DRN-5014613

The complaint

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

What happened

The facts are well known to both parties, so I have outlined the key details. In summary, Mr A says that he received an unexpected phone call on WhatsApp. The caller told him that he could make money trading cryptocurrency. Mr A explains this was attractive to him because he was working on a temporary contract and needed the extra money. Unfortunately, Mr A was really interacting with a fraudster. The fraudster coached Mr A through the process of setting up the accounts, including a Revolut account and an account at a cryptocurrency exchange that I'll refer to as B. Mr A recalls that the fraudster was professional and provided a London address for the investment company. Mr A says that the fraudster spoke about the profits that other investors had made. Mr A decided to go ahead.

Mr A made the following card payments to B:

	Date	Amount	Completed?
1	12/12/2022	£3,000	No -reverted back to Mr A's Revolut account by B- no loss
2	13/12/2022	£3,000	Yes
3	25/1/2023	£5,100	Yes
4	27/1/2023	£1,800	Yes
5	1/2/2023	£7,250	Yes
6	3/2/2023	£23,000	Yes
7	4/2/2023	£4,500	Yes
		Total: £44,650	

All of these payments were used to purchase cryptocurrency from B, which credited Mr A's own cryptocurrency wallet. From his cryptocurrency account at B, Mr A sent cryptocurrency to fraudsters. He was told that some of these payments were towards the investment. From February 2023 onwards the payments were amounts Mr A was told to pay in order to access his profits. After Mr A made the final payment, he did not receive any profits or his money back and he was no longer able to make contact with the fraudsters.

Mr A, through a professional representative, referred the matter to Revolut. In its final response letter dated 7 September 2023, Revolut said it was unable to dispute card payments where the service was considered provided and as described, as it says was the case here when the funds were deposited to the beneficiary account. It added the fraudulent activity didn't take place on the Revolut platform as Revolut had been used as an intermediary to move funds on to Mr A's account with the cryptocurrency exchange. It considered Mr A lost control of the funds further on in the chain and concluded that Revolut hadn't acted unfairly by declining his claim. It said it sympathised with Mr A's loss, but it was not able to find any fraudulent activities.

Mr A, through a professional representative, referred the matter to our service.

One of our Investigators upheld the complaint in part. He said that when Mr A made the third payment, Revolut ought to have realised the transaction carried an elevated risk of being related to a fraud or a scam. He referred to widespread coverage in the media about the increase in losses to cryptocurrency scams and thought Revolut should have provided a tailored written warning as Mr A was making a payment of £5,100. After gathering evidence, including details of interactions Mr A had with another financial firm, our Investigator said he had no reason to believe that Mr A wouldn't have listened to a warning provided by Revolut. He was mindful that Mr A missed some clear red flags about the situation and said a fair outcome would be for Revolut and Mr A to share responsibility for the losses he had suffered.

Revolut didn't agree and wanted the complaint to be reviewed. It said if an Ombudsman is going to depart from the law, this must be acknowledged and explained. Revolut said it does not owe a duty to prevent fraud or scams and there are only limited circumstances in which it is obliged by law to reimburse customers who have suffered loss through frauds or scams. It highlighted it is required to process payments promptly and the Financial Ombudsman Service is overstating Revolut's duty to its customers. It highlighted the reimbursement codes and rules do not generally apply. It also highlighted that Mr A was making payments to another account in his name which he had control over. It felt that either the Financial Ombudsman Service was incorrectly applying reimbursement rules to self-to-self transactions and making an error in law, or the service has irrationally failed to consider the transactions are distinguishable from transactions subject to the regulatory regime concerning APP fraud. It considered there is no rational explanation as to why Revolut should be held responsible for loss, particularly where the transactions are self to self. It said there are other authorised banks and financial institutions in the payment chain that have greater data on the customer than Revolut did, but they are not being held responsible in the same way.

Mr A's representatives did not agree either, but did not provide any reasons.

As no agreement could be reached, the case has been 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.

For the reasons I shall set out below, I consider Revolut should, at the least, have provided a written warning specific to cryptocurrency investment scams prior to the third payment. If it had done so, I'm satisfied the scam, as well as the losses to Mr A from that payment onwards, would more likely than not have been prevented. But I am also satisfied that in the circumstances of this complaint, Mr A should bear some responsibility (50%) for the losses he suffered. 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 A 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 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 January 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 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

[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] 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.

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 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 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

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

- 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 when Mr A made some of these payments, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr A has fallen victim to a cruel scam, nor that he authorised the card payments he made to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

I'm aware that cryptocurrency exchanges like B generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Mr A's name.

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

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[4]. 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 around the time Mr A was making these payments, 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,

[4] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in early 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.

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 A might be at a heightened risk of fraud that merited its intervention.

The merchant Mr A is paying is a well-known cryptocurrency provider, so I think Revolut should have identified from the outset that these payments were going to a cryptocurrency provider. But I am mindful that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions. I don't think Revolut ought to have been concerned about the first two transactions that Mr A made. The first transaction didn't debit Mr A's account as B reverted it back, so Mr A made it again the following day. I don't think Revolut ought to have been sufficiently concerned about the running of Mr A's account at this point that it would be fair and reasonable to expect it to have provided warnings to Mr A. I don't think I can fairly say that Revolut should have suspected that these payments might be part of a scam.

But I'm satisfied that Revolut ought to have recognised that the third card payment carried a heightened risk of financial harm from fraud because it was for a much higher amount of money and because it was potentially indicative of an emerging pattern of Mr A making payments to a cryptocurrency exchange. I think that a proportionate response to that risk would have been for Revolut to warn Mr A 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 third payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

For the reasons I've set out above I'm satisfied that around the time Mr A was making these payments Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Mr A?

Revolut says considering the merchant category code for the payments, the card payments being biometrically approved by Mr A and B being a supported merchant that its customers

can make payments to, there was no reason for it to suspect there to be any issues. It has not explicitly said that it provided any warning prior to these card payments being made.

I don't think this was a proportionate way to deal with the risk that these payments presented. I think Revolut needed to do more.

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.

Taking that into account, I think Revolut ought, when Mr A attempted to make the third 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. I accept that there are a wide range of scams that could involve payments to cryptocurrency providers. I am also mindful that those scams will inevitably evolve over time (including in response to fraud prevention measures implemented by banks and EMI's), creating ongoing challenges for banks and EMI's.

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 A by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

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

If Revolut had provided a warning of the type described, would that have prevented the losses Mr A suffered from the third payment onwards?

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. I think that a warning of the type I've described would have identified to Mr A that his circumstances aligned with an increasingly common type of scam.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr A's payments, such as being assisted by an investment broker and being asked to download remote access software. I've not seen any evidence to suggest

that Mr A was told to disregard any warnings or that the fraudster had given him a cover story to say if the payments were challenged.

Mr A tried to make payments from his current account to his Revolut account on 9 December 2022 and 10 December 2022. His bank told us that it spoke to Mr A twice in connection with those payments. I have listened to recordings of the two conversations Mr A had with his bank. I've not heard anything that makes me think Mr A would have misled a financial business or that he would have moved past a warning. In the conversations I have heard, Mr A's bank didn't provide a cryptocurrency scam warning. The bank was predominately concerned with how Mr A had opened the Revolut account and whether he was able to control it himself.

Therefore, on the balance of probabilities, had Revolut provided Mr A with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe he would have been receptive to it and that it would have resonated with his circumstances. I am not persuaded that Mr A would have trusted the fraudster more than Revolut.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr A 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 third payment was made to another financial business (a cryptocurrency exchange based in another country) 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 A might have been at risk of financial harm from fraud when he made the third 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 A went on to suffer. 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 B does not alter that fact and I think Revolut can fairly be held responsible for Mr A's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr A has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr A could instead, or in addition, have sought to complain against those firms. But Mr A 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 consumer'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 A's loss from the third payment onwards (subject to a deduction for Mr A's own contribution which I will go on to consider later in this decision).

Revolut has argued that we are applying the provisions of the CRM Code to complaints against it, despite it not being a signatory and in circumstances where the CRM Code would not, in any case, apply. I do not seek to treat Revolut as if it were a signatory to the CRM Code, and I have not sought to apply it by analogy. The CRM Code does not apply to card payments like the ones Mr A made. I've explained in some detail why I think it fair and reasonable that Revolut ought to have identified that Mr A may have been at risk of financial harm from fraud and the steps it should have taken before allowing the third card payment to leave Mr A's account. And the Financial Ombudsman Service's jurisdiction is neither the same as nor tied to the CRM Code.

Revolut has also highlighted that the mandatory reimbursement rules were not in force at the time of events complained about and so should not be applied either. But the PSR's mandatory reimbursement scheme is not relevant to my decision about what is fair and reasonable in this complaint. They were not in force when Mr A made the payments in dispute and, in any event, they do not apply to card payments. I do not consider that the fact that the PSR's reimbursement rules are narrower than the circumstances in this complaint means that Revolut should not compensate Mr A in circumstances when it failed to act fairly and reasonably, as I have found was the case here.

I do not consider it to be relevant that the circumstances here do not fall under the specific definition of an APP scam set out in the CRM Code and DISP rules. Those definitions define the scope of the CRM Code and eligibility of payers to complain about a payee's PSP respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made the third payment without providing a warning to Mr A.

Overall, considering what is fair and reasonable in all the circumstances, I'm satisfied Revolut should have made further enquiries and provided a warning before processing the third payment. If it had, it is more likely than not that the scam would have been exposed and Mr A would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mr A's loss.

Should Mr A bear any responsibility for his losses?

I've thought about whether Mr A should bear any responsibility for his losses from the third payment onwards. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Mr A's own actions and responsibility for the losses he has suffered.

I recognise that, as a layman who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Mr A has recalled that the fraudster and his company were very professional, and that the fraudster put in place security processes that mirrored what a genuine financial business would do. I can see why

the look and feel of a platform to access and manage profits could give some validation to the situation.

I've not been provided with all of the messages that Mr A exchanged with the fraudster which makes it difficult for me to gain a complete understanding of exactly how each interaction developed. But from what I have been told about the scam, I'm mindful that Mr A accepted the situation at face value. He's said that he received a phone call via WhatsApp from an unknown person. This unknown person told Mr A that he could make him a lot of money. I think Mr A should have been more suspicious of this unsolicited contact and questioned in his own mind whether it was a credible opportunity right from the outset.

Although I accept it is possible to make significant profits when investing in cryptocurrency, I also think Mr A should have questioned the plausibility of the developing situation, especially when he faced difficulties withdrawing the alleged profits.

The fraudsters told Mr A he'd made a profit of over £23,000, but he needed to pay 30% of the amount he was due to receive up front as part of anti-money laundering checks which he would receive back once the checks had been completed. Mr A paid the money but was then told that as the funds came from a cryptocurrency exchange, he had to make a *"Reversal Transaction of PPI Liquidity (Matching Transfer) of £22,840.00 onto your cryptocurrency Revolut account wallet".* This explanation for needing to pay a significant amount of money does not make sense.

Mr A was then told that he needed to pay a further £23,000 due to *"Escrow Requirements."* When Mr A challenged this, he was informed that he could pay 10% of the total due back to him instead as this would be sufficient to execute the final transfer of money into his account.

I recognise that the scam operates on a cruel mechanism by always making the victim believe that one final payment is all that's required to get back what they've put in and to access the profits they've made. But the funds that Mr A was being asked to pay increased significantly and ultimately totalled more than the amount of profit he thought he'd made, which I think should have given him cause for concern. I also think Mr A should have been concerned that he was told he needed to pay a further £23,000, but this was then reduced to £4,500 seemingly for no reason.

Looking at the circumstances as they are here, I think Mr A should have realised there was a possibility the situation was not genuine. As such, it would not be fair to require Revolut to compensate him for the full amount of his losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mr A in relation to the payments he made from the third payment onwards because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

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

The payments were made by card to a cryptocurrency provider. Mr A sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that B provided cryptocurrency to Mr A, which he subsequently sent to the fraudsters. So, I don't think it would be fair and reasonable to conclude that Revolut should have done anything more to try and recover Mr A's funds.

Putting things right

To put things right, Revolut Ltd should now:

- Pay Mr A 50% of the payments he made from the third payment onwards – a total of £20,825
- Pay 8% simple interest per annum on £20,825 from the date of each payment to the date of settlement*

I consider that 8% simple interest per year fairly reflects the fact that Mr A has been deprived of this money and that he might have used it in a variety of ways.

*If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from the interest I've awarded, it should tell Mr A how much it's taken off. It should also give Mr A a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

For the reasons given above, I uphold this complaint in part and require Revolut Ltd to pay Mr A as I have set out above.

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

Claire Marsh
Ombudsman