DRN-5093793

The complaint

Mrs A complains about the actions of Revolut Ltd when she lost money to a scam.

Mrs A is being represented by a claims management company but for ease I'll only refer to Mrs A.

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 early July 2023 Mrs A was added to a group chat on a messaging service – she doesn't know how the third party obtained her number – and took an interest in the investment discussion on the group. After doing some research into the people providing trading advice on the group she was told to create an account on a platform run by the same people in the group chat. She was then told to wait for signals on the group chat to start purchasing crypto. Mrs A then went on to make the following payments;

Date	Type of transaction	Amount
11 July 2023	Credit from crypto exchange	£81.86
11 July 2023	Debit card to crypto exchange	£81.82
12 July 2023	Credit from crypto exchange	£3,089.70
17 July 2023	Debit card to crypto exchange	£4,119.60
17 July 2023	Debit card to crypto exchange	£3,000
18 July 2023	Debit card to crypto exchange	£10,000
18 July 2023	Debit card to crypto exchange	£5,000
20 July 2023	Debit card to crypto exchange	£4,149.66
24 July 2023	Debit card to crypto exchange	£3,089.70
31 July 2023	Credit from crypto exchange	£2,470.56
	Total loss	**£35,082.90**

After her account maintained a negative balance on the platform, she realised she had been scammed. So, she made a claim to Revolut to try and recover her money. Revolut considered the claim but said it wasn't prepared to provide Mrs A with a refund in the circumstances because it hadn't done anything wrong in allowing the payments to be sent. Unhappy with this response, Mrs A brought her complaint to this service.

Our investigator felt the complaint should be upheld in part. She said that by payment three here Revolut should've provided an in-app warning to Mrs A but that this wouldn't have likely stopped the scam at that point because she had traded in crypto before and that many of the key scam features – such as pressure to invest, failed withdrawal requests and payment for fees hadn't presented themselves yet. The investigator felt that by payment six Revolut should've stepped in again in the form of human intervention. And that Mrs A would've likely provided accurate and truthful responses to Revolut's questions which would've more than likely uncovered the scam. The investigator added that Mrs A should bear some

responsibility for her losses (50%) which leaves a total refund of £12,354.96 with 8% simple interest per year to be added to that amount.

Mrs A accepted the investigator's opinion.

Revolut disagreed and has asked for an Ombudsman's decision. In summary it said that this was a me2me case where money was sent by Mrs A to an account in her own name at the crypto exchange before being sent to the scammer. So, the money wasn't lost from the Revolut account. It said the payments here were not out of character for how an Electronic Money Institute (EMI) works at the moment. That's because restrictions by high street banks on people sending money to crypto exchanges leads customers to open an account with Revolut in order to make crypto investments. So, it didn't consider the payments unusual here. Revolut added that the banks that Mrs A used to send the money to her Revolut account should be considered in tandem with this complaint to see if Mrs A ignored any warnings.

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.

Having done so, I agree with the investigator that this complaint should be upheld in part and for largely the same reasons.

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

I've read and considered the whole file. But I'll concentrate my comments on what I think is relevant. If I don't mention any specific point, it's not because I've failed to take it on board and think about it, but because I don't think I need to comment on it to reach what I think is a fair and reasonable outcome.

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 Mrs A modified the starting position described in *Philipp,* by – among other things – expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*" (Section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

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

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in July 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 did in fact seek to take those steps, often by:

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

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

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

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017, BSI Code[3], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

- 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 July 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;
- 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 July 2023, Revolut should in any event have taken these steps.

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

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

By July 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 transactions. And by July 2023, when these payments took place, 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 them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs A made in July 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 July 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks. 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 most of the payments in this case were going to an account held in Mrs A'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 A might be at a heightened risk of fraud that merited its intervention.

By the time Mrs A sent the third payment here (£3,000) I think there was enough happening here that Revolut should've been suspicious. By that point Mrs A had sent over £7,000 to a crypto exchange with £3,000 being sent in one payment. And given what Revolut knew about the destination of the payment and the high value, I think that the circumstances should've led Revolut to consider that Mrs A was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

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

If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mrs A 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 don't think it would have. Like the investigator, I think a warning at this point in the scam would've come to early as Mrs A hadn't come across the usual pressure to make more payments from the scammer that is usually associated with such a scam. I've also considered that Mrs A had traded in crypto before by herself, hadn't had any failed withdrawal requests nor been asked to make any payments for fees.

However, by the time of the fourth payment (£10,000) here, I'm satisfied this payment represented a heightened risk of financial harm and Revolut should've therefore taken additional steps before allowing it to debit Mrs A's account. By this point the value of the payment had significantly increased by more than double the previous high value payment to the crypto exchange the previous day with over £21,000 being sent to the crypto exchange.

If Revolut had attempted to establish the circumstances surrounding the £10,000 payment, would the scam have come to light and Mrs A's loss been prevented?
Overall, I'm satisfied that if Revolut had asked some probing questions of Mrs A about why she was making the payment she would've been honest that she was being asked to make the payment in relation to an investment opportunity and that there was a third party involved in asking her to send the money to the crypto exchange. This would've been a clear red flag for Revolut who would been able to provide a clear warning to Mrs A that she was highly likely to be falling victim to an investment scam.

I've found no persuasive evidence to suggest that Mrs A was asked, or agreed to, disregard any warning and human intervention provided by Revolut. I've also seen no indication that Mrs A expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning.

Therefore, on the balance of probabilities, had Revolut provided Mrs A with an impactful human intervention that asked probing questions about the reasons for the payments followed by a clear warning giving 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 this before proceeding, as well as making further enquiries into cryptocurrency scams. I'm satisfied that a timely warning to Mrs A from Revolut would very likely have caused her to take the steps she did take later – revealing the scam and preventing her further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs A paid money from her Revolut account before forwarding it to an account in her own name at the crypto exchange, 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 partly responsible for Mrs A's losses from the £10,000 18 July payment, subject to a deduction for Mrs A'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.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs A might have been at risk of financial harm from fraud when they made the £10,000 payment, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses she 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 Mrs A's own account does not alter that fact and I think Revolut can fairly be held responsible for her 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.

Should Mrs A bear any responsibility for their losses?

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 won't go into detail here – as Mrs A accepted the investigator's view, but for completeness I agree with the investigator and broadly for the same reasons. My intention is not to further Mrs A's distress where she's already been the victim of a cruel scam. But certainly, by the time of the transaction I'm upholding, I think there were signs that things weren't quite right that she could have scrutinised further.

Mrs A was contacted out of the blue and didn't question how the third party had come across her details. Although Mrs A said she conducted some research I've not found any details of the scammer's details and that the fake company they used had a legitimate site. And given that Mrs A had traded in crypto before I'd expect her to have a better understanding of how the crypto markets work and that the gains she was promised (without a discussion about potential losses) were unrealistic.

As a result of the above, I believe Revolut can fairly deduct 50% from the final payment made towards this scam, to the refund it must make here.

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

I've thought about whether Revolut did enough to attempt to recover the money Mrs A lost, as there are some instances where debit card transactions can be refunded through making a chargeback claim.

A chargeback wouldn't have been successful for the debit card payments to the account in Mrs A's name at the genuine crypto exchange, as Mrs A was able to move the money onto the scammers. So, Mrs A duly received the service she paid for on her debit card. The debit card transactions and the transfers Mrs A made were subsequently lost from her other account when it was moved to the scammers. So, she couldn't claim that she didn't receive the goods or services paid for from her Revolut account to the crypto exchange nor that there were any further funds to recover from the crypto exchange.

As a result, I don't think Revolut have acted unreasonably by failing to pursue a chargeback claim or try and recover Mrs A's money here.

I note the investigator confirmed that Revolut wasn't aware of her vulnerabilities at the time of the payments here – so she's right to say that this means Revolut didn't treat Mrs A unfairly here. And I've seen that the investigator didn't make any award to Mrs A on the trouble and upset she says Revolut caused her after reporting this scam. Mrs A accepted the investigators opinion. But to be clear I agree with the investigator's reasoning here. And I won't be making any further award to Mrs A.

My final decision

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

- £12,354.96
- 8% simple interest per year on that amount from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 27 February 2025.

Mark Dobson
Ombudsman