DRN-5109218

The complaint

Mr B complains that Revolut Ltd ('Revolut') won't reimburse the funds he lost when he fell victim to a scam.

What happened

Mr B says he found an investment company I'll refer to as G online. G offered an opportunity that involved making money through cryptocurrency. Mr B didn't know at the time, but G wasn't a genuine investment company.

Mr B had an account manager who called him regularly and sent messages and emails. A screen sharing application was used and Mr B says he was shown impressive growth charts which duped him into believing his investment was doing well.

I have set out in the table below the transactions Mr B made on the advice of the scammer(s). All transactions were to a known cryptocurrency exchange ('C').

Transaction	Date	Amount
1	21/02/23	£10
2	21/02/23	£3,500
3	07/04/23	£14,000
Total		**£17,510**

Mr B says he realised he was the victim of a scam when he was asked to pay money to release his funds and he contacted the police. He reported what had happened to Revolut.

Revolut said it wasn't at fault and had provided Mr B with sufficient warnings. It had also done what it could to recover his funds. Revolut was able to recover £10 from Mr B's cryptocurrency wallet.

Mr B was unhappy with Revolut's response and brought a complaint to this service.

When the complaint came to this service Revolut added:

- All payments were initiated and authorised by Mr B.
- It had sufficient scam controls in place. Revolut intercepted payment two and provided warnings that were relevant to Mr B's circumstances. It would be unreasonable to expect Revolut to intervene again when payment three was made to the same merchant and Mr B had acknowledged the scam warnings.
- 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.
- Neither the CRM Code nor the PSR mandatory reimbursement rules impose a duty on Revolut to reimburse customers for self-to-self transactions.

- It is illogical to hold Revolut responsible for a customer's losses when it is merely an intermediate link and other banks have greater knowledge.
- Mr B acted with gross negligence in not completing any research and not recognizing typical hallmarks of a scam, like remote access and initial high profits followed by a request to pay a fee to withdraw funds.

Our investigation so far

The investigator recommended that Revolut reimburse 50% of payments two and three. He thought that the on-screen cryptocurrency warning didn't go far enough to highlight the essential features of a cryptocurrency investment scam. But Mr B should share responsibility for his loss because he didn't do enough to ensure the investment opportunity with G was legitimate.

Mr B accepted the investigator's findings, but Revolut did not. It raised 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.
- Many people use Revolut accounts to buy cryptocurrency, particularly since high street banks have restricted their customers from sending funds to cryptocurrency exchanges.
- 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 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 Mr B and the Payment Services Regulations to carry out his 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.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in February and April 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 am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system 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 am also mindful that:

---

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

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

- 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.
- 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 February/April 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

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

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 Mr B was at risk of financial harm from fraud?

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, 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 February and April 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 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 early 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 Mr B'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 Mr B might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all three payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). But transaction one is of such a low value I don't consider Revolut ought to have suspected it might be part of a scam.

Payment two was out of character with Mr B's normal use of his Revolut account (which he opened in 2019). It was much higher in value than the usual transactions on the account and, as I have said above, was identifiably to a provider of cryptocurrency. There were no cryptocurrency related transactions on Mr B's account until 14 February 2023 when Mr B made low value transactions (£15, £64 and £10) to two cryptocurrency exchanges that weren't C. Then on 17 February 2023, the day Mr B made his first payment to C, he received £10 from one of the other providers and £121.10 from C.

So I consider Revolut ought reasonably to have recognised a risk and taken additional steps, as it did in this case.

What did Revolut do to warn Mr B?

Revolut say that when transaction one was made Mr B received a new payee 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.

Revolut says it recognised a scam risk when payment two was made and put the payment on hold. It provided educational stories which warned that victims lose millions of pounds a year to bank transfer scams and that fraudsters are professionals. Revolut then asked Mr B to provide the purpose of the payment. Mr B chose the 'Crypto Currency' option and was provided with screens that said:

"*Moving funds to your own account?*
Please ensure no-one besides you has access to that account

Asked to download software?
If someone has asked you to download any software (like AnyDesk), this could be a scam!

Are you making a new investment?
Research if what you're investing in is a legit company or cryptocurrency".

So Revolut recognised a scam risk and took some steps to warn Mr B. But I'm not satisfied that the warning it provided gave Mr B enough information to identify that he may be at risk or gave sufficient information on what to do to avoid falling victim to a cryptocurrency investment scam. And it doesn't bring to life cryptocurrency investment scams. I will discuss this in more detail in the section below.

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.

When Mr B attempted to make payment two, I think Revolut ought fairly and reasonably to have recognised there was a heightened possibility that the transaction was linked to a scam. In line with the good industry practice that I've set out above, I think a proportionate response to that risk would have been for Revolut to have provided a written warning tailored to cryptocurrency investment scams which were the most prevalent cryptocurrency scams at the time.

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; too good to be true returns that are presented as carrying little or no risk; and a small initial deposit which quickly increases in value.

Revolut identified a scam risk but the warning it provided didn't cover many of the common features of cryptocurrency investment scams. There was no mention of an account manager, high rates of return that may be guaranteed, or difficulties when trying to withdraw funds. Whilst Revolut's warning refers to screen sharing applications such as the one Mr B says the scammer used, the warning only says if Mr B has been asked to use such software it 'may' be a scam. I don't consider this warning goes far enough, as a legitimate investment company would not require the use of a screen sharing app. And whilst Revolut mentioned research it didn't provide any information on the kind of research that could be completed or how to spot a scam. Overall, I don't think Revolut's warning went far enough.

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

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.

Mr B had an account manager or trader who was acting on his behalf and kept in regular contact, had made a small deposit that quickly increased in size and had been advised of significant returns. The scammer had also advised him to download remote access software. So I think a better warning would have resonated with him and led him to pause and complete some checks. Mr B was a first-time cryptocurrency investor so I see no reason why he wouldn't have heeded advice from Revolut, as the expert here.

I think it's more likely than not that any suggestion Mr B might be the victim of a scam would have prevented him from continuing his relationship with G. 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 given the activity on this account.

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 Revolut wasn't the original source of the funds for the money Mr B lost to the scam. Mr B had moved the money from another bank to his Revolut account, before sending the funds onto a cryptocurrency wallet.

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 two, and in those circumstances its intervention should have been better. If it had been, 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 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 Mr B 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. As I have noted above, Mr B's bank didn't intervene when he transferred funds to Revolut but there were high value transactions from the account.

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 Mr B's loss from payment two (subject to a deduction for Mr B's own contribution which I will consider below).

I'm also aware that the Payment Service Regulator's ("PSR") mandatory reimbursement scheme doesn't require Revolut to reimburse Mr B. This scheme doesn't apply 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 loss?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that there were persuasive elements to this scam and that fraudsters used the apparent success of early trades and the apparent ability to withdraw funds to encourage larger deposits. But, overall, I think it would be fair and reasonable to hold Mr B partly responsible for his loss.

My intention is not to further Mr B's distress when he has already been the victim of a cruel scam. But, I am satisfied that Mr B should've had serious concerns about what he was being told by representatives of G from the outset and that he should've questioned the legitimacy of the supposed investment.

Mr B says he was persuaded by G's website and the scammer's communications with him. But Mr B didn't complete any independent research into G to verify what he was told. If he had done so, Mr B wouldn't have found any information about G, which ought reasonably to have concerned him. The poor reviews and FCA warning the investigator referred to came after Mr B sent funds to G.

At the time the payments were made Mr B hadn't been provided with any documentation, such as terms of business or contracts, that you'd reasonably expect to see when dealing with a legitimate company. The messages Mr B has provided show that on 5 April, before he made the more significant payment of £14,000, Mr B asked his account manager to email him a plan and statement of how the investment had done so far as he likes emails. This didn't happen, and Mr B proceeded to make a significant payment at G's request. And Mr B was only able to see profits when the scammer showed him them on the platform that he now knows to be fake.

Overall, I've concluded that Revolut can fairly reduce the amount it pays to Mr B because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

My final decision

I uphold this complaint and require Revolut Ltd to:

- Pay Mr B £8,750; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of each transaction to the date of settlement.

If Revolut Ltd is legally required to deduct tax from the interest it should send Mr B a tax deduction certificate so he can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 22 April 2025.

Jay Hadfield
Ombudsman