DRN-4908098

The complaint

Mrs W complains that Revolut Ltd won't refund money she lost when she fell victim to a cryptocurrency scam.

Mrs W is being represented by solicitors in this complaint.

What happened

Mrs W says that in January 2023 she came across an advertisement for an investment trading broker "B" on a news app on her phone. She clicked on the link and was taken to B's website, where she left her contact details after having reviewed Trustpilot reviews about the company. Shortly after, Mrs W was contacted by an individual who claimed to be a representative of B. They talked her through the cryptocurrency investment opportunity and Mrs W decided to open an account with B.

Under the instructions of her 'account manager', Mrs W opened an account with a cryptocurrency exchange "G" as well as an e-money account with Revolut. She started with an initial deposit of £200 which she sent from her account held with a bank. For subsequent deposits, Mrs W first transferred funds from her bank account to her e-money account with Revolut. The money was then sent on to her wallet with G for conversion into cryptocurrency. Once converted, under the guidance of her account manager, Mrs W sent the cryptocurrency to wallets as instructed. At the time, she believed the cryptocurrency was being deposited into her investment account with B.

Seeing her investment making profits, under the guidance of her account manager, Mrs W took out several loans to fund the subsequent deposits. The use of remote access software was also involved. Mrs W was also able to make two withdrawals during this time.

When she asked to make a further withdrawal in May 2023, Mrs W was initially told the withdrawal would be processed in a few days. Subsequently, she was told she needed to wait for 14 days. At the end of that period, Mrs W was informed that she needed to pay an upfront commission to complete the withdrawal process. She made two transfers on 5 June, but these were returned because her account with G had been closed. Mrs W purchased cryptocurrency from a peer-to-peer seller the following day before sending it on.

When she was asked to make a further payment to withdraw her profits, Mrs W realised she had fallen victim to a scam and reported this to Action Fraud and Revolut.

The following transactions are relevant to this complaint –

	Date	**Type**	**Payee/details**	**Amount**
Payment 1	31 January	Transfer	Mrs W's wallet with G	£10.00
	3 February	Credit		£60.00 ***(credit)***
Payment 2	1 March	Transfer	Mrs W's wallet with G	£500.00
Payment 3	1 March	Transfer	Mrs W's wallet with G	£4,000.00
	9 March	Loan 1	Loan paid into Mrs W's bank account	£15,000.00

Payment 4	9 March	Transfer	Mrs W's wallet with G	£15,000.00
	10 March	Loan 2	Loan paid into Mrs W's bank account	£11,500.00
Payment 5	10 March	Transfer	Mrs W's wallet with G	£11,500.00
	14 March	Loan 3	Loan paid into Mrs W's bank account	£12,000.00
Payment 6	14 March	Transfer	Mrs W's wallet with G	£12,000.00
	15 March	Loan 4	Loan paid into Mrs W's bank account	£12,000.00
Payment 7	15 March	Transfer	Mrs W's wallet with G	£10.00
Payment 8	15 March	Transfer	Mrs W's wallet with G	£11,990.00
	4 April	Credit		£1,997.15 ***(credit)***
	5 June	Loan 5	Loan paid into Mrs W's business account	£23,000.00
Payment 9	5 June	Transfer	Mrs W's wallet with G	£10,500 ***(payment returned)***
Payment 10	5 June	Transfer	Mrs W's wallet with G	£11,500 ***(payment returned)***
Payment 11	6 June	Transfer	Unknown third party (peer-to-peer purchase of cryptocurrency)	£22,000
			Total loss	**£74,952.85**

Revolut declined to refund any of the disputed payments, saying that Mrs W had authorised them and a new beneficiary warning was provided at appropriate times.

Unhappy with this, Mrs W referred her complaint to our service through her representative. Our investigator thought the first two payments weren't unusual, but Revolut ought to have provided a warning specific to cryptocurrency scams when Mrs W authorised Payment 3. Had it done so, the investigator was persuaded that the scam would have been uncovered and further losses prevented. They asked Revolut to refund Mrs W's losses from that payment onwards along with interest, but with a 50% deduction for contributory negligence.

Mrs W accepted the investigator's outcome, but Revolut didn't. In summary, it says:

- The transfers weren't considered unusual as they matched the account opening purpose provided.

- Payment 3 went to a beneficiary that Mrs W had already transferred funds to before and had received a credit from. Also, the beneficiary account was in her name and in her control, so these were self-to-self payments.

- As Mrs W lied about the loan purpose, most probably she would have given wrong answers if it had asked about the real purpose of the payment.

- Mrs W had an email exchange with G when it was concerned about her increased crypto activity. As she didn't consider its concerns as a red flag and found other means of making payments towards the scam, Revolut doesn't consider a warning would have made a difference to Mrs W. It says it's more likely that Mrs W would have hidden the real purpose of the payment as she did when she applied for the loans, since she was following the scammer's advice.

As an agreement couldn't be reached, the complaint has been passed to me to decide.

What I've decided – and why

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

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

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 W modified the starting position described in *Philipp,* by expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with Mrs W 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, 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.

[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).

And, I'm 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 January 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

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

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

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

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

- 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.

---

[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.

- The October 2017, BSI Code[4], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in January 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.

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

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

I'm aware that cryptocurrency exchanges like G generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely

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

have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Mrs W's name.

By January 2023, when these transactions started, 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[5]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. 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 W made from January 2023 onwards, 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.

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 W'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 W might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that Payments 1-10 were going to a cryptocurrency provider. The first two payments were very low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam. However, Payment 3 was significantly larger than any other payment that had debited Mrs W's account since it was opened a few months prior, and it was made on the same day as the previous payment. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mrs W was at heightened risk of

[5] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Mrs W?

Revolut says it provided a number of warnings to Mrs W when she set up new beneficiaries prior to making the "transfers". It says it warned Mrs W that she might be falling victim to a scam by providing the following message:

"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"

While I don't discount this warning entirely, it is very general in nature and it's difficult to see how it would resonate with Mrs W or the specific circumstances of the transactions in question. I don't think that providing the warning above in relation to earlier payments was a proportionate or sufficiently specific mechanism to deal with the risk that Payment 3 presented. I think Revolut needed to do more.

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 W attempted to make Payment 3, 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 W 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 warning of the type described, would that have prevented the losses Mrs W suffered from Payment 3 onwards?

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 W's payments, such as finding the investment through an advertisement, being assisted by a broker and being asked to download remote access software so they could help her.

I've also reviewed the text conversation between Mrs W and the fraudsters (though I note that Mrs W appears to have also spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations). I've found nothing within those conversations that suggests Mrs W was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mrs W expressed mistrust of Revolut or financial firms in general.

Revolut submits that Mrs W lied about the purpose of the loans that she took out to fund the scam payments. It argues that she would most probably have lied about the payment purpose had it made enquiries. But my finding here isn't that it should have made further enquiries with Mrs W. As I've set out above, given the nature of the transaction, I consider that it should have provided a warning that should have addressed the risks of cryptocurrency investment scams. Revolut's point about Mrs W not revealing the true purpose of the loans is less relevant in that instance. Had she been presented with a clear warning that matched her circumstances, there's nothing to suggest that Mrs W would have continued with the payment in question.

I can see that the investigator, and later Revolut, has mentioned that Mrs W continued finding a way to make scam-related payments in June when G closed her account. The investigator considered Mrs W's actions were grounds for contributory negligence, whereas Revolut submits that they show a warning wouldn't have stopped her from going ahead with the payment. The problem with Revolut's argument is that it is essentially suggesting an intervention on 1 March is unlikely to have worked because of actions Mrs W took over three months later, on 5-6 June. Payments 9-11 were made in relation to withdrawing from the investment. The chat correspondence with the scammer shows that by that point, Mrs W was desperate to get her funds out as she needed money to look after an ill family member. By contrast, the payments made on 1 March were deposits made in the early stages. I should also mention that G hadn't contacted Mrs W about its review by that point.

I've taken into account that Mrs W had received a single actual return at the point of the suggested intervention, but it was modest. The weight of evidence that I've outlined persuades me that Mrs W was not so taken in by the fraudsters that she wouldn't have paid attention to a scam warning by Revolut on 1 March, or that she would have misled it.

Therefore, on the balance of probabilities, had Revolut provided Mrs W 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, for instance, paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Mrs W from Revolut would very likely have caused her to decide not to go ahead with Payment 3.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mrs W purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I've carefully considered Revolut's view that it shouldn't be held responsible for losses that occurred on a third-party site. But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs W might have been at risk of financial harm from fraud when she made Payment 3, and in those circumstances, it should have taken additional steps before processing it. If it had taken those steps, I'm satisfied that it would have limited the losses that Mrs W suffered. The fact that the money wasn't lost at the point it was transferred to G does not alter that fact and I think Revolut can fairly be held responsible for Mrs W's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against the firm that the point of loss.

I've also considered that Mrs W has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mrs W could instead, or in addition, have sought to complain against those firms. But Mrs W has not chosen to do that and ultimately, I can't compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs W's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I've set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mrs W's loss from Payment 3 (subject to a deduction for Mrs W's own contribution which I will consider below).

Should Mrs W bear any responsibility for her losses?

Mrs W has accepted that she should share equal responsibility for her losses, as per our investigator's outcome. For completeness, I'll address why I'm in agreement that liability should be shared equally between the parties.

There's a general principle in law that consumers must take responsibility for their decisions. I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking platform. I also understand that Mrs W checked B's reviews which were largely positive. So, I can imagine that this would have given some validation to the investment opportunity it offered.

But, Mrs W doesn't appear to have had any concerns when the scammer kept encouraging her to take out multiple loans to fund her investment – in total, she took out five loans. Or when misleading the lenders about the purpose for borrowing money was suggested. Moreover, having reviewed the chat correspondence between her and the scammer, during the later stages of the scam – when excuses were being made about why she couldn't withdraw her funds – Mrs W had concerns about what she had been told about the investment at the outset. Yet she didn't carry out any independent due diligence before parting with even more money.

Having thought carefully about this, I'm in agreement with the investigator that Mrs W ought to bear some responsibility for her losses and that compensation should be reduced accordingly. Weighing up everything, I consider that it would be fair to reduce compensation payable by 50%. As I've mentioned, Mrs W accepts this.

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

Except for the final payment, Mrs W sent money to a cryptocurrency provider before transferring it to the fraudster (albeit she didn't know that at the time). So, Revolut wouldn't have been able to recover the funds from the cryptocurrency provider.

The final payment appears to have been made to an individual selling cryptocurrency, who was very likely unconnected to the fraudsters. As the individual was unlikely to be involved in the fraud, even if it were practical or possible to recover funds from them, it would be unlikely to be fair for that to happen (given that they'd legitimately sold cryptocurrency). So, I don't think it would be fair and reasonable to conclude that Revolut should have done anything more to try and recover Mrs W's money.

Putting things right

Revolut Ltd needs to refund Payments 3-8 as well as 11 (9 and 10 were returned), making a 50% deduction for contributory negligence. From that refund, it can also deduct any credits Mrs W received.

Revolut Ltd also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of refund.

My final decision

For the reasons given, my final decision is that I uphold this complaint. I require Revolut Ltd to put things right for Mrs W as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs W to accept or reject my decision before 8 October 2024.

Gagandeep Singh
Ombudsman