

## **The complaint**

Mr D complains that Revolut Ltd (Revolut) is refusing to refund him the amount he lost as the result of a scam.

Mr D is being represented by a third party. To keep things simple, I will refer to Mr D throughout my decision.

## **What happened**

Mr D has told us that in early September 2022 he came across an advertisement on social media showing details of an individual making a substantial amount of money investing in cryptocurrency. The advertisement was associated with a company that claimed to be an expert in cryptocurrency trading. I will call the company "X".

X also appeared to be endorsed by a well-known celebrity. Mr D says he searched X online and was able to find a positive article about it. Having carried out some research Mr D decided to click on the link provided.

Mr D tells us the website he was directed to looked legitimate with aspects he had come to expect from a website associated with a genuine company. Mr D completed an online data capture form with his personal details and received a call from X shortly after.

During the initial call with X Mr D was told that if he chose to proceed with the investment, he would be allocated an account manager who would make informed trades on his behalf using an expert AI algorithm. Mr D agreed to invest and was assigned an account manager as promised.

Mr D was required to download remote access software so X could help him with the process of trading and so he could learn how to access the markets. He was also required to setup a cryptocurrency account and was provided access to X's trading platform.

Mr D started to make payments into the investment and as he was happy with the returns he appeared to be making, agreed to make further and further payments. Mr D's account manager with X changed several times throughout the investment process but each time the account managers encouraged Mr D to make further payments.

Mr D has told us that around 21 October 2022 he was allocated a VIP account manager as his account balance had increased. Mr D was advised that he would need to make larger deposits and that they would create a higher return. As Mr D's investment appeared to be doing well, he agreed and started making larger payments.

After making a £15,000 payment on 11 November 2022 Mr D was again asked to make further payments but was unable to as he had depleted his available funds. X explained that to make a withdrawal from the investment Mr D would have to make further payments first.

In an effort to withdraw from the investment Mr D made two further payments on 18 November 2022 funded by a loan he had taken (which was paid back within the cooling off

period).

After making the final payments Mr D did not receive the withdrawal he had requested and was no longer able to contact X. At this point Mr D realised he had fallen victim to a scam. Mr D made the following payments in relation to the scam from his Revolut account and also received some small refunds.

Payment	Date	Payee	Payment Method	Amount
	13 September 2022	Binance UAB	Credit	£136.44cr
1	14 September 2022	Binance UAB	Debit card	£4,172.00
2	14 September 2022	Binance UAB	Debit card	£15.00
3	16 September 2022	Binance UAB	Debit card	£8,279.00
	20 September 2022	Binance UAB	Credit	£105.72cr
	20 September 2022	Binance UAB	Credit	£21.08cr
	22 September 2022	Binance UAB	Credit	£31.52cr
	20 October 2022	Binance UAB	Credit	£414.80cr
	20 October 2022	Binance UAB	Credit	£29.66cr
	21 October 2022	Binance UAB	Credit	£476.27cr
4	29 October 2022	Binance UAB	Debit card	£5,000.00
5	2 November 2022	Binance UAB	Debit card	£10,000.00
6	2 November 2022	Binance UAB	Debit card	£10,000.00
7	6 November 2022	Binance UAB	Debit card	£5,000.00
8	11 November 2022	Binance UAB	Debit card	£15,000.00
9	18 November 2022	Binance UAB	Debit card	£15,000.00
10	18 November 2022	Binance UAB	Debit card	£3,000.00

Our Investigator considered Mr D's complaint and didn't think it should be upheld. Mr D disagreed, so this complaint was passed to me to decide.

in my provisional decision sent on 3 January 2025 I said:

*"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 D 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.*

*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 September 2022 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;<sup>1</sup>*
- *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*

*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)<sup>2</sup>.*

---

<sup>1</sup> 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\\_further\\_reduction\\_in\\_card\\_fraud\\_and\\_had\\_offers\\_from\\_banks/](https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_further_reduction_in_card_fraud_and_had_offers_from_banks/)

<sup>2</sup> 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-

- 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 customers’ accounts and scrutinise transactions.
- The October 2017 BSI Code<sup>3</sup>, 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.

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 September to November 2022 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,

---

date the Consumer Duty and so it does not apply.

<sup>3</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

- 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 September to November 2022, Revolut should in any event have taken these steps.*

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

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

*Whilst I have set out in detail in this decision the circumstances which led Mr D 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 D might be the victim of a scam.*

*Firstly, I don't think that Revolut would have had any reason to intervene when Mr D made payments 1 and 2. Although these payments were being made to a known cryptocurrency exchange, they were not of a significant value that I would have expected to have triggered Revolut's fraud prevention systems prompting it to intervene.*

*Payment 3 was of a more significant value. It was the second large payment Mr D had made to a cryptocurrency exchange in just two days and was almost twice the value of the previous large payment which was starting to show a pattern of increased value payments.*

*Even though Mr D had given the account opening purpose as "crypto" when the account was opened, I think payment 3 should have alerted Revolut that Mr D could have been at risk of financial harm from fraud.*

*What did Revolut do to warn Mr D?*

*Revolut has explained that each time Mr D made a payment he was required to confirm it was him making the payment via 3DS secure on his device.*

*While I don't discount this entirely, as it would have confirmed it was Mr D authorising the payments, and not a third party without Mr D's permission, it is difficult to see how it would resonate with Mr D or the specific circumstances of the payments in question.*

*I don't think that providing this specific mechanism was able to deal with the risk that the payment presented. I think Revolut should have done 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 the ones Mr D made in relation to the scam will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly.*

*Taking that into account I think Revolut should have had concerns when Mr D made payment 3. Considering the value of the payment and the risk associated with it at the time I think a proportionate intervention would have been for Revolut to have asked about the purpose of the payment (for example by asking Mr D to select a payment reason from a list of possible reasons) and provided a warning which covered the key scam features of the payment purpose selected.*

*If Revolut had provided a tailored warning when payment 3 was attempted, would the scam have come to light and Mr D's loss been prevented?*

*Mr D was making payments via a cryptocurrency exchange to an investment company he had found on social media, that appeared to have been endorsed by a well-known celebrity. Mr D has also told us he was required to download remote access software so that X could help him with the investment process.*

*I note that Mr D has been able to provide very little of his interactions with the fraudsters. Ultimately, as Revolut didn't provide an intervention like that I've described above, it can provide no compelling evidence that such a warning would not have resonated with Mr D and that he would have continued to make the payment.*

*The details of the scam explained above were common with cryptocurrency scams at the time and had Revolut intervened as I've explained it should have, I'm satisfied Mr D would have taken notice of the warning provided, that would have been tailored to the type of scam he was experiencing and stopped making the payments.*

*Mr D did make payments from other accounts he held elsewhere into his Revolut account before they were forwarded to the scam. One of the other account providers did intervene, and a warning message was shown before a payment was processed, however the warning did not specifically cover the risks associated with the scam Mr D was experiencing.*

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

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

*But as I've set out in some detail above, I think that Revolut still should have recognised that Mr D might have been at risk of financial harm from fraud when he made payment 3 and provided an appropriate intervention. If it had taken those steps, I am satisfied it would have prevented the losses Mr D suffered from payment 3 onwards. 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 D's own account does not alter that fact and I think Revolut can fairly be held responsible for*

*Mr D'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 D has only complained against Revolut. It appears there is little evidence of any other party providing a proportionate intervention, and 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 D could instead, or in addition, have sought to complain against those firms. But Mr D has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.*

*I'm also not persuaded it would be fair to reduce Mr D's compensation in circumstances where Mr D has only complained about one respondent from which he is entitled to recover his 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 D's loss from payment 3.*

*Should Mr D 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 I consider to be fair and reasonable in the circumstances of this complaint.*

*There were relatively sophisticated aspects to this scam. Mr D found a professional looking advertisement for a cryptocurrency investment company on social media endorsed by a well-known celebrity. Upon clicking on the link Mr D was provided with what he considered to be a legitimate website that didn't cause him any concerns.*

*Upon signing up to have an account with X Mr D was given access to a trading account and was able to withdraw some funds throughout the investment process. Mr D was also assigned several different account managers which I think would have added to Mr D's belief that he was dealing with a large company.*

*As I've already set out, I can't put significant weight on Revolut requiring Mr D to authorise the payments using 3DS secure as this did not provide the appropriate intervention that I think it should have.*

*However, Mr D has explained that he was asked to make payments to withdraw from the investment and was encouraged to take a loan to cover the required payments. I think this should have been a red flag to Mr D and if he had taken more care, he may also have been able to prevent the scam. So I think it would be fair for Mr D to share responsibility for his loss.*

*Recovering the payments Mr D made*

*I have also thought about whether Revolut was able to recover the payments Mr D made. But Mr D made payments into the scam via his debit card. When payments are made by card the only recovery option available to Revolut is to request a chargeback.*

*The chargeback scheme is a voluntary scheme set up to resolve card payment disputes between merchants and cardholders. The card scheme operator ultimately helps settle disputes that can't be resolved between the merchant and the cardholder.*

*Such arbitration is subject to the rules of the scheme, meaning there are only limited grounds and limited forms of evidence that will be accepted for a chargeback to be*

*considered valid, and potentially succeed. Time limits also apply.*

*Mr D was dealing with X, which was the business that instigated the scam. But Mr D didn't make the debit card payments to X directly, he paid a separate cryptocurrency exchange. This is important because Revolut would only have been able to process chargeback claims against the merchant he paid, not another party (such as X).*

*The service provided by the cryptocurrency exchange would have been to convert or facilitate conversion of Mr D's payments into cryptocurrency. Therefore, it provided the service that was requested; that being the purchase of the cryptocurrency.*

*The fact that the cryptocurrency was later transferred elsewhere – to the scammer – doesn't give rise to a valid chargeback claim against the merchant Mr D paid."*

I gave Mr D and Revolut time to respond to my provisional decision.

### **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.

Neither Mr D nor Revolut provided anything further for me to consider so I see no reason to reach a different outcome to that explained in my provisional decision.

### **Putting things right**

To put things right I require Revolut Ltd to:

- Refund 50% of the payments Mr D made into the scam from payment 3 onwards (less the credits received).
- Revolut Ltd should add 8% simple interest per year to the amount it pays Mr D from the date of loss to the date the payment is made (less any lawfully deductible tax).

### **My final decision**

I uphold this complaint and require Revolut Ltd to put things right by doing what I've outline above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 14 February 2025.

Terry Woodham  
**Ombudsman**