DRN-5405117

The complaint

Mr F complains that Revolut Ltd didn't do enough to protect him when he was making payments toward an investment scam. He also complains it's not refunded him since the scam was reported.

What happened

Mr F saw an advert for a cryptocurrency investment opportunity on social media. It appeared to be endorsed by a well-known television celebrity, which Mr F has said gave it an air of legitimacy. So he clicked on the link and was soon contacted by someone claiming to work for the firm and describing themselves as a broker. But Mr F had actually been contacted by a scammer.

Mr F was shown an online trading platform and was convinced to invest, believing all to be legitimate. He was told he'd need to open a Revolut account and a cryptocurrency wallet, which he did. He was also instructed to download AnyDesk.

He made an initial payment of £250 from an account held elsewhere. Seeing what appeared to be returns on that investment generated quickly, and having been able to withdraw some funds, Mr F decided to invest more. At the scammer's instruction he credited his Revolut account with funds from accounts held elsewhere.

Once the money was in his Revolut account he sent it on to his cryptocurrency wallet by way of card payments. From there it was sent on to a wallet controlled by the scammer, though each payment appeared to be reflected on the fake trading platform he'd been given access to.

But when it came to trying to withdraw the supposed earnings, Mr F found barriers kept being put in his way. By June 2023 he was being told he'd have to pay various fees and taxes to get access to the money. He paid these to begin with, sending the money by bank transfer, before realising he'd been caught up in a scam. Mr F applied for loans to cover those fees.

By the time the scam was revealed the following payments had been made.

Date	Time	Amount	Type of payment
2 February 2023	02:47	£2,500	Card
17 February 2023	15:24	£5,000	Card (declined)
20 February 2023	15:23	£5,000	Card
20 February 2023	15:23	£6,000	Card
13 June 2023	08:07	£10,000	Transfer (Reverted)
13 June 2023	08:53	£10,000	Transfer
20 June 2023	13:21	£10,914	Transfer

Over the course of the scam, Mr F had been able to withdraw a total of £3,270.36.

Mr F contacted Revolut to report what had happened. It requested some more evidence, but this wasn't provided before it issued its final response. As a refund hadn't been offered Mr F brought his complaint to our service.

One of our investigators considered the complaint and recommended it be upheld in part. he acknowledged Mr F had authorised the payments himself, but felt Revolut ought to have done more to protect him, specifically from 17 February 2023 as Revolut had intervened but not to the extent warranted by the scam risk presented. he was satisfied that, had it done so, Mr F's loss could have been prevented so he believed it was fair and reasonable to hold Revolut responsible for Mr F's loss.

She went on to say that Mr F ought to bear some responsibility too, given his actions hadn't been reasonable throughout. he noted Mr F had been dishonest with the lenders when he applied for the loans, and that the proposed investment seemed too good to be true (given it offered a 100% return on investment). Her conclusion was then that the loss from 17 February 2023 onwards ought to be shared between Mr F and Revolut.

Mr F accepted those findings, but Revolut didn't. It requested an ombudsman review the complaint.

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.

Having done so I'm upholding it. I'll explain why.

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

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and

[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_/

control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[3], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their 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

[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"

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 February 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 February 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr F has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to third parties and to his 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 Mr F to make the payments using his 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 Mr F might be the victim of a scam.

I'm aware that cryptocurrency exchanges like the one used here 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 card payments would be credited to a cryptocurrency wallet held in Mr F's name.

By February 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. And by February 2023, when these payments took place, 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 F made in February 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle (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 February 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

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

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

I think Revolut should have identified that payment one was going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). But the value was low enough so as to not cause significant concern at that stage, and I don't think Revolut should reasonably have suspected that it might be part of a scam.

Payment two (the attempted payment on 17 February 2023) was clearly going to a cryptocurrency provider. It was significantly larger than the previous payment that had debited Mr F's account.

Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr F was at heightened risk of financial harm from fraud. And there are other relevant factors at play here too.

Mr F's account was being quickly topped up and emptied, a common feature of cryptocurrency scams. Some of the top-ups had failed, indicating there could be something wrong. And Mr F had told Revolut the account was to be used for transfers, not for card payments to cryptocurrency exchanges. So there was a clear detachment of purpose, and the activity was not what Revolut ought to have been expecting.

In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr F before this payment went ahead.

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 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.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by February 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.

It's also the case that Revolut must agree, to at least some extent, that the activity presented a risk that warranted intervention, given it didn't allow the payment through without some discussion.

What did Revolut do to warn Mr F?

When Mr F tried to make payment two, it wasn't allowed to go through. Revolut directed him to the in-app chat to ask some questions. The brief conversation went as follows.

Revolut: So that we can help to keep you protected, we need to check some details with you. For identification purposes, could you please provide me with a selfie while holding a piece of paper with "Revolut 17/02/2023 1745" handwritten on it similar to what the example below shows. Please make sure that the following requirements are present:

- You are the one taking the picture

- Your face, hand and the paper are visible/clear

- The wording above is handwritten

2 - Please provide us with your phone number.

3 - Please specify, if in recent weeks you have received:

Any suspicious text messages (SMS)/emails with link or authentication codes?

Any suspicious calls from anyone claiming to be Revolut or any official bank's representative.

4 - Please list all devices you have used so far to access your Revolut account (model of mobile phone, computer applications)

5 - Do you use any finance managing or shared wallet applications?

6 - Have you recently downloaded any screen sharing application e.g. AnyDesk?

7 - What is the nature of your account? What is the purpose of it?"

Mr F: No suspicious messages or calls.

Mobile i phone and laptop

No shared applications

No any desk.

The account is for personal reasons

Revolut hasn't been entirely clear about what happened next. But we know the payment was declined. And it seems it may have said to Mr F:

I am afraid this payment was declined due to its possible high risk nature, in this case, sadly similar payments directed to the same merchant might not get completed due to the same reason. I am sorry if this has caused you any issues!

It's unclear where and how this message was delivered, if at all, but it certainly wasn't part of the in-app chat he'd been engaged in, where there was no further discussion about the payment.

There were later warnings provided by Revolut, given when Mr F was making the transfers in June 2023. These said:

Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment.

For the payment on 20 June 2023 Mr F was asked to select a payment purpose after the above warning. Given a list of options, he selected 'safe account'. He was then given a warning relating to fraudsters impersonating Revolut (and others) and some of the risks. Mr F proceeded with that payment.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Mr F attempted to make the 17 February 2023 payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a

warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, 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. 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.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr F by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

What seems somewhat odd here, is that Revolut clearly identified a scam risk, but provided no warning to mitigate against it. The in-app conversation simply ended without Mr F being spoken to any further and with no warning being provided.

Revolut has also pointed to later warnings, particularly the one about safe accounts. But the content of that warning was irrelevant to Mr F's circumstances. That's somewhat understandable, given Mr F wasn't caught up in a safe account scam. And, in any case, Revolut ought to have been very concerned about such a payment purpose being selected, given it is an incredibly high-risk and easily identifiable scam. So it ought to have started to question Mr F further here; not allow him to move on without further significant intervention.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr F suffered from the 17 February 2023 payment?

I'm satisfied Mr F's loss could have bene avoided here. The circumstances Mr F found himself in matched the very most common features of a cryptocurrency investment scam. And those features ought to have been pointed out and described to him.

Had they been, I'm satisfied such a warning would have resonated with him and been impactful. I'm satisfied it's more likely than not he would have either stopped what he was doing immediately or, at the least, to have sought further advice from Revolut or one of his other account providers.

In making that finding I have in mind that Mr F received no scam education specific to cryptocurrency investment scams at any point.

I have taken account of the fact it appears Mr F was being coached by the scammer, at least to some extent. But that is a further feature that could and should have been explained to him.

Whilst that coaching did lead to Mr F misleading his other account provider when it asked about a payment he was making to Revolut, and the lenders from whom he borrowed, the explanations he was giving there simply couldn't have stood up to scrutiny, given the payments were identifiably going to a cryptocurrency exchange. So he would have had to have given an explanation much closer to the truth, allowing far greater opportunity for the scam to be exposed.

Revolut has said in its submissions to this service that if Mr F had replied to its questions with the exact information it could have assisted properly and provided scam advice. But I can't see how his answers fairly and reasonably led to no scam advice being provided. Furthermore, I don't consider Mr F's answers to be an avoidance or mis-answering of the questions. The questions themselves are closed, not particularly clear, and it's not self-evident what the purpose of them is. And the only question Mr F seems to have answered

incorrectly is the one about AnyDesk. I'm not persuaded a different answer to this question would then have led to a more detailed and appropriate response from Revolut.

On the subject of his other account provider intervening, it's also evident from that call that Mr F could not provide satisfactory detail about the payment purpose to allow the payment to go through. Mr F tried to explain he was buying a car, but the member of staff soon found there were numerous holes in that story, and it fell apart, with the payment being refused. I see no reason why any other attempt to disguise the purpose of the payment would have been more successful.

Later on in the scam, when the payment on 20 June 2023 was blocked, Mr F told Revolut he was making a payment to a 'safe account'. I've already explained the significant risk that sits behind that payment purpose. I then consider it highly unlikely Mr F selected the payment purpose in an attempt to disguise what he was doing, either on the advice of a scammer or of his own volition. Instead, I consider it more likely than not Mr F was paying an account he believed to be safe. To me, this suggests he would have been upfront about the purpose of other payments, if questioned earlier.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr F purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his 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.

In reaching my decision, I have taken into account that the payments were made to other financial businesses and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr F might have been at risk of financial harm from fraud when he attempted the payment on 17 February 2023, 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 F suffered. 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 Mr F's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr F'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 Mr F 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 Mr F could instead, or in addition, have sought to complain against those firms. But Mr F has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr F'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 Mr F's loss from the 17 February 2023 payment (subject to a deduction for Mr F's own contribution which I will consider below).

Should Mr F bear any responsibility for his losses?

Our investigator found that Mr F ought to bear some responsibility for his losses, even from the point at which Revolut ought to have done more. Mr F agreed with that assessment. And Revolut has always thought Mr F should bear responsibility for his loss. And so there's actually little left in dispute in terms of what I need to make a finding on here. But, for completeness, I'll say this:

- I can understand why Mr F put faith in what appeared to be a genuine, celebrity endorsed advert on social media. That can be a powerful tool used by scammers, and it appears to have struck a chord with Mr F;
- I accept it's likely the fake trading platform he saw did appear convincing and the scammer's seemed genuine and professional; *but*
- I think the proposed returns were unrealistic from the outset and ought to have been viewed with a good deal of skepticism, to the extent of them being too good to be true;
- Those returns were shown to be exceptionally large as time went on, with an investment of just over £13,000 having grown to over £180,000;
- There appears to have been very little discoverable online about the broker, from being a registered company to having detailed reviews. A lack of such information ought fairly and reasonably be viewed as concerning;
- Mr F misled his other account provider and lenders about what he was doing. Had he been completely upfront about what he was doing, the scam would likely have been avoided.

With all this in mind I find it would be fair and reasonable for the loss to be shared equally between Mr F and Revolut.

Could Revolut have done anything to recover Mr F's funds?

Unfortunately, there was nothing Revolut could have done to recover the payments made by card. Given they were properly authorised, went to a cryptocurrency wallet in Mr F's name, and he moved the funds on from there, there was no way to pull the money back. There was no chargeback right available, and the cryptocurrency provider had provided the goods and services it was contracted to.

Whilst there are mechanisms to try and recover money sent by bank transfer, I'm not persuaded there's more for Revolut to do here. I'm conscious that he didn't contact Revolut for nearly three weeks from the last payment made. And so the likelihood of any funds remaining in any of the beneficiary accounts is very low. Typically, funds are moved out of such accounts very quickly.

Putting things right

On Mr F's acceptance Revolut must:

- Refund 50% of Mr F's loss from the attempted payment of 17 February 2023 onwards (total sent – returns = total loss, to then be divided by two)

- Pay interest on that sum at 8% simple per year, calculated from the date the claim was declined to the date of loss.

My final decision

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 18 June 2025.

Ben Murray
Ombudsman