DRN-5078091

The complaint

Mr C is unhappy that Revolut Ltd won't reimburse money he lost to a scam.

What happened

In December 2023, Mr C saw an advert on social media. A famous investor claimed to have made significant amounts of money from trading in cryptocurrency.

He responded to the advert and was contacted by someone claiming to represent a cryptocurrency investment platform ("S").

Mr C agreed to invest. In order to fund his investment account he was required to purchase cryptocurrency, which credited his account at a genuine cryptocurrency exchange ("O") before being sent to S. He initially purchased cryptocurrency using his account at another payment service provider ("W").

Those payments were all peer-to-peer cryptocurrency purchases (that is a transfer made directly to sellers of cryptocurrency who then credited his account at O with cryptocurrency) and spanned 9 December – 30 December 2023. Mr C made payments totalling around £15,000 from his account at W.

On 30 December W contacted Mr C and asked him about the purpose of his account. He said that he was trading in cryptocurrency and had recently sold his car to fund the investment. A few days later W told Mr C that it was closing his account.

On 2 January 2024 Mr C opened his Revolut account. He told it at account opening that the purpose of the account was purchases of cryptocurrency.

His first payment was another peer-to-peer cryptocurrency purchase on 3 January 2024 (a payment that wasn't included in Revolut's complaint summary, but I'm satisfied forms part of the scam and was reported to it). Mr C then switched to making transfers to a cryptocurrency exchange ("U") (though he says he had no relationship with that exchange and was simply making payments where he had been instructed to do so by the fraudster).

Between 3 – 30 January 2024 Mr C made payments totalling £23,804.71 to the fraudsters. From 9 January 2024 the payments were all made to pay various charges and fees that the fraudsters claimed were due before his investment could be withdrawn.

On 30 January 2024, Revolut contacted Mr C with concerns about the payments he was making. During that conversation the scam came to light and Mr C didn't make any further payments.

The payments into Mr C's account were funded from his and his wife's accounts at another bank – T. Mr C says his wife lent him the money on the condition that he'd pay her back immediately after being able to access his investment.

He asked Revolut to consider reimbursing him, but it declined. It said that it had provided warnings about the payments on 3 and 9 January 2024 (which will be discussed in more detail later in my decision), but he had decided to proceed regardless.

Mr C referred a complaint to our service and one of our investigators upheld it in part. They thought that Revolut should have done more when Mr C attempted a payment on 17 January 2024 and, had it contacted Mr C, the scam would have been unearthed at that point (rather than on 30 January 2024). However, they also thought that Mr C should bear some responsibility for his loss, so they recommended Revolut reimburse 50% of the payments from 17 January 2024.

Mr C seems to have accepted this recommendation, but Revolut did not. In summary:

- It referred our investigator back to its original submission in which it argued, among other things, that departures from the law must be explained and acknowledged, it owes no duty to prevent fraud and scams, it had warned Mr C before making the payments and he hadn't acted with enough care.
- It repeated its original submissions by arguing the payments were all 'self-to-self' payments as Mr C controlled the beneficiary accounts the payments were sent to. Revolut was merely an intermediary link between Mr C's main bank account (at T) and the cryptocurrency account. Therefore the scam didn't take place on Revolut's platform and the money lost wasn't, in any case, his.
- By deciding that it is responsible for payments to a consumer's own account it has been left 'holding the baby' – an approach that is at odds with the PSR's APP Reimbursement Rules.
- In addition, it argued we should use our powers to obtain evidence from the other firms involved in the payments to establish whether they warned Mr C. We should also consider informing Mr C that it might be appropriate to make a complaint about one of those firms.

Mr C also complained to W. It accepted it could have done more to warn him about the final payment he made from his account at W and offered to refund 50% of that payment. He referred that complaint to our service and one of our investigators concluded that offer was fair.

But, as no agreement could be reached on this complaint, it was passed to me for a final decision.

What I've decided – and why

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

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

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in January 2024 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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;[2]

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

- 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, 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[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).
- Since 31 July 2023, under the FCA's Consumer Duty[4], 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*

---

[2] 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_/

[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

[4] 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.

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"[5].

- 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.

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 January 2024 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.

Should Revolut have recognised that Mr C was at risk of financial harm from fraud?

Mr C made 10 transfers each of around £2,150 all to the same merchant. 9 of those payments were made in the 11 days between 9 and 20 January 2024.

Mr C informed Revolut that he was trading in cryptocurrency before he made the payments on 3 and 9 January 2024. As the payee remained the same for all of the payments after 9 January 2024, it should have assumed that all the payments were being used to purchase cryptocurrency.

By early 2024 Revolut ought to have considered that payments to cryptocurrency providers carry an elevated risk of fraud.

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

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

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. And by January 2024 further restrictions were in place.

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 Mr C made in January 2024, 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.

It's relevant to note here that despite Revolut's arguments, the evidence suggests that Mr C didn't have control over the cryptocurrency account and it was, in fact, operated by the fraudster (albeit it was likely opened in his name). I can see that Mr C was directed to a third party identity verification service around the time he was told to make the payments and there's no evidence he ever interacted with the cryptocurrency platform that the payments were sent to. So, I don't think these payments were 'self-to-self' as Revolut claims.

Given the risk associated with the payments I would have expected Revolut initially to have warned its customer (as it did). I would have expected that intervention to take the form (at least) of a series of automated questions to understand the purpose of the payment and the circumstances surrounding it. I'd expect those questions to take into account Revolut's knowledge that the payment was going to a cryptocurrency provider. Once the payment of the purpose had been established I'd expect Revolut to have provided a tailored warning based on the main risk associated with the payment.

As the payments went on, the risk increased and I think Revolut should have done more, particularly as the answers that Mr C gave when it actually did intervene, were not particularly reassuring (as I'll come onto).

By the point Mr C made the seventh disputed payment on 17 January 2024, he had already sent payments to the same payee of over £10,000 in a little over a week. I think the risk had changed at this point. Revolut should have attempted to establish the circumstances surrounding the payments in more detail, for example by directing him to its in-app chat.

What did Revolut do to warn Mr C?

Revolut provided warnings and had interactions with Mr C prior to the payments on 3 and 9 January 2024.

On 3 January it paused the peer-to-peer cryptocurrency payment Mr C was attempting. Mr C disclosed that he was purchasing cryptocurrency and that he was trading.

Its advisor said:

"Alright. Make sure any research you do is your own – fraudsters create convincing-looking posts on social media, or share articles about investing. If someone says you need to send money as a tax or fee to access your funds, you are being scammed. Are you comfortable with proceeding with the transaction?"

Mr C confirmed he was. At this point it's relevant to note that Mr C had not been asked to pay any fees.

Revolut intervened again on 9 January 2024 (when Mr C was attempting the first payment to U). It initially showed a fairly generic warning about trusting the payee. Mr C was then shown a message saying that the payment had been flagged as a potential scam.

Mr C was then shown some additional screens. They highlighted the importance of answering questions honestly and not being guided how to answer them. Mr C had to acknowledge and/or answer each question presented.

Mr C was then directed to a questionnaire. He again disclosed that he was purchasing cryptocurrency, but denied that he'd downloaded any remote access software or that he'd been enticed into the investment by an advert on social media. He also said that he'd invested in cryptocurrency before and had carried out research.

Mr C was then directed to a further series of screens. These were tailored warnings about cryptocurrency investment scams and warned Mr C:

- "crypto scams promise high returns in short periods of time, and might even have professional looking platforms"
- "fraudsters use social media to promote fake investment opportunities"
- Fraudsters would ask him to install remote access software.
- To do research and that most cryptocurrency providers aren't regulated.
- Not to be rushed and to say no if being pressured to invest.

Mr C decided to proceed with the payment and was directed to an in-app chat with Revolut. He again disclosed that he was purchasing cryptocurrency. It initially warned him about safe account scams before providing the same message he was sent on 3 January 2024, that warned Mr C about paying taxes or fees to access his investment (by this point, Mr C was doing exactly that).

Considering the above, I'm satisfied with the steps that Revolut took on 9 January 2024, it provided a relevant warning after attempting to establish the circumstances surrounding the payment. While the warning didn't highlight all of the relevant features of a cryptocurrency investment scam, it did highlight some key features that were present in Mr C's circumstances.

When Revolut contacted Mr C again on 30 January 2024, its advisor initially went through a very similar series of questions with Mr C. But when asked whether he had carried out

research, Mr C asked whether Revolut had any information about the investment that could help him.

Revolut repeated the same messages about doing research and that only scammers would ask him to pay taxes and fees. It then asked him whether he was able to withdraw money that he'd deposited. Mr C said that he hadn't been able to.

Revolut replied with more warnings about cryptocurrency investment scams and then asked Mr C for the website or company that advertised the investment to him and whether anyone endorsed that advert.

At this point Mr C shared an 8 January 2024 email from S which said that he'd made $200,000 and demanded various fees. He then shared an email from 22 January 2024 demanding more fees and revealed that the investment had been promoted by a famous investor. After Mr C shared various other screenshots (including of S' platform) and the information was passed to another team, Revolut confirmed that Mr C was falling victim to a scam.

As I've set out above, I'm satisfied that following the payment on 9 January 2024, Revolut should not have let Mr C make another 9 payments to the cryptocurrency provider before it intervened again. By the payment on 17 January 2024, it ought to have been apparent that the risk of fraud had significantly increased. At this point Revolut should have contacted Mr C as it did on 30 January 2024.

The scam did come to light on 30 January 2024, so I've thought about whether Revolut should have brought it to light on 17 January 2024.

I don't think this is an easy decision. I'm conscious that Mr C had bypassed relevant warnings on both 3 and 9 January 2024. Those on 9 January 2024 were particularly relevant to him – as they warned him against paying taxes or fees to access an investment and highlighted celebrity endorsements as a common feature of cryptocurrency investments scams.

On the other hand, those earlier interventions were fairly automated (even when Mr C was communicating with a human) and it's clear stock phrases were being used. No attempt was made to establish the wider circumstances surrounding the payments. As I've said, I think that was proportionate at that stage. But later, when the risk had increased, I think any intervention had to be more dynamic and agile – reacting to what Mr C said and exploring the circumstances surrounding the payment.

On 30 January 2024, it seemingly only took one or two possibly off-script questions to prompt Mr C into significant disclosures – not least the email demanding fees – which any competent fraud specialist at Revolut would have been able to immediately identify as fraudulent and consistent with exactly the kind of fraud Mr C had been warned about. So, on the face of it, a few open questions about the wider circumstances would have brought the scam to light earlier than 30 January 2024.

In order to try and shed some further light on this, the investigator contacted W and T to see if Mr C had received any warnings from either firm. T declined to provide this information (despite more than one request) stating only that Mr C had been sent a text message advising that it does not allow cryptocurrency purchases. I can't compel T to provide evidence as it is not a party to the complaint. W displayed only a warning about a different type of scam, so it didn't provide any relevant warnings.

It appears that T did speak to Mr C's wife about the payments to Mr C's Revolut account. She recalls being asked some security questions and informing T that she was making the payment to her husband. I haven't heard those conversations (and given T's response in relation to our investigators request about Mr C's account, it's unlikely I'd be able to obtain them) but, in any case, I think it's unlikely that a conversation with C's wife would have brought the scam to light, given that it was Mr C rather than her that was falling victim to the scam.

I've also thought about how Mr C's circumstances changed between 17 and 30 January 2024. On 17 January Mr C had paid about £13,000 towards the £18,000 he believed he had to pay to access his funds. Whereas on 30 January he'd made one payment towards an additional £13,000 in fees and charges that he'd been informed of, via email and to his surprise, on 23 January 2024. I also understand that a friend of Mr C's had warned him about S being a potential scam (he hasn't pinpointed exactly when this happened – but I understand it happened before 30 January 2024) and that he raised this with the fraudster.

I can also see that Mr C wrote to the fraudsters on 23 January 2024 to complain about the additional £13,000 he was being asked to pay. So, it's clear Mr C had more reasons to be concerned on 30 January 2024. He'd met the fraudster's demands to pay £18,000 and still didn't have his money. He was now very reluctantly trying to meet the further demands of the fraudster. I accept those different circumstances may have made him more susceptible to listening to Revolut's warnings. I am also conscious that Mr C had already gone to fairly extreme lengths to fund the scam – including selling his car.

I've thought about this carefully, and I think it's quite a finely balanced point, but like the investigator I've concluded that a conversation on 17 January 2024 is likely to have revealed the scam as it did on 30 January 2024. In deciding that, I've taken into account that it took only very limited enquiries of Mr C on that day to reveal the scam and that he was prepared to show Revolut evidence of his correspondence with the fraudster. As I've set out, that correspondence couldn't have left Revolut in any doubt about the legitimacy of the scheme and it would have been in a position to give a very clear warning that he was almost certainly falling victim to a scam. So, while Mr C might have been reluctant to accept that – given how much he'd already paid, I think, like he did later, he would have accepted that the scheme wasn't genuine.

That means that I've decided that Revolut should reimburse the payments from 17 January 2024. However, I've also thought about Mr C's role in what happened. In doing so 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 there were sophisticated aspects to this scam – not least the provision of a trading platform and a faked celebrity endorsement (though this seems not to be a paid-for advert but rather a social media page – so I'm not sure the extent to which Mr C could have expected such a page to be vetted). But I'm concerned that Mr C took the claim that he'd made around $200,000 in less than a month and with an investment of less than £20,000 at face value, particularly when subsequently asked to pay various unexpected taxes and fees (some which appear very arbitrary and were conveyed in an email riddled with errors).

I've also taken into account that Revolut did specifically warn him about paying taxes or fees on 3 and 9 January 2024, but he doesn't seem to have taken this on board. Overall, I think that Mr C should have stopped at this point (and certainly by 17 January 2024) and sought further advice or researched the fraudsters online. His own correspondence with the fraudsters shows that he did this and found very little about them online (a fact that he found surprising). But I think further searches would have shown that his circumstances were consistent with a cryptocurrency investment scam.

Weighing up the fault on both sides I think that Mr C's redress should be reduced by 50%.

Is it fair and reasonable for Revolut to be held responsible for Mr C's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that the money that funded Mr C's Revolut account came from another of his accounts and that of his wife. As I've set out above, I'm not persuaded that the funds went to an account under Mr C's control – there's no evidence of that and Mr C denies it. Correspondence with the fraudster suggests that account was set up by the fraudster but in Mr C's name – so the money was likely lost at the point it left Revolut.

In any case, as I've set out in some detail above, I think that Revolut still should have recognised that Mr C might have been at risk of financial harm from fraud when he made the 17 January 2024 payment, 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 Mr C suffered. The fact that the money used to fund the scam came from elsewhere does not alter that fact and I think Revolut can fairly be held responsible for Mr C'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 the firm that is the origin of the funds.

I've also considered that Mr C has only complained against Revolut in relation to these payments. 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 Mr C could instead, or in addition, have sought to complain against those firms (though much of the money came from Mr C's wife, not from his own accounts). But Mr C has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr C'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 about these payments 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 Mr C's loss from the 17 January 2024 payment with a deduction for Mr C's own contribution.

Recovery of funds

The funds that Mr C sent were paid to a cryptocurrency account. Although it does not appear that Mr C had control of that account, given its nature it's very likely that the funds Mr C sent would have been converted into cryptocurrency and sent to a third party. And when Revolut did attempt to recover the payments it was informed that no funds remained.

Putting things right

I've found that Revolut should have prevented the final five payments to the scam (a total of £10,732.96) but that Mr C should bear 50% of the responsibility for the loss. So Revolut should reimburse £5,366.48.

Our investigator recommended that interest should be paid on the funds reimbursed to Mr C. However, I understand that Mr C borrowed money from his wife in order to fund the payments. I can't make an award for Mr C's wife being deprived of the money and I understand that no interest was charged by her to Mr C. So I make no award for interest and Mr C has accepted this.

My final decision

I uphold this complaint about Revolut Ltd and instruct it to pay Mr C:

- £5,366.48

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 16 April 2025.

Rich Drury
Ombudsman