DRN-4448984

The complaint

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

What happened

In early 2023, Mr W came across an advert on a social media platform. It appeared to show that two celebrities had been very successful at trading in cryptocurrency.

Mr W accessed a website, which he says he was very impressed with. He decided to leave his contact details using a form on the website and subsequently he was contacted by someone claiming to represent the investment company. They told him that he could purchase cryptocurrency, as well as shares using the platform.

Unfortunately, this was not a genuine investment opportunity and he was actually communicating with a fraudster.

The fraudsters asked for an initial investment of £150 – which he believes was paid using his account at N (though he is unsure when this payment was made). Mr W also set up an account with a cryptocurrency platform – "S". The fraudster suggested that Mr W open an account With Revolut – advising that it was standard practice for consumers to have a dedicated account for investments.

The fraudster helped Mr W set up his accounts using remote access software. Mr W identified that there was a discrepancy between the name of the initial company and the one he was making payments to. It was explained that one firm introduced clients to another. The fraudster claimed to be only receiving commission of around 2-3% on each trade.

On 18 April 2023, Mr W paid £5,000 from his account at another bank – "N" – to his account at Revolut and from there to S. From S the money was converted into cryptocurrency and sent to a wallet controlled by the fraudster.

Soon after making this payment Mr W found negative reviews of the platform online and asked the fraudster about this. The fraudster dismissed the negative reviews and directed him to a website with positive reviews. Mr W also requested a withdrawal of some of his money and he received £475 into his account at N. However, having seen the negative reviews, he doesn't appear to have regained confidence in the fraudsters and in early May 2023, he asked to withdraw £5,000 from his trading account.

Soon after Mr W received an email which appeared to come from a legitimate cryptocurrency exchange (but had actually been impersonated by the fraudsters). The email claimed that Mr W would need to pay fees to 'liquidate' his investment. Mr W was concerned, so he contacted the genuine cryptocurrency exchange. At that point the scam was revealed and, on 10 May 2023, Mr W reported the matter to Revolut.

Revolut rejected his claim. It explained that it had provided several warnings to Mr W, including asking him for the purpose of the payment. He indicated the payment was for 'goods and services' rather than 'investment' so he didn't receive the most relevant warning. It also thought that Mr W had acted with contributory negligence by failing to choose the correct payment reason. It also said that the account opening reason was given as transfers and that's what the account was used for.

Mr W referred the matter to our service through a professional representative and one of our Investigators upheld the complaint in part. They argued that based on what Revolut knew about the payment (that it was going to a cryptocurrency exchange) it ought to have provided a warning that was specific to cryptocurrency investment scams and, if it had done, the scam would have come to light and Mr W's loss would have been prevented. However, they also thought that Mr W should bear some responsibility for his loss – as he hadn't carried out adequate checks into the company and hadn't picked the most appropriate purpose for the payment when asked by Revolut.

Mr W accepted our Investigator's recommendation, but Revolut did not. In summary it argued:

- It has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of *Philipp v Barclays Bank UK plc [2023] UKSC 25*.

- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment ("APP") fraud. By suggesting that it does need to reimburse customers, it says our service is erring in law.

- It would not be required to reimburse 'self-to-self' transactions even if it were a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("CRM Code"). And, our service appears to be treating Revolut as if it were a signatory to the CRM Code.

- The Payment Service Regulator's ("PSR") proposed (at time of reply) mandatory reimbursement scheme will not require it to refund payments made in these circumstances either.

- 'Self-to-self' payments don't meet either the Dispute Resolution Rules ("DISP Rules") or CRM Code definition of an APP scam.

- Mr W was grossly negligent by ignoring the warnings it gave. The PSR's mandatory reimbursement scheme will allow it to decline claims where a consumer has been grossly negligent, taking into account any warnings a firm has provided.

- Mr W's loss did not take place from his Revolut account as he made a payment to his own cryptocurrency wallet before transferring that cryptocurrency to the fraudster. It's unfair and irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions. Other firms will have a better

understanding of the destination of the funds and/or Mr W's finances and account activity.

As no agreement could be reached, the case was passed to me for a final decision.

What I've decided – and why

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

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

For the reasons I shall set out below, I've decided that Revolut should have provided a written warning specific to cryptocurrency investment scams prior to the payment in dispute. If it had done so, I'm satisfied the scam, as well as the loss to Mr W from that payment, would more likely than not have been prevented. But I am also satisfied that in the circumstances of this complaint, Mr W 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 consumer modified the starting position described in *Philipp,* by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with consumer and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

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

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in April 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

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

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

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

---

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

[2] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

[3] 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.

- 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[4], 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.

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

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

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

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

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Should Revolut have recognised that Mr W was at risk of financial harm from fraud and were the steps it took to warn him sufficient?

It isn't in dispute that Mr W has fallen victim to a cruel scam here, nor that he authorised the disputed payments he made to his cryptocurrency wallet (from where his funds were subsequently transferred to the fraudster).

Whilst I have set out in detail in this decision the circumstances which led Mr W 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 Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr W might be the victim of a scam.

I'm satisfied for the same reasons as the investigator that the payment in dispute was identifiably going to a cryptocurrency provider. The name of the merchant is a reasonably well-known cryptocurrency provider and the sort code of the account is associated with a payment service provider for cryptocurrency firms. I'm also aware that cryptocurrency exchanges like S generally stipulate that the account used to purchase cryptocurrency at its exchange must be held in the name of the account holder. Revolut would have been aware of this fact.

But by April 2023, firms like Revolut had been aware of the risk of multi- stage scams involving cryptocurrency (that is scams involving funds passing through more than one account controlled by the customer before being passed to a fraudster) 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 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[5]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions.

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 the vast majority of

[5] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.

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.

So, taking into account all of the above, I am satisfied that, by the end of 2022, prior to the payment Mr W made in April 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

So I've gone onto consider, taking into account what Revolut knew about the payments whether it ought to have identified that Mr W might be at a heightened risk of fraud.

Should Revolut have identified that Mr W might be at a heightened risk of fraud?

Mr W's account was opened for the purpose of the scam – so there was no other account activity (other than the credit to the account) which came before. I accept that this didn't give Revolut any real picture of how Mr W might normally operate his account.

Nevertheless, Revolut ought to have identified, in April 2023, that a £5,000 payment to a cryptocurrency provider presented additional risk to its customer. It seemingly did recognise this risk, so I've gone onto consider whether the steps it took to warn its customer were sufficient.

Revolut initially provided a very general warning, that didn't contain any information about cryptocurrency or investment scams. I can't reasonably conclude that this warning would have alerted Mr W to the fact he might be falling victim to a cryptocurrency scam or that it was proportionate to the risk the transaction presented.

Mr W also saw a second set of warnings. They suggested that the payment had a high chance of being related to a scam, but didn't explain why. They also provided some general information about the risk of scams, but nothing specific to cryptocurrency or investments.

He was then asked to provide a reason for the payment. He chose 'goods and services', when investment was also an option. Mr W says that the fraudsters told him to select this option and, at the time, had control of his device through remote access software. I understand that due to restrictions Revolut have in place, it would not have been possible for the fraudster to have been in control of the application at this time.

So, while I accept that Mr W may have been instructed to choose this option, I'm more sceptical of his claim that another party was in control of his device at the relevant time and, on balance, it seems more likely that Mr W would have seen any warning that Revolut would have displayed. This, as I'll come onto, is important.

The warning Mr W did see contained information relevant to purchase scams, but was understandably not relevant to investment scams.

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 W attempted to make the payment in dispute knowing that it 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 W by covering the key features of scams affecting many customers, not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mr W incurred after that point?

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, such as finding the investment through an advertisement endorsed by a public figure, being assisted by a broker and being asked to download remote access software so they could help him open a cryptocurrency wallet.

I've also reviewed some of the text conversations between Mr W and the fraudsters (though I note that Mr W appears to have spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations or seen any messages which predate the payment in dispute). But, I've found nothing within those conversations that suggests Mr W was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr W expressed mistrust of Revolut or financial firms in general. In fact, Mr W appears to be quite suspicious of the fraudster after he made the payment in dispute.

I acknowledge that Mr W seems to have been directed by the fraudsters to select the payment reason, but as I've set out, I don't think the warning that Revolut should have provided ought to have been dependent on Mr W's choice of payment purpose, so I don't think this is particularly significant.

N (the origin of the money that funded the £5,000 transaction) says that it also provided a warning to Mr W. He can't recall which warning he saw and unfortunately N is unable to evidence exactly which warning was displayed. N says that there would have been a warning specifically about investing in cryptocurrency – though that warning focuses more on control of the cryptocurrency account, rather than other features of a cryptocurrency investment scam. In any case, without knowing what was selected, I can put little weight on

what Mr W *might* have seen and, as with Revolut, he says that he was directed to pick certain payment reasons, so he may not have seen the most relevant warning.

I've also considered that Mr W had received modest actual returns at the point of suggested intervention, but also that he started to become suspicious soon after making the £5,000 payment (as I'll discuss below). Taking everything into account, the weight of evidence persuades me that Mr W was not so taken in by the fraudsters that he wouldn't have listened to the advice of Revolut.

Therefore, on the balance of probabilities, had Revolut provided Mr W 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 paused and looked more closely into the broker before proceeding (for example, by carrying out further research, as he did later). I'm satisfied that a timely warning to Mr W from Revolut would more than likely have caused him to have more significant suspicions at an earlier point and that, in light of that warning, he would not have gone ahead with the payment.

Is it fair and reasonable for Revolut to be held responsible for some of Mrs S' loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr W paid money using his Revolut account to another account in his own name, rather than directly to the fraudster, so he remained in control of his money after he made the payments, and there were further steps before the money was lost to the scammer.

But as I've set out above, I think that Revolut still should have recognised that Mr W might have been at risk of financial harm from fraud when they made the payment in dispute, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mr W suffered. 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 W's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr W'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 W 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 W could instead, or in addition, have sought to complain against those firms. But Mr W has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr W'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 W's loss (subject to a deduction for his own contribution which I will consider below).

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. It also argues that the PSR's APP reimbursement rules will not require Revolut to reimburse Mr W.

I do not seek to treat Revolut as if it were a signatory to the CRM Code. I've explained in some detail the basis on which I think, fairly and reasonably, Revolut ought to have identified that Mr W was at risk of financial harm from fraud and taken further steps before the payment in dispute debited his account.

I'm also aware that the PSR's APP Reimbursement Rules would not require Revolut to reimburse Mr W. The PSR's rules are not relevant to my decision about what is fair and reasonable in this complaint. But I do not consider the fact that the PSR's rules do not make it compulsory for payment service providers to reimburse consumers who transfer money to an account in their own name as part of a multi-stage fraud, means that Revolut should not compensate Mr W in circumstances when it failed to act fairly and reasonably, as I have found was the case here. Indeed, the PSR has recently reminded firms that fraud victims have a right to make complaints and refer them to the Financial Ombudsman Service that exists separately from the intended reimbursement rights and that APP scam victims will still be able to bring complaints where they believe that the conduct of a firm has caused their loss (in addition to any claim under the reimbursement rules)[6].

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 payment in dispute without providing a warning to Mr W.

So, I'm satisfied Revolut should fairly and reasonably have provided a warning before processing the payment. If it had, it is more likely than not that the scam would have been exposed and Mr W would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mr W's loss.

Should Mr W bear any responsibility for his loss?

I've thought carefully about whether there should be any reduction to the amount reimbursed to Mr W. In doing so, I've taken into account what the law says about contributory negligence, as well as what's fair and reasonable in the circumstances of this case.

It's clear that there were sophisticated aspects to this scam – not least the faked celebrity endorsement and provision of a trading platform. I can understand why this would have given the scam a fairly high degree of plausibility.

I can see from the conversation between Mr W and the fraudster that his first £150 deposit appears to have made profit. This seems to have prompted Mr W to make the £5,000 payment. However, quite soon after making that payment it's evident that Mr W started to make his own enquiries about the legitimacy of the trading platform. He seems to have found only negative information about it and forwarded a link to the fraudster which suggested the trading platform was not legitimate. Despite the fraudster sharing links to a website with

[6] *"The reimbursement rules and their award limit differ from the rules which govern complaints under the Financial Ombudsman Service's dispute resolution rules (DISP). PSPs should therefore inform victims of APP scams that, in addition to their right to seek reimbursement under the reimbursement rules, they have the right to bring complaints against sending and receiving PSPs if they are dissatisfied with their conduct and consider this has caused their loss. Such complaints may ultimately be referred to the Financial Ombudsman Service."* PSR PS23/4 7.18

positive reviews of the trading platform (those websites appear to be linked to or created by the fraudsters), Mr W never seems to regain his faith in the legitimacy of the platform. By early May 2023, he'd asked for the returns of his funds and was sceptical about the fraudsters claim that they had been returned.

In advance of this decision I asked Mr W's representative what had led him to make further enquiries after making the £5,000 payment. Mr W said he started to see some bad reviews and became suspicious because of the way the scammer was acting. But from the messages I've seen it's not clear that the fraudster's conduct changed after the £5,000 payment. I think it's also unlikely that Mr W would have come across negative reviews of the (quite obscure) trading platform unless he went looking for them. I also asked Mr W for any messages that were exchanged between him and the fraudster prior to the payment in dispute, but he was unable to provide them – this makes it difficult to assess the plausibility of the fraudster's conduct prior to the payment being made.

Overall, having considered the matter carefully, I think Mr W likely rushed into making the £5,000 payment, having been enticed by the apparent returns on his initial investment. It's evident that Mr W could and did establish the legitimacy of the trading platform independently and I think, on balance, that he should have made those enquiries prior to the £5,000 payment.

Overall then, considering the fault on both sides, I think responsibility for that payment should be shared between Mr W and Revolut.

Recovery

As Mr W sent money to his own cryptocurrency account before converting it into cryptocurrency and sending it to the fraudsters, I can't see that there was any realistic prospect of recovery.

Putting things right

For the reasons I've explained, Revolut should reimburse 50% of the loss from Mr W's Revolut account, taking into account the return that he received (£475). Mr W has been unable to definitively identify the initial £150 payment made from his account at N, so I'm not going to take that payment into account when deciding redress. It follows that Revolut should reimburse Mr W a total of £2,262.50.

My final decision

For the reasons given above, I uphold in part this complaint and direct Revolut Ltd to pay Mr W:

- £2,262.50
- 8% simple interest per year on that amount from the date of each payment to the date of settlement[7].

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 22 November 2024.

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

Rich Drury
Ombudsman