DRN-4847776

The complaint

Mrs S is unhappy that Revolut Ltd won't reimburse money she lost to a scam.

What happened

On 8 May 2024, I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any more evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Mrs S had recently received a cash lump sum from her pension. In April 2023, she was looking to invest. She went online and came across an advert that suggested that a well-known media personality had made significant amounts of money trading in cryptocurrency. She left her contact details on an online form and was swiftly called back by someone claiming to represent an investment company.

The caller introduced her to a trading platform and invited her to make an initial deposit of £200. Mrs S agreed and made that payment using her debit card for another of her accounts held at a bank – "J". She was then passed to another person – "AW" who introduced themselves as her account manager. Mrs S says that she looked up AW on a website which is a register of brokers and could find him – listed as a broker working for a large investment bank. Mrs S didn't check the Financial Conduct Authority ("FCA") Register to see if the investment company was regulated (it wasn't, but a warning about the firm wasn't issued by the FCA until July 2023).

Mrs S was advised to open an account with Revolut – the fraudster claimed that Revolut was one of the firms which worked with cryptocurrency providers. The payments Mrs S made from Revolut were funded by her account at J.

The majority of the payments Mrs S made from Revolut went to a legitimate cryptocurrency firm – "C". From C Mrs S' funds were converted into cryptocurrency and sent to cryptocurrency wallets controlled by the fraudsters.

Her initial investment appeared to be doing well and she decided to make a modest withdrawal from the investment account on 5 May 2023. She was subsequently encouraged to make further deposits. Although returns were not guaranteed, the scammer told her that she could expect a return of around 50% (though quite what period this was over isn't clear). She was told that her capital was not at risk.

Mrs S says that she was cautious at first, she waited until 17 May 2023 to invest a further £800 and it wasn't until 31 May 2023, that she began to make more significant payments – two £5,000 payments on the same day. She believed that those payments were to fund a specific investment opportunity that had arisen.

By 7 June 2023, Mrs S wanted to withdraw her investment. She received an email which appeared to come from Revolut, but had in fact been sent by the fraudsters. It claimed that

due to restrictions in place on her account, she'd need to pay £8,000 to Revolut in order to release her profits.

Mrs S attempted to pay £8,000 to her account at C. C told our service that it 'instantly cancelled' her payment after an 'assessment' of her account activity. It hasn't said that it shared any concerns it may have had with Mrs S. The £8,000 payment was returned to her account at Revolut. The fraudsters instead instructed her to set up an account with another cryptocurrency firm – "B". And, instead of paying B directly the fraudsters used remote access software to show Mrs S (with help from her son) how to make a peer-to-peer cryptocurrency purchase.

After she made the £8,000 payment Mrs S says that she received emails that appeared to come from Revolut that suggested that final checks were being carried out before her funds could be released. The last time she heard from the fraudsters was 13 June 2023, her promised returns never arrived.

She reported the matter to Revolut through its in-app chat on 12 June 2023. It appears that, at that point, she still held some sort of belief (or, at least, hope) that Revolut had actually asked her for the £8,000 as she asked Revolut why she wasn't able to withdraw funds from her trading account.

A list of the payments made in relation to the scam are set out below:

Payment number	*Date and time*	*Recipient / Origin*	*Credit/Debit*	*Amount*
	24 April 2023	*J*	*Debit*	*£200*
	To/from Revolut			
1	*4 May 2023, 10:46*	*C*	*Debit*	*£30*
	4 May 2023, 11:51	*C*	*Credit*	*£30*
	5 May 2023, 17:36	*C*	*Credit*	*£96.42*
2	*17 May 2023, 16:50*	*C*	*Debit*	*£100*
3	*17 May 2023, 16:52*	*C*	*Debit*	*£700*
4	*31 May 2023, 13:24*	*C*	*Debit*	*£5,000*
5	*31 May 2023, 13:25*	*C*	*Debit*	*£5,000*
6	*7 June 2023, 17:13*	*C*	*Debit*	*£8,000*
	7 June 2023, 19:44	*C*	*Credit*	*£8,000 (payment returned)*
7	*8 June 2023, 9:20*	*C*	*Debit*	*£100*
8	*8 June 2023, 14:26*	*Peer-to-peer cryptocurrency purchase*	*Debit*	*£8,000*
	8 June 2023, 17:53	*C*	*Credit*	*£100*

Mrs S raised a claim with Revolut and subsequently made a complaint through a professional representative. Revolut declined her claim and said that it hadn't been provided with enough information in order to consider it.

Once the matter was referred to our service, Revolut argued that Mrs S' account was new, so it had no previous activity to compare her payments against and decide whether they were unusual. It also said that it was reasonably reassured by the credits into her account and that the reason she gave for opening her account was 'gaining exposure to financial assets', which was consistent with the activity she went on to undertake.

One of our Investigators looked into the complaint and upheld it in part. They thought that Revolut should have identified that Payment 5 was concerning and should have questioned Mrs S about it before it debited her account. If Revolut had done this, the Investigator thought that the scam would have come to light and Mrs S' further loss would have been prevented. However, they also thought that Mrs S had a role in what happened and should have been more sceptical about the returns being offered and the lack of risk to her capital. The Investigator thought that a fair deduction to the amount reimbursed would be 50%.

Mrs S said that she was disappointed, but accepted the outcome. Revolut didn't agree. In summary, it said:

- *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"). Our service appears to be treating Revolut as if it were a signatory to the CRM Code.*

- *The Payment Service Regulator's ("PSR") 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.*

- *Mrs S 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.*

- *Mrs S' loss did not take place from her Revolut account as she made payments to her own account at another regulated EMI before converting her money into cryptocurrency and 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 Mrs S' finances and account activity.

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

What I've provisionally 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 am minded to conclude Revolut should have provided a written warning specific to cryptocurrency investment scams when Mrs S was attempting the £5,000 payment made on 31 May 2023 at 13:24 ("Payment 4"). If it had done so, I'm satisfied the scam, as well as the loss to Mrs S from that payment onwards, would more likely than not have been prevented. But I am also satisfied that in the circumstances of this complaint, Mrs S should bear some responsibility (50%) for the losses she suffered.

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.*
- *The express terms of the current account contract may modify or alter that position. For example, 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 duty to do so.*

In this case, the terms of Revolut's contract with Mrs S at the time did expressly require it to refuse or delay a payment for a number of reasons. Those reasons included "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 Mrs S and the Payment Services Regulations to carry out her 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 in Mrs S' case, 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 May and June 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 that view, 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; and*
- *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:

- *FCA regulated firms are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6)[3].*
- *Over the years, the FSA, and its successor the FCA, 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 here, but I nevertheless consider these*

---

[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.

requirements to be relevant to the consideration of a firm'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) and it has since been withdrawn, 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 the practices articulated in the BSI Code remain a starting point for what I consider to have been the minimum standards of good industry practice in May 2023 (regardless of the fact the BSI Code was withdrawn in 2022).*

- *Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency. 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 the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.*

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably in May and June 2023:

- *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 financial harm from 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;*
- *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.*

<u>Should Revolut have recognised that Mrs S was at risk of financial harm from fraud and were the steps it took to warn her sufficient?</u>

It isn't in dispute that Mrs S has fallen victim to a cruel scam here, nor that she authorised the disputed payments she made to her account at a cryptocurrency provider (from where her funds were subsequently converted into cryptocurrency and transferred to the scammer).

Whilst I have set out in detail in this provisional decision the circumstances which led Mrs S to make the payments using her Revolut account and the process by which that money

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

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 Mrs S might be the victim of a scam.

Mrs S' Revolut account was newly opened for the scam, so Revolut had no sense of what typical account activity for her was – in the same way that J, as her current account provider, is likely to have had. All of the activity on her Revolut account was related to the scam and I accept that this was broadly consistent with the reason she gave for opening the account – that is to 'gain exposure to financial assets'.

I'm also aware that C (which, actually operates two separate entities in the U.K. – one is a regulated EMI, the other is an unregulated cryptocurrency firm – Mrs S likely held an account with both) stipulates that the account that is used to fund, and receive payments from, a customer's account must be held in the name of the customer. Revolut would have reasonably been aware of this. So, it could have reasonably assumed that all of the payments in question were being made to an account held in Mrs S' own name.

But by May 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]. And by May 2023, when these payments took place, further restrictions were in place[6]. 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 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 payments Mrs S made in May 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.

---

[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.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

[6] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mrs S' own name should have led Revolut to believe there wasn't a risk of fraud.

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

Should Revolut have identified that Mrs S might be at a heightened risk of fraud?

I'm conscious that the initial payments to C were modest and there were several credits to her Revolut account from C during the period. There were also fairly significant gaps between some of the payments – a little under two weeks between the initial payments and the first of any size and then a further two weeks before Mrs S made two £5,000 payments on the same day (on 17 May 2023).

I can't see any reason for Revolut to have been particularly concerned about the payments that were made prior to 17 May 2023. They were for relatively modest amounts and fairly spread out. I can't see that these payments alone would have indicated that Mrs S might be at risk of financial harm from fraud.

I also need to take into account that Revolut needs to strike a balance between protecting against fraud and not unduly hindering legitimate transactions, so I don't think Revolut ought to have been so concerned about those payments that it ought to have provided specific warnings to Mrs S at this point.

However, Payment 4 (the first £5,000 payment on 17 May 2023) was significantly higher than the payments which had come before it. It was more than seven times larger than the previous payment and, in my view, the payment was a clear escalation in value and had the potential to cause significant financial harm to Mrs S. Taken together with the earlier payments, I consider Revolut ought reasonably to have identified that a pattern had developed – of increasingly large payments to a cryptocurrency provider – that could indicate Mrs S was at risk of financial harm from fraud.

So when Mrs S attempted to make Payment 4, taking into account what I've said about the increased risk that cryptocurrency transactions presented, I think Revolut ought fairly and reasonably to have recognised the risk had increased and there was a heightened possibility that the transaction linked to a cryptocurrency scam. In line with the good industry practice that I've set out above, I think Revolut should have provided a specific and impactful warning, before allowing Payment 4 to go ahead. But it did not provide any warning in relation to this payment.

I'm aware that Revolut did provide a warning when Mrs S made the first £30 payment. That warning said:

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

But I don't consider the provision of this warning in relation to a much earlier payment to be a proportionate response to the risk Payment 4 presented. While I understand it is intended to be a warning that covers a broad range of scenarios, it didn't, as I think a proportionate warning needed to, address the specific risk the payment presented.

To be clear, I do not suggest that in May 2023 every payment used to purchase cryptocurrency presented such a heightened risk of fraud that Revolut should have warned its customer before processing them. Instead, as I've explained, I think it was a combination of the characteristics of this payment and the circumstances in which the payment was made (including the payments Mrs S had made before) to a cryptocurrency provider, that ought to have given Revolut sufficient cause for concern that Mrs S could be at risk of suffering financial harm from fraud when she attempted to make Payment 4. In those circumstances, it should fairly and reasonably have taken additional, proportionate, steps before completing the payment.

What kind of warning should Revolut have provided?

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

Taking that into account, I think Revolut ought, when Mrs S attempted to make Payment 4, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

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

If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mrs S incurred after and including Payment 4?

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 her open cryptocurrency wallets.

Although Mrs S has provided some evidence of her correspondence with the fraudsters it appears that the majority of those conversations took place over the phone (so I haven't been able to listen to them). But I've seen nothing to suggest that Mrs S was asked, or agreed to, disregard any warnings provided by Revolut. The Investigator also contacted J to find out whether it had provided Mrs S with any warnings. It confirmed that it hadn't, other

than one in relation to safe account scams (which wasn't relevant to her circumstances). While C says that it returned Mrs S' payment due to the account activity, it has indicated that it did not share any of its concerns with Mrs S or provide a warning to her.

I've also taken into account that Mrs S had received modest actual returns at the point of suggested intervention (I can see that the fraudsters credited her account at C with an amount of cryptocurrency equal to the sum withdrawn back to her Revolut account on 5 May 2023). Undoubtedly this would have added some plausibility to the scheme, but I haven't seen sufficient compelling evidence that Mrs S was so taken in by the fraudsters that she would have disregarded a clear and specific warning.

Overall, on the balance of probabilities, had Revolut provided Mrs S with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams. I'm satisfied that a timely warning to Mrs S from Revolut would have very likely caused her to have sufficient doubt to not go ahead with the payments.

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 Mrs S paid money using her Revolut account to another account in her own name, rather than directly to the fraudster, so she remained in control of her money after she made the payments, and there were further steps before the money was lost to the scammer.

However, for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mrs S' losses from Payment 4, subject to a deduction for Mrs S' own contribution towards her loss. As I have explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice, I consider it fair and reasonable that Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

I have also taken into account that Payment 4 was made to a regulated business – C, and Mrs S might potentially have a claim against C in respect of its actions (although C is not a party to this complaint and so I make no finding about its role here). The same is true of J – the origin of the money that funded the scam.

Whilst the dispute resolution rules (DISP) give me the power (but do not compel me) to require a financial business to pay a proportion of an award in circumstances where a consumer has made complaints against two financial businesses about connected circumstances, Mrs S has not referred a complaint about C or J to me and DISP does not empower me to instruct Mrs S to make or refer a complaint to me about another business.

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 Payment Service Regulator's ("PSR") proposed mandatory reimbursement scheme will not require Revolut to reimburse Mrs S. 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 Mrs S was at risk of financial harm from fraud and taken further steps before Payment 4 debited her account.

I'm also aware that the PSR's mandatory reimbursement scheme would not require Revolut to reimburse Mrs S. The PSR's proposals are not yet in force and 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 does not propose to 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 Mrs S 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)[7].

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 payment 4 without providing a warning to Mrs S.

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

Should Mrs S bear any responsibility for her loss?

In considering this point, 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 complaint.

I recognise that, as a layman, there were aspects to the scam that would have appeared convincing. Mrs S was introduced to it through an advert appearing to show a well-known media personality promoting cryptocurrency. Mrs S has provided a snippet of this advert and I've seen many like it. In my experience, they often appear as paid adverts on social media websites and a reasonable person might expect such adverts to be vetted in some way before being published.

I've also taken into account the provision of the trading platform (which, I understand, would have used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that fraudsters used the apparent success of early trades and, as in this case, the apparent ability to withdraw funds to encourage increasingly large deposits. So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mrs S to be reduced. I think it should be.

I'm concerned that Mrs S was told that there was no risk to her capital and I think that the suggested returns of 50% (even if over a period of months) should have led her to have some concerns about the legitimacy of the scheme. I understand Mrs S had some

---

[7] *"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

experience of investing in shares and is likely to have understood that all investment carries risk and that the returns being suggested were likely to be too good to be true. I think these claims should reasonably have put Mrs S on notice that something might not have been right and she should have made further enquiries, certainly before making the larger payments beginning with Payment 4.

I understand that she did carry out checks on the broker and while that indicated that AW was a registered broker, it did not suggest he was working for the investment company that Mrs S thought she was dealing with. In fact, it showed that he worked for a large investment bank, so I'm not sure that the enquiries she did make should have provided much reassurance.

Once Mrs S was, or should have been, on notice that the scheme was too good to be true, I think that she should have made further enquiries that would have likely led her to realise that the scheme wasn't genuine. She could, for example, have found that the investment company wasn't regulated in the U.K. (or seemingly anywhere else) and that the celebrity had made a number of well-publicised statements saying they did not promote cryptocurrency. To be clear, I do not suggest that it was necessarily unreasonable for Mrs S not to have made these enquiries prior to engaging with the fraudsters. I don't think it was unreasonable for her to take the advert she saw at face value, instead I think it was the unlikely claims made by the fraudsters (such as the lack of risk to her capital) that should have led her to make these further enquiries that should have revealed the scam.

And, once Mrs S received a request for fees to release her money, particularly one that supposedly came from Revolut, I think she certainly should have considered this request to be unusual and taken further steps before agreeing to make the payment. It would have been relatively straightforward to contact Revolut in its app to confirm the legitimacy of the email (a step she took later when she reported the scam).

Taking all of the above into account I think that Revolut can fairly reduce the amount it pays to Mrs S because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

<u>Could Revolut have done anything else to recover Mrs S' money?</u>

I've also thought about whether Revolut could have done more to recover the funds after Mrs S reported the fraud.

Most of the payments were sent to Mrs S' own account at C, converted into cryptocurrency and then sent to the fraudster. I can see that all of the money was paid away in cryptocurrency, so no recovery would have been possible. The final payment was a peer-to-peer cryptocurrency purchase. While I can't see that Revolut attempted to recover this payment, as the seller is unlikely to be involved in the scam and genuinely sold cryptocurrency, it would be unlikely to be fair for any funds to be recovered from them. So I don't think there was anything more Revolut could've done to recover Mrs S' money in these circumstances.

My provisional decision

For the reasons given above, I am provisionally minded to uphold in part this complaint and intend directing Revolut Ltd to pay Mrs S:

- *50% of payments 4, 5 and 8 – a total of £9,000.*
- *8% simple interest per year on that amount from the date of each payment to the date of settlement.*

Both Mrs S and Revolut accepted my provisional 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.

As Mrs S and Revolut have accepted my provisional decision, my final decision is the same as my provisional decision, which I've set out above.

My final decision

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

- 50% of payments 4, 5 and 8 – a total of £9,000.
- 8% simple interest per year on that amount from the date of each payment to the date of settlement.

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 10 July 2024.

Rich Drury
Ombudsman