

The complaint

Mr B complains that Revolut Limited ('Revolut') won't refund the money he lost when he fell victim to a scam.

What happened

Mr B says he saw an advertisement online that referred to making money through cryptocurrency investment through a company I'll call W in this decision. Mr B believed that his investment would be in stocks, shares, and commodities and that he would receive a return of 10% plus a month. He didn't know at the time, but W wasn't a genuine investment company.

I have set out in the table below the payments Mr B made on the instructions of the scammer. All payments were card payments to cryptocurrency exchanges where Mr B bought cryptocurrency which he sent to wallet address details a representative of W gave him. The entry in italics is a return that credited Mr B's Revolut account.

Transaction	Date	Amount	Recipient
1	23/01/23	£4,050	Crypto 1
2	23/01/23	£2,000	Crypto 1
3	30/01/23	£1,000	Crypto 1
4	31/01/23	£5,000	Crypto 1
5	01/02/23	£3	Crypto 2
	<i>02/02/23</i>	<i>£284.70</i>	<i>Crypto 2</i>
6	03/02/23	£10,000	Crypto 1
7	10/02/23	£5,000	Crypto 1
8	11/03/23	£5,000	Crypto 1
Total		£31,768.30	

Mr B had regular calls with a representative of W and had access to an online portal where he could see how his investments were performing and his deposits.

Mr B says he realised he was the victim of a scam when his contact at W stopped responding to him. His professional representative contacted Revolut in November 2023.

Revolut didn't agree to reimburse Mr B. It said that chargeback was the appropriate way to challenge card payments, but Mr B hadn't raised any claims.

Mr B was unhappy with Revolut's response and brought a complaint to this service. He said Revolut should have intervened when he made out of character payments.

When the complaint came to this service Revolut added:

- All payments were initiated and authorised by Mr B.

- Revolut was only used as an intermediary between Mr B's bank and cryptocurrency accounts. These cryptocurrency accounts carry out identity checks and only allow customers to deposit funds from external cards or accounts in their own name.
- Mr B had made cryptocurrency related payments in 2022 and received returns, and no evidence of a scam had been provided to it.
- This service is permitted to depart from the law but where we do should explain that we have done so and explain why. If we apply the law or legal duties, we should apply it correctly and if we err in law, we are susceptible to judicial review on the grounds of error in law in relation to our identification of what the law is (as well as perversity and irrationality).
- Revolut is bound by contract, applicable regulations and common law to execute valid payment instructions. The duty is strict and there are only limited exceptions. Revolut referred to specific terms in its terms and conditions and went on to say that although the relationship between a payment service provider (like Revolut) and a customer is one of contract, such contracts are performed in a heavily regulated legal environment. The most significant legislation is the Payment Services Regulations 2017 which impose obligations to execute authorised payments promptly. By suggesting that it needs to reimburse customers, it says our service is erring in law.
- This service has overstated Revolut's obligations. Revolut recognises its obligations and has put adequate procedures in place. But the duty is not absolute and doesn't require Revolut to detect and prevent all fraud.
- It does not need to concern itself with the wisdom or potential for financial loss of a customer's payment instructions. This was confirmed in the recent Supreme Court judgement in the case of *Philipp v Barclays Bank UK plc [2023] UKSC 25*.
- It appears reimbursement has been awarded on the basis of The Payment Service Regulator's ("PSR") mandatory reimbursement scheme or the Contingent Reimbursement Model Code (CRM Code). But the PSR rules weren't in force at the time and Revolut isn't a signatory to the CRM Code.

Our investigation so far

The investigator who considered this complaint recommended that it be upheld in part. She said Revolut ought to have had concerns about payment one in the table above and provided Mr B with a written warning tailored to cryptocurrency investment scams. Such a warning would have resonated with Mr B, and he wouldn't have gone ahead with the payments. But the investigator felt that Mr B should share responsibility for his loss. This meant Mr B should receive 50% of all payments less any credits received, plus interest.

Revolut didn't agree with the investigator's findings, so Mr B's complaint has been passed to me to decide. Revolut referred to its earlier submissions (set out above) and made the following points:

- This case involves 'Self-to-Self' transactions to accounts owned and controlled by Mr B, so the fraudulent activity didn't occur on Mr B's Revolut account.
- Funds were transferred from an existing bank account to Revolut, so this service should consider possible interventions by other banks.
- It is irrational and illogical to hold Revolut liable when it is merely an intermediate link and there are other regulated financial institutions that hold more data on the customer, but which haven't been held responsible in the same way.

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 Mr B 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 January 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 January 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

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/

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.

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 Code³, 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 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 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

³ BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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

Revolut has suggested Mr B might not have been the victim of a scam. He has provided evidence of the scam to this service, including screenshots from the fake investment platform and communications with the scammer. I also note that the FCA issued a warning about W in May 2021.

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

It isn't in dispute that Mr B has fallen victim to a cruel scam here, nor that he authorised the payments he made to his cryptocurrency wallets (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in this decision the circumstances which led Mr B to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr B might be the victim of a scam.

I'm aware that cryptocurrency exchanges 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 have been aware of this fact too. So, it could have reasonably assumed that all payments would be credited to a cryptocurrency wallet held in Mr B's name.

By January 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 January 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 Mr B made in January 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, 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 January 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.

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 Mr B might be at a heightened risk of fraud.

Mr B opened his Revolut account in 2019. In the 12 month period before the first scam payment Mr B had used his account for low value transactions of up to £500. So, when Mr B made the first payment, I consider Revolut ought to have recognised that it carried a heightened risk and taken additional steps before processing it. It was a higher value transaction that was identifiably going to a cryptocurrency provider. While I agree with Revolut that Mr B bought cryptocurrency in 2022, he only made three transactions of between £15 and £200. There was a marked change in spending patterns when Mr B made payment one.

What did Revolut do to warn Mr B?

When Mr B set up each new payee Revolut provided a warning that said,

"Do you know and trust this payee?"

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

This warning is very general in nature and it's difficult to see how it would resonate with Mr B when he was making a payment to a well known cryptocurrency exchange. I don't think this

was a proportionate or sufficiently specific response to the risk that payment one presented so 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.

I think that when Mr B made payment one Revolut should have recognised the increased risk of fraud associated with that payment and I think that a proportionate response to that risk would have been for Revolut to have provided a written warning to Mr B. Knowing that the payment was going to a cryptocurrency provider, Revolut ought to have provided a warning that was specifically about the risk of cryptocurrency scams, given how prevalent they were by January 2023. 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.

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 it ought to have provided should have highlighted, in understandable terms, the key features of that kind of scam, for example: an advertisement on social media, that might be 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.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr B suffered from payment one?

On balance I consider a written warning of the type I have described above would have resonated with Mr B and meant he didn't make the payment.

When Mr B made payment one, he hadn't built up a trusting relationship with the representative of W or received any returns that might have led him to believe the investment was legitimate. But he had responded to an advertisement, had an account manager or trader who was acting on his behalf and kept in regular contact, and been advised of significant returns. I can also see from the platform screenshots Mr B has provided that a representative of W had remote access and was controlling his screen.

Mr B also couldn't afford to lose this money, and I think it's more likely than not that any suggestion he might be the victim of a scam would have prevented him from getting involved with W. Mr B has explained that he was in a difficult financial position and decided to invest to try to improve the position. Overall, I'm not satisfied that I can fairly say Mr B would've ignored the warning and made the payment regardless.

It's worth noting that the bank where Mr B held his account that funded the Revolut payments, didn't intervene on any of the payments he made as they didn't identify a potential fraud risk.

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

In reaching my decision about what is fair and reasonable, I have taken into account that funds went from Mr B's Revolut account to legitimate providers of cryptocurrency which Mr B then passed on to the scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr B might have been at risk of financial harm from fraud when he made payment one, 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 Mr B suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr B's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr B'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 either the firm that is the origin of the funds or the point of loss.

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

I'm also not persuaded it would be fair to reduce Mr B'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 have set out above, I am satisfied that it would be fair to hold Revolut responsible for consumer's loss from the first payment in the table above (subject to a deduction for consumer's own contribution which I will consider below).

I'm also aware that the Payment Service Regulator's ("PSR") proposed mandatory reimbursement scheme doesn't require Revolut to reimburse Mr B. This scheme doesn't apply to in this case and neither does the Contingent Reimbursement Model Code so are not relevant to my consideration of it.

Should Mr B bear any responsibility for his 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 recognise that there were persuasive elements to this scam including a platform but, overall, I consider a 50% deduction to reflect Mr B's actions is fair. Mr B has no contract or formal documentation to set out his agreement with W and was offered a rate of return that was too good to be true. Even his representative said the promised returns were 'unrealistic'.

Mr B says he looked at reviews of W. I can see multiple negative reviews that were posted before Mr W made his first investment which say it was operating a scam. And if I search W online the Financial Conduct Authority's warning about W comes up. This was published in May 2021.

Mr B was investing a significant amount of money and appears to have relied on information provided to him by W. I think he ought reasonably have done more to check the opportunity was legitimate.

Overall

I'm very sorry Mr B has lost such a significant amount of money and to hear about the impact this has had on him. Overall, I think a fair resolution would be for Revolut to refund 50% of payment one and all subsequent transactions, plus interest as set out below.

My final decision

For the reasons stated, I uphold this complaint and require Revolut Ltd to:

- Reimburse 50% of all transactions from (and including) payment one in the table above (less the credit Mr B received of £284.70); and
- Pay interest on the above amount at the rate of 8% simple per year (less tax if properly deductible) from the date of each transaction to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 9 January 2025.

Jay Hadfield
Ombudsman