DRN-5209116

The complaint

Mr P complains that Revolut Ltd failed to protect him when he fell victim to a cryptocurrency investment scam.

Mr P is represented by solicitors in this complaint.

What happened

The detailed background to this complaint is well known to both parties and has been previously set out by the investigator. So, I'll provide an overview and focus on giving my reasons for my decision.

In August 2023, Mr P was tricked into parting with his funds in connection to what he thought was an investment opportunity. But it turned out to be a scam. He'd been looking to invest and was contacted by an individual on a popular social media platform who said they worked on behalf of a firm, "C". The representative told Mr P that they would complete trades on his behalf, and he only needed to deposit cryptocurrency into his investment account. Mr P states he reviewed C's social media account and could see lots of positive posts by users who had made profits.

Persuaded to invest, Mr P followed C's instructions and opened an e-money account with Revolut. After transferring funds from his account with a high street bank, Mr P exchanged fiat money into cryptocurrency before sending some of it on to his investment account ('cryptocurrency withdrawal'). When he experienced issues doing this, Mr P used his Revolut card to purchase cryptocurrency from a cryptocurrency provider.

The following transactions are relevant to this complaint –

Date	Transaction Type	Amount
17 August	Fiat to Crypto exchange	£300.00
17 August	Crypto withdrawal	0.01268336 BTC
17 August	Fiat to Crypto exchange	£1,000.00
17 August	Crypto withdrawal	0.04442363 BTC
19 August	Fiat to Crypto exchange	£425.00
19 August	Crypto withdrawal	0.01994473 BTC
22 August	Fiat to Crypto exchange	£1,000.00
22 August	Crypto withdrawal	0.04690425 BTC
22 August	Fiat to Crypto exchange	£1,864.00
22 August	Debit card payment	£1,730.65*
22 August	Debit card payment	£270.00
22 August	Fiat to Crypto exchange	£1,500.00
25 August	Debit card payment	£1,000.00
25 August	Debit card payment	£1,000.00
26 August	Debit card payment	£800.00
28 August	Debit card payment	£1,000.00
*trigger point		

Mr P realised that he'd been scammed when he paid a fee to make a withdrawal from his investment, but funds weren't released. He reported the matter to Revolut a few weeks later but didn't respond when it made further enquiries. Subsequently, Revolut received a complaint from Mr P through his representative. It refused to refund any of the transactions and the matter was referred to our service.

In its complaint file submission, Revolut said Mr P had authorised the transactions and the funds went to an account in his name. It also said our service didn't have jurisdiction to consider the cryptocurrency withdrawals Mr P made in relation to the scam.

Our investigator explained that although our service couldn't consider cryptocurrency withdrawals in isolation, the process of making those withdrawals involved earlier steps such as Revolut accepting Mr P's fiat money into the account and exchanging it into cryptocurrency. The investigator concluded that our service could consider the merits of Mr P's complaint, at least in respect of the card payments and the exchange of fiat money into cryptocurrency.

The investigator concluded that Revolut should have identified Mr P was at heightened risk of fraud when he authorised a card payment of £1,730.65 on 22 August. Had it taken additional steps and provided a scam warning which covered typical features of investment scams involving cryptocurrency, the investigator was persuaded that Mr P's losses could have been limited. They recommended a refund of all the disputed transactions from that payment onwards along with interest, but with a 50% deduction for contributory negligence on Mr P's part. The investigator noted that no cryptocurrency withdrawals took place after the suggested trigger point, so they weren't included in the recommendation.

Mr P accepted the investigator's findings, but Revolut didn't. In summary, it said the payments were self to self and the scam didn't occur on its platform. Revolut also said that the part of the complaint which encompasses cryptocurrency withdrawals should be considered ineligible.

The investigator replied and said they'd already considered Revolut's arguments relating to the transactions being self to self. They also said they'd previously explained that there were no cryptocurrency withdrawals after the suggested trigger point, so they weren't included in the recommendation.

Revolut didn't respond and so the complaint has been passed to me to decide.

Preliminary matters

Revolut hasn't replied to the investigator's last correspondence in relation to matters concerning our jurisdiction. For completeness, I agree that I can't consider cryptocurrency withdrawals in isolation given it's not a regulated activity. But the exchange of fiat money into cryptocurrency, which although not a regulated activity in itself, is one which our service would consider ancillary to payment services. This is in the same way we consider exchanging GBP into foreign currency an ancillary activity.

Therefore, given the nature of Mr P's complaint, I'm satisfied that I can consider whether Revolut did what it should have, in relation to his funds and account when he used Revolut to exchange his money from GBP to cryptocurrency.

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'm 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 P 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"*.

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***
>
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
>
> - *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 P and the Payment Services Regulations to carry out her instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I'm satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in August 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

While the Consumer Duty doesn't mean that customers will always be protected from bad outcomes, Revolut was required act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I've taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I'm also mindful that in practice, while its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But the basis on which I'm 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.

While the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in August 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I'm mindful that in practice all banks and EMIs like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

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

I'm also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3).

- 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 don't suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[2], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

---

[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_/

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

- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[4].*

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in August 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;

---

[3] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

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

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

- 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.

While I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in August 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr P has fallen victim to a cruel scam here, nor that he authorised the payments he made.

I think Revolut should have identified that the card payments were going to a cryptocurrency exchange (the merchant involved is a well-known cryptocurrency exchange). I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Mr P's name.

By August 2023, when these transactions started, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[6]. And by March 2023, further restrictions were in place[7]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related

[6] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.
[7] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

to 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'm satisfied that by the end of 2022, prior to the payments Mr P made, 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.

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 the card payments in this case were going to an account held in Mr P'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 transactions, at what point, if any, it ought to have identified that Mr J might be at a heightened risk of fraud that merited its intervention.

I don't think there was anything particularly unusual about the money Mr P exchanged into cryptocurrency between 17-21 August such that I consider Revolut should have had cause for concern. Or, for that matter, the first two exchanges on 22 August. It seems Mr P accepts this finding given he didn't dispute it when the investigator reached the same conclusion. By the time Mr P authorised the next transaction that day – a card payment of £1,730.65 – given the increased cryptocurrency activity in such a short period, I think that the circumstances should have led Revolut to consider that he was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Mr P?

Revolut says the card payments were biometrically or password approved, so there was no reasons for it to suspect there to be any issues.

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

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

The investigator concluded that an appropriate intervention from Revolut would have been a tailored written warning about the main type of cryptocurrency scam risk, i.e., cryptocurrency investment scams. But I think that by August 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. As I explained earlier in this decision, I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider a firm should by August 2023, on identifying a heightened scam risk, have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that the payment in question was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation, and investment scams.

Taking that into account, I'm satisfied that, by August 2023, fairly and reasonably, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mr P made the card payment in question, Revolut should – for example by asking a series of questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely cryptocurrency related scam he was at risk from.

In this case, Mr P was falling victim to an investment scam – he believed he was making payments in order to deposit funds into his trading account. As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Mr P gave.

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; promises of returns that are too good to be true; 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 P by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have limited the losses Mr P suffered?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr P's payments, such as finding out about the opportunity through someone he'd met a social

media platform, being assisted by a broker who assisted him in making deposits to his trading account and trading on his behalf.

I've also reviewed the written correspondence between Mr P and the scammer (though I note that he appears to have also spoken to them, not just communicated through instant messages, and I haven't heard those conversations). I've found nothing within the written correspondence that suggests he was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr P expressed mistrust of Revolut or financial firms in general.

What I have seen is that in the days prior to the suggested trigger point, Mr P expressed concerns that he was unable withdraw anything from his investment account. For instance, on 17 August, when the scammer encouraged him to make a further deposit to hit the 'profit target', Mr P told them he couldn't just put in more money into something that hadn't made him any profit and he couldn't withdraw his investment. This suggests he appeared to have had some misgivings of his own. Given this, I think Mr P was more likely to have been influenced by a scam warning from Revolut.

On the balance of probabilities, had Revolut provided Mr P with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have, for instance, paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Mr P from Revolut would very likely have caused him to decide not to go ahead with the card payment in question on 22 August.

What this means is that Revolut could have prevented Mr P's losses from that point onwards. Although he exchanged £1,500 into cryptocurrency in relation to the scam later that day, there were no further cryptocurrency withdrawals. As such, there's no loss from that exchange and Mr P's losses from the suggested trigger point stem only from the six card payments to the cryptocurrency provider.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mr P purchased cryptocurrency using his card which credited a cryptocurrency wallet held in his own name, rather than making a payment directly to the scammer (he does appear to have sent the cryptocurrency he exchanged through Revolut directly to the scammer). So, he remained in control of his money after he made the card payments from his Revolut account, and it took further steps before the money was lost to the fraudsters. I've carefully considered Revolut's view that the fraudulent activity didn't occur on its platform.

However, for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mr P's losses from the first card payment on 22 August onwards, subject to a deduction for his own contribution (which I'll consider below). As I've explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice, I consider it fair and reasonable that Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr P's own cryptocurrency wallet doesn't alter that fact and I think Revolut can fairly be held responsible for his 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.

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I've not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I won't be commenting on it.

I note that Revolut says it hasn't asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it's asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

Our service did contact the relevant financial institutions and there were no claims or interventions to note. I've also considered that Mr P has only asked us to consider his complaint against Revolut. He hasn't chosen to complain to the other financial institutions and ultimately, I can't compel him to.

Therefore, I'm not persuaded that it would be fair to reduce Mr P's compensation in circumstances where: the consumer has only complained to our service about one respondent from which they are entitled to recover their losses in full; 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) and for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mr P's loss starting from the first debit card payment on 22 August (subject to a deduction for his own contribution which I will consider below).

Should Mr P bear any responsibility for his losses?

Mr P has already accepted that he should share equal responsibility for what happened here. But for completeness, I'll explain why I agree that it would be both fair and reasonable in the circumstances of this complaint that Revolut's liability is reduced by 50%.

There's a general principle in law that consumers must take responsibility for their decisions. I recognise that, as a layperson who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. I've taken into account the provision of the trading platform (which, I understand, used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that the scammer used the apparent success of early trades to encourage increasingly large deposits. I can understand how what might have seemed like taking a chance with a relatively small sum of money snowballed into losing a life changing amount of money.

So, I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr P to be reduced. I think it should.

Other than checking the scam company's account on the social media platform, Mr P doesn't appear to have done any research into the investment opportunity before he invested. That fact alone wouldn't necessarily be enough for me to consider that there should be a deduction to the amount awarded. But Mr P had been promised unusually high returns (£1,000 turning into over £14,000) and his investment had generated significant profits in a very short period. Offers like this ought to have given him cause for concern, enough to warrant checking that everything was above board. As I've mentioned above, Mr P seems to have had his own misgivings about the opportunity yet he carried on.

Having weighed the liability which I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything else to recover Mr J's money?

The transactions from Mr P's Revolut account were to either purchase or exchange cryptocurrency, which was then sent to the fraudster (albeit he didn't know that at the time). Revolut in this instance would have been unlikely, given the cryptocurrency was already in the hands of the fraudster.

Specifically for the card payments, I don't consider that a chargeback would have had any prospect of success. There's no dispute that the merchant (cryptocurrency exchange) provided the cryptocurrency. In other words, the merchant Mr P paid using his card did render the services he paid for.

Putting things right

Revolut Ltd needs to refund Mr P all the six card payments he made in relation to this scam from 22 August 2023 onwards (see above table), making a 50% deduction for contributory negligence. It also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of settlement.

If it considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, Revolut Ltd should tell Mr P how much it's taken off. It should also provide a tax deduction certificate if Mr P asks for one, so the tax can be reclaimed from HM Revenue & Customs if appropriate.

My final decision

For the reasons given, my final decision is that I uphold this complaint. Revolut Ltd needs to put things right for Mr P as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 4 April 2025.

Gagandeep Singh
Ombudsman