DRN-5183438

The complaint

Mrs G is unhappy that Revolut Ltd haven't refunded money she lost as a result of a scam.

Mrs G is being represented by a claims management company but for ease of I'll only refer to Mrs G in the decision.

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 2023 Mrs G received an e-mail about investing in crypto. She clicked on the link and provided her contact details. She was then called by a representative of a merchant who introduced her to a trading platform and said the broker was regulated by the Financial Conduct Authority (FCA). Satisfied she was dealing with a legitimate company she proceeded to make the following payments via her Revolut account;

	Date	**Method**	**Amount**
1	11 April 2023	Transfer to crypto exchange	£9
	13 April 2023	Withdrawal	£80
	02 May 2023	*Card Payment to crypto exchange (declined)*	*£4,044.42*
2	02 May 2023	Card Payment to crypto exchange	£4,111.36
3	02 May 2023	Card Payment to crypto exchange	£1,871.33
	10 May 2023	Withdrawal	£105
4	15 May 2023	Card Payment to crypto exchange	£5,047.54
5	15 May 2023	Transfer to Third-Party	£100
6	15 May 2023	Transfer to Third-Party	£4,800
7	05 June 2023	Card Payment to crypto exchange	£5,922.95
8	06 June 2023	Card Payment to crypto exchange	£5,140.23
9	06 June 2023	Transfer to crypto exchange	£4,990
10	07 June 2023	Transfer to crypto exchange	£6,000
11	07 June 2023	Transfer to crypto exchange	£6,500
12	07 June 2023	Transfer to crypto exchange	£7,500
	07 June 2023	Withdrawal	£391
		Total withdrawals received	**£576**
		Total loss	**£51,416.41**

Some of the above payments were made by Mrs G towards fees for withdrawals but when she was still asked for further fees she realised she had been scammed. So, she made a

complaint to Revolut who said that it wouldn't be providing her with a refund. Unhappy with this response Mrs G brought her complaint to this service.

Our investigator said the complaint should be upheld in part. He said that Revolut should've been concerned by payment 2 here because it blocked the previous payment due to its high-risk nature. And if Revolut had stopped payment two the scam would've likely been uncovered. The investigator added that Revolut could fairly reduce Mrs G's award here by 50% because she contributed to her losses.

Mrs G agreed to the investigator's opinion.

Revolut disagreed and asked for an Ombudsman's review. It said the payments were self-to-self because Mrs G owned and controlled the beneficiary account. As a result, Revolut said the loss didn't occur from Revolut – instead it occurred on the crypto platforms. It added that it didn't consider the payments to be unusual and that other interventions from accounts Mrs G holds at other banks should be considered in line with this complaint.

What I've decided – and why

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

In deciding what's fair and reasonable, I'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 G 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 19).

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 May 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.

For example, it is my understanding that in May 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and

[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_/

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.
- 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

[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"

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 May 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 May 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mrs G 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 May 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 May 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 G 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 Mrs G'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 May 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 G'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 G might be at a heightened risk of fraud that merited its intervention.

Although payment 1 here was going to a crypto exchange, I don't think this alone was enough for Revolut to have stepped in here. It was a very small payment, and I don't think this would've seemed sufficiently suspicious for Revolut to have believed it was more than likely be part of a scam. I note Revolut declined a £4,044.42 payment on 02 May 2023 before payment 2 here because it considered it suspicious. But no question were asked of Mrs G at the time. Instead, the payment was declined. This led Mrs G to attempt another payment on the same day shortly afterwards.

So, by the time she made payment 2 here on the same day, I'm satisfied that Revolut ought to have been reasonably suspicious of the transactions. £4,111.36 was being sent to a new payee (a high-risk crypto exchange) and Revolut itself had declined an earlier payment that day because it was suspicious which was to the same exchange and for almost exactly the same amount.

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 G attempted to make the second payment here, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

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 G 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 G incurred after that point?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs G's payments, being assisted by a broker, being asked to download remote access software so they could help her open cryptocurrency wallets and starting off with a small deposit which quickly increases in value.

I've also reviewed the text conversation between Mrs G and the fraudsters (though I note that Mrs G appears to have spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations). From reading those, I can see that Mrs G was suspicious of the scammer at first and asked for her initial investment back. She asked multiple times for her initial deposit to be returned and that she wasn't comfortable with it.

I've also found nothing within those conversations that suggests Mrs G was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mrs G 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. I understand that Mrs G's difficulty in withdrawing money that made her realise she had been scammed. I've also been persuaded that Mrs G did have her doubts at the beginning of the scam which I think would've resurfaced if a crypto investment scam warning had been provided.

Revolut has mentioned that the last four payments were stopped, and Mrs G was asked why she was making them. Mrs G said that the payments were for crypto and the final three were to a safe account. Revolut then provided some generic warnings in response which wouldn't have resonated with Mrs G at the time. I think it's also worth pointing out that Revolut was aware that the last three payments were going to a crypto exchange. So, Mrs G selecting 'safe account' should've seemed suspicious to it. But I note it didn't ask any further questions or invite Mrs G to the in-app chat to ask her about that inconsistency which I think was another missed opportunity on Revolut's part here.

I've considered whether Mrs G would've likely provided similar answers if Revolut had stopped and asked further question about payment 2 here. Having done so, I don't think Mrs G would've. At the end of the scam, she was trying to send money as quickly as possible so that she could make her withdrawals and was pressured by the scammer to do it so that she could get her money back. Whereas earlier in the scam there wasn't that sense of urgency and panic about trying to withdraw her money.

Therefore, on the balance of probabilities, had Revolut provided Mrs G 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 acted more strongly on her earlier doubts about this potentially being a scam, as well as making further enquiries into cryptocurrency scams and whether or not the 'broker' was regulated in the UK. I'm satisfied that a timely warning to Mrs G 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 G's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs G 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 G's losses that I've set out here. 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.

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 G has not referred a complaint about the other account that funded this scam to me and DISP does not empower me to instruct Mrs G to make or refer a complaint to me about another business.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs G might have been at risk of financial harm from fraud when she made the second 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 G'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 G 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.

The investigator felt Revolut could fairly reduce Mrs G's award here by 50% which Mrs G agreed with. To be clear I think that would be a fair reduction here. Mrs G said she conducted her own due diligence on the merchants. But I can see that she had her doubts from the chats she had with the scammer. These messages were sent very early on in the scam, and she said that she had conducted some more research and wasn't sure if this was a scam or not. It appears Mrs G was then persuaded by the scammer telling her profits had been generated from the initial investment she made from one of her other banks. Mrs G made two payments to an individual who she was told worked in the finance department and then made very large payments towards the end of the scam (£20,000 in total) for withdrawal fees. I think these should've been red flags to her especially considering her doubts at the beginning of the conversation with the scammer.

As a result, I think Revolut can fairly reduce her award by 50%.

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

I've thought about whether Revolut did enough to attempt to recover the money Mrs G 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 G name at the genuine crypto exchanges, as Mrs G was able to move the money onto the scammers. So, Mrs G duly received the service she paid for on her debit card. The money was subsequently lost from her other account when it was moved by 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.

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

Mrs G made transfers to a crypto exchange and an individual during the scam Revolut attempted to recover the payments to the individual that were sent internally to another Revolut account. But when it tried to recover the money after the scam was raised it had already been transferred out of the Revolut account. And it wouldn't have been possible for Revolut to recover the transfers Mrs G made to the crypto exchange here as she has confirmed this money was sent to the scammers.

My final decision

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

- Refund all transactions from and including payment two minus 50%.
- 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 G to accept or reject my decision before 14 April 2025.

Mark Dobson
Ombudsman