DRN-5330970

The complaint

Mr C complains that Revolut Ltd didn't do enough to protect him from the financial harm caused by an investment scam, or to help him recover the money once he'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In August 2023, Mr C came across a company I'll refer to as "J" while he was researching investments. He clicked on a link to the website and was satisfied the website seemed genuine and featured a homepage which stated that J was a leading cryptocurrency market trader. He completed an online contact form and was subsequently contacted by someone claiming to be an account manager, who I'll refer to as "the scammer". The scammer said he could make good returns by investing in cryptocurrency and that he would be paid 10% commission on his profits.

Mr C could hear background noise which gave the impression the scammer was calling from a busy office, and he used trading terminology. Unfortunately, J was in fact a clone of a genuine company which was regulated by the Cyprus Securities and Exchange Commission (CySEC) and which had 'passporting' rights through the Financial Conduct Authority (FCA) – which meant it could offer its services to UK customers as recorded on FCA website.

The scammer told Mr C to download AnyDesk remote access software so he could show him how to log into his trading account. He also told him to open accounts with Revolut and a cryptocurrency exchange company which I'll refer to as "B". He told him to first purchase cryptocurrency through B and then load it onto an online wallet. Following these instructions, Mr C sent funds to Revolut from Bank B and on 21 August 2023 he exchanged £500 to cryptocurrency on the Revolut platform. Between 28 August and 13 September 2023, he made three card payments to B totalling £11,000. The payments were partly funded by a loan he took out under the guidance of the scammer.

On 14 September 2023, Mr C asked to make a withdrawal and was told he'd have to pay fees, eventually realising he'd been scammed when he was unable to contact the scammer and his trading account was blocked.

He complained to Revolut when he realised he'd been scammed. Revolut successfully recovered £5,000 via the chargeback process, but the other claims were successfully defended and Revolut refused to refund those funds.

Mr C complained to this service with the assistance of a representative. He said he wasn't an experienced investor and that he'd believed the scammer was genuine because he'd had access to the trading portal and had done some basic research. He said he'd received a successful chargeback of £5,000 and questioned why Revolut had only recovered half of his loss. He also said that Revolut didn't intervene or give him any effective warnings.

Mr C's representative said that even though there was no spending history to compare the payments with, there were obvious red flags including the fact Mr C had made high value payments in quick succession to new payees, which were high risk cryptocurrency merchants. He'd also made transfers into the account immediately before the payments, which is a known fraud indicator.

They said Revolut ought to have intervened on 28 August 2023, when Mr C paid £5,000 to B and that it should have asked probing questions about the payment including how he found the opportunity, whether there was a third party involved, whether he'd downloaded AnyDesk, whether he'd been promised unrealistic returns, whether he'd made any withdrawals and whether he'd done due diligence. It should also have educated him on the high-risk associated with crypto-assets and trading. And it done so, Mr C hadn't been prompted to give false answers and so he'd explained that he was acting under the instructions of a third-party, and it would have been apparent that he was falling victim to a scam.

Responding to the complaint, Revolut said the account was opened on 6 April 2023 and Mr C declared the purpose of the account was 'kids account'. It said cryptocurrency withdrawals don't fall within our jurisdiction, and two of the chargeback disputes were challenged, with B providing proof that the service was provided.

It explained it is an Electronic Money Institution ("EMI"), and typically this type of account is opened and used to facilitate payments to cryptocurrency wallets, so the type of payments weren't out of character with the typical way in which an EMI account is used and there was no reason for it to have been suspicious about the payments. It also said Mr C received educational emails prior to the scam telling him about current fraud patterns and educating him on how to keep his account safe, so he was aware of the means of social engineering used by scammers.

Finally, it argued that it was used as an intermediary to receive funds from Mr C's external account before transferring them to legitimate external accounts in his name, from where he subsequently lost control of the funds.

Our investigator explained this service doesn't have jurisdiction to consider the withdrawal of cryptocurrency as we can only consider complaints which are about FCA regulated activities. But he could consider the element of the complaint that related to the exchange of cryptocurrency on the Revolut platform.

Our investigator thought Revolut should have intervened when Mr C made the first payment on 28 August 2023 because the amount was significantly higher than previous transactions on the account and he was paying a high-risk cryptocurrency merchant. Further, he had selected the purpose of the account as 'kids account', which the payment contradicted. He said Revolut should have asked Mr C a series of questions about the payment to narrow down the specific scam risk and, once the risk had been identified, it should have provided a warning which covered off the key features of cryptocurrency investment scams. This would have resonated with Mr C and his loss would have been prevented.

He recommended that Revolut should refund the money Mr C had lost from the second payment onwards, and he didn't think Mr C had acted unreasonably because this was a sophisticated scam, which would have been difficult to uncover using basic research.

Finally, our investigator was satisfied that chargeback claims were raised when Revolut was made aware of the scam and there was nothing further it could have done given B defended the claims. And he didn't think Mr C was entitled to any compensation.

Mr C was satisfied with our investigator's recommendation, but Revolut asked for the complaint to be reviewed by an Ombudsman. It said the payments were to account in Mr C's own name, the fraudulent activity didn't occur on the Revolut platform and the payments weren't out of character or unexpected with the typical way in which an EMI account is used.

It argued that this service's recent reliance on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) amounts to a legal error and the question of whether Mr C was warned by his external bank is relevant to whether he acted negligently.

My provisional findings

I made the following findings in my provisional decision:

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

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

• The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.

• At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mr C modified the starting position described in Philipp, by expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks".

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 C and the Payment Services Regulations to carry out their 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 am 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.

Whilst the Consumer Duty does not 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 have 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 am also mindful that in practice, whilst 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 am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R:

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

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in 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 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;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 am also mindful that:

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

• Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of 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 Code2, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

• Since 31 July 2023, under the FCA's Consumer Duty3, 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".

• Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency5 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;

• in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and

• have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi- stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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

What did Revolut do to warn Mr C?

- Revolut didn't intervene or provide any warnings.

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

There's no dispute that this service can't consider the withdrawal of cryptocurrency on the Revolut platform, but we can look at the exchange Mr C made on 21 August 2023.

It isn't in dispute that Mr C has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to her cryptocurrency wallet (from where that cryptocurrency as subsequently transferred to the scammer). Whilst I have set out in detail in this decision the circumstances which led Mr C to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that he might be the victim of a scam.

Firstly, I don't think that Revolut would have had any reason to intervene when Mr C exchanged £500 to cryptocurrency on 23 August 2023.

I'm aware that cryptocurrency merchant stipulates 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 three payments out of the account would be credited to a cryptocurrency wallet held in Mr C's name.

By August 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions. By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions6. And by August 2023, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for the – 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 to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of. So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr C made in August 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at

an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in August 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 (including the Consumer Duty), 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.

I think Revolut should have identified that the first payment Mr C made to B on 28 August 2023 was high value, it was going to a cryptocurrency provider, and the purchase of cryptocurrency wasn't consistent with the account opening purpose. These circumstances should have led it to consider that Mr C was at heightened risk of financial harm from fraud.

In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr C before this payment went ahead. To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by August 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud.

Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

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 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.

In light of the above, I think that by August 2023, 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. I understand in relation to Faster Payments it already had systems in place that enabled it to provide warnings in a manner that is very similar to the process I've described. 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 that by August 2023, on identifying a heightened scam risk, a firm such as Revolut should 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 the payment was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. I am satisfied that, by August 2023, Revolut ought to have attempted to narrow down the potential risk further by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment Mr C was making and provided a scam warning tailored to the likely cryptocurrency related scam he was at risk from.

In this case, Mr C was falling victim to 'investment scam' – as such, I'd have expected Revolut to have asked a series of simple questions 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 C gave. I'd expect any such warning to have covered off key features of such a scam. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but as Mr C was sending funds to a cryptocurrency merchant, I'm satisfied the process should have resulted in a warning tailored to cryptocurrency investment scams.

As I have explained above, the Consumer Duty (which came into force on 31 July 2023 after an extended implementation period), required Revolut to take steps to avoid foreseeable harm – for example by having adequate systems in place to detect and prevent scams from 31 July 2023. 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 £5,000 payment to make further enquiries and with a view to providing a specific scam warning of the type I've described.

<u>If Revolut had provided a warning of the type described, would that have prevented the losses Mr C suffered from the payment he made to B on 28 August 2023?</u>

Bank B has confirmed that Mr C stated that the payments he was making from that account were for 'friends and family', but as he was sending funds to a cryptocurrency merchant, I would expect Revolut to have given him a written warning tailored to cryptocurrency investment scams, regardless of his responses to questioning around the purpose of the payment.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr C's payments, including the fact the Revolut account was newly opened, he was being advised by account manager, he'd been asked to download remote

access software, and he'd been instructed to make a onwards payments from the cryptocurrency exchange. Consequently, I would expect Mr C to have been warned that the investment was probably a scam.

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 haven't seen any evidence that Mr C was asked, or agreed to, disregard any warning provided by Revolut or any indication that he expressed mistrust of Revolut or financial firms in general. Neither do I think he'd developed a closeness of relationship with the account manager that Revolut would have found difficult to counter through a warning.

While it's clear he'd believed the scammer was genuine, the weight of evidence that I've outlined persuades me that he was not so taken in by the scam that he wouldn't have listened to advice from Revolut. And there's no evidence that he ignored an effective warning from Bank B. Therefore, on the balance of probabilities, had Revolut provided Mr C 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 and that he'd have paused and looked more closely into J before proceeding.

It's significant that J was a clone company and so a basic search would likely have shown information about the genuine company. But if Mr C had decided to proceed with the payment, as I'm satisfied Revolut would have had enough information to detect the scam, I would expect it to have gone a step further and required Mr C to engage in further discussion about the payment via it's in app chat when it should reasonably have told him how to check he was dealing with a genuine company, including contacting the details on the CySEC or FCA websites.

I've no reason to think Mr C wouldn't have followed this advice and so I'm satisfied he'd have discovered that the investment was a scam. Consequently, I'm minded to agree with our investigator that Revolut should refund the money he lost from the second payment onwards.

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

I've set out in some detail above, I think that Revolut still should have recognised that Mr C might have been at risk of financial harm from fraud when he made the first payment on 28 August 2023, and in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses he suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr C's own account does not 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.

I've also considered that Mr C 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 he could instead, or in addition, have sought to complain against those firms. But Mr C has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr C's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained 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.

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have 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 do not intend to comment on it. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is 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. I'm satisfied I've done so.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr C's loss.

Should Mr C bear any responsibility for his loss?

Mr C has described that he came across J when he was research investments, and so there was nothing suspicious about the way he was introduced to the investment.

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I don't think it was unreasonable for him to have believed what he was told by the broker in terms of the returns he was told were possible, notwithstanding the fact it was highly implausible.

Mr C was an inexperienced investor and because J was a clone of a genuine company, there was no information available online about J which would have raised concerns. He hadn't been a victim of a scam before and without receiving scam information from Revolut, he wouldn't have known that downloading remote access software or transferring funds onwards from the cryptocurrency exchange are red flags for fraud and she wouldn't have known how to check the information he'd been given. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact he trusted the scammer and the fact he believed the trading platform was genuine and had his own log in details.

Significantly, Mr C wasn't given any scam warnings during the scam period, and he's said he thought the investment must have been legitimate, otherwise, his bank would have stopped him. So, I don't think he can fairly be held responsible for his own loss.

Recovery

I don't think there was a realistic prospect of a successful recovery because Mr C paid an account in his own name and moved the funds onwards from there.

Mr C's own testimony supports that he used cryptocurrency exchanges to facilitate the payments. Its only possible to make a chargeback claim to the merchant that received the disputed payments. B was able to evidence they'd done what was asked of them. That is, in exchange for Mr C's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. Therefore, I'm satisfied that Revolut's decision not to pursue the two chargeback claims that were defended was fair.

Compensation

The main cause for the upset was the scammer who persuaded Mr C to part with his funds. I haven't found any errors or delays to Revolut's investigation, so I don't think he is entitled to any compensation.

Developments

Mr C has indicated that he accepts my provisional findings, and Revolut hasn't responded.

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.

Because neither party has submitted any further evidence or comments for me to consider, the findings in my final decision will be the same as the findings in my final decision.

My final decision

My final decision is that Revolut Ltd should:

• Refund the money he lost from the first payment on 28 August 2023, less the money it successfully recovered.

• pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Mr C with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 13 March 2025.

Carolyn Bonnell
Ombudsman