further payments to the scammers. So, I see no reason why Revolut too wouldn't have ascertained that she had been scammed. Revolut would have discovered Ms N had been contacted via a messaging app by a company offering to pay her for completing tasks, but she had been told she would have to pay money using cryptocurrency to unlock more tasks and that by this point she had made a number of payments and still had not received any returns. As this is not how companies operate, I think it would have highly likely raised suspicions with a Revolut advisor; even if they were not intimately aware of the features of job scams.

The situation Ms N had found herself had the hallmarks of an advance fee scam; wherein a victim is continually asked to make payments whilst being told all funds will shortly be realised after another payment is made. I think Revolut would have been reasonably able to express to her that there was a significant risk that these payments were part of a scam. As Ms N acted on NatWest's discussion, I'm persuaded she would have done so in a similar situation with Revolut as well.

Is it fair and reasonable for Revolut to be held responsible for Ms N's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Ms N purchased cryptocurrency which 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.

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.

However, I think that Revolut still should have recognised Ms N might have been at risk of financial harm from fraud when she made payment 14. Revolut should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Ms N suffered from that point onwards. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to her own account does not alter that fact. I think Revolut can fairly be held responsible for Ms N'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 Ms N 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 Ms N could instead, or in addition, have sought to complain against those firms. But Ms N 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 Ms N'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 Ms N's loss from payment 14 (subject to a deduction for Ms N's own contribution which I will consider below).

Should Ms N bear any responsibility for her losses?

I've thought about whether Ms N should bear any responsibility for her losses. 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 including taking into account Ms N's own actions and responsibility for the losses she has suffered.

I do accept there were relatively sophisticated aspects to this scam, such as a platform to manage the user's apparent earnings and tasks. I've also kept in mind the scammer built rapport with her and she was able to 'withdraw' some funds during the initial demonstration. But, ultimately the opportunities offered by the scam appear to have been fairly dubious. While I haven't seen everything that Ms N saw, the scammer's explanation for how the scheme worked is implausible and I think Ms N ought reasonably to have questioned whether the activity she was tasked with carrying out (which does not appear to be particularly time-consuming or arduous) could really be capable of generating the returns promised.

I've considered that Ms N says she has earnt a similar amount for part-time work before. However, I find it doubtful her previous part-time work was anything like this

work for such promised returns. The requirement to send funds, which she first had to convert to cryptocurrency, to acquire the profits she'd supposedly already earned from completing some of the tasks should have been a red flag as well. I also think Ms N ought reasonably to have recognised the platform could effectively prevent her from withdrawing her funds by continuing to grant her 'premium' tasks; without a clear explanation of why she was being so 'lucky' to be assigned such tasks.

I've noted that as Ms N was utilising employment-focused social media platforms and actively applying for jobs she believed the opportunity to be genuine. However, receiving an unsolicited job offer via a mobile messaging service app from a firm she hadn't applied to, even if it was from what she believed to be a well-known company, should've reasonably led her to complete some due diligence. I also think as additional details were supplied to her by the scammers, which given the overall implausibility of the scam and the risk of being continuously asked to pay additional funds, it should have led to her to question whether the job was genuine.

Given the above, I think Ms N ought reasonably to have had concerns about the legitimacy of the job offered. In these circumstances she should bear some responsibility for her losses. Weighing the fault that I've found on both sides I think a fair deduction is 50%.

Could Revolut have done anything to recover Ms N's money?

The payments were made by card to a cryptocurrency provider with a wallet held in Ms N's own name. It was only when Ms N sent that cryptocurrency to the fraudster's wallet did the loss occur. Ms N states there was some delays in responding to her and Revolut made some duplicate requests. However, although I don't doubt this was frustrating, this ultimately would not have impacted the outcome of the chargeback. Revolut would only ever have been able to attempt to recover the funds from where they were originally sent, which was Ms N's own wallet. If these funds had not already been transferred to the scammer, they would be in her control to access as and when she chose.

I'll also note here that I don't consider a chargeback would have had any prospect of success because there's no dispute that cryptocurrency was provided in exchange for the payments, which were then sent in relation to the scam.

Therefore, there was nothing further Revolut could have done here.

Putting things right

To resolve this complaint Revolut Ltd should:

- *Refund the payments Ms N lost to the scam from, and including, payment 14, less a deduction of 50% in recognition of Ms N's own contributory negligence towards her loss.*
- *Pay 8% simple interest per year on £485 of this amount, calculated from the date of loss until the date of settlement, minus any applicable tax. As some of the funds (£2,500 after the contributory negligence deduction) Ms N lost were borrowed from her sister she has not been deprived of the use of her own money. So, Revolut does not have to pay 8% simple interest per year on this proportion. However, if Ms N is able to evidence she has repaid her sister 8% from that point would be applicable.*

Ms N responded and accepted my provisional decision. There was no response from Revolut. The case has now been passed back to me.

Putting things right

I remain of the view that this complaint should be upheld in the way I've said. So, I'm going to require Revolut Ltd to:

- Refund the payments Ms N lost to the scam from, and including, payment 14, less a deduction of 50% in recognition of Ms N's own contributory negligence towards her loss.
- Pay 8% simple interest per year on £485 of this amount, calculated from the date of loss until the date of settlement, minus any applicable tax. As some of the funds (£2,500 after the contributory negligence deduction) Ms N lost were borrowed from her sister she has not been deprived of the use of her own money. So, Revolut Ltd does not have to pay 8% simple interest per year on this proportion. However, if Ms N is able to evidence she has repaid her sister 8% from that point would be applicable.

My final decision

My final decision is that I'm upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms N to accept or reject my decision before 25 April 2025.

Lawrence Keath
Ombudsman