DRN-4997567

The complaint

Mr L says Revolut Ltd didn't do enough to protect him when he fell victim to a cryptocurrency investment scam.

What happened

Mr L saw an advert online for a cryptocurrency investment firm. He sent funds between March and April 2023 to an account he created with a genuine cryptocurrency provider and then lost the funds from here to the scammer. Mr L funded this investment with his own money initially, but then borrowed funds too. He borrowed money from his father; his business; had an invoice paid directly to his Revolut account rather than his business; and borrowed funds from a friend.

Mr L says Revolut ought to have warned him about these scams when he was making the payments and if it had, it would've prevented his loss. Revolut didn't uphold his complaint and said Mr L's payments couldn't be recovered by a chargeback claim.

Mr L brought his case to our service and our Investigator partially upheld it. Revolut disagreed with their view, so the case has been passed to me for a 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.

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 L 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 March 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.

[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_/

For example, it is my understanding that in March 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 have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.
- The October 2017, BSI Code[3], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

---

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

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

- 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 March 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in March 2023, Revolut should in any event have taken these steps.

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

When the transactions for this scam 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 in prevalence. 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. These restrictions – and the reasons for them – would have been well known across the industry.

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 L made in March 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. I have therefore considered whether, due to this, Revolut ought to have been concerned Mr L was at risk of financial harm when he was making the payments to this scam.

I don't consider Revolut ought to have had concerns about the first payment Mr L made, as I have to look at a number of factors in addition to the payment destination, including the value of the payment and the purpose of the account to assess whether it posed a risk of financial harm. This was a lower value payment and in line with the account purpose. But by the time Mr L made the second payment on 23 March 2023, he was then attempting to send £3,000 to a merchant Revolut should've been able to identify as a cryptocurrency provider. This was a higher value payment and the second amount in a few days. So I do think it should've recognised a risk of financial harm at this time.

What did Revolut do to warn Mr L? And what kind of warning should Revolut have provided?

Revolut didn't provide Mr L with any warnings on the first or second payments he made towards this scam. It did display a warning on a payment attempted on 17 April 2023, but this was after I think Revolut ought to have intervened. And this warning said the payment had been declined due to its potential high risk nature, but didn't elaborate any further on what this was.

The payments Mr L was making were all identifiably going to a cryptocurrency merchant. As I've explained above, by March 2023, these kind of investment scams were unfortunately more commonplace. On him attempting the payment on 23 March 2023, I would've expected Revolut to provide Mr L with an automated warning tailored to this kind of scam, to try and mitigate the financial risk presented by the payment. It should've provided a warning that covered off key features of a cryptocurrency investment scam, such as warning him about celebrity endorsements; the use of AnyDesk; a broker who isn't regulated; being promised high returns; and being asked to move money between accounts to buy cryptocurrency. A number of these things would've directly related to Mr L's situation.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr L suffered from the 2nd payment of £3,000 onwards?

Mr L has shared the circumstances of this scam and as above, a number of its features would've been covered by a cryptocurrency investment warning. At this time, it doesn't seem he was overly invested in the scam and he hasn't described a level of pressure that would indicate he would've quickly by-passed a warning without properly reading it. I also haven't seen evidence he was actively coached to ignore a warning – the scam chat I do hold suggests he made the payments independently, as the scammer checks in to see if they have been completed. So, I haven't seen any reason he wouldn't have read the warning and realised that his investment opportunity mirrored the scams described. And that the payment he was trying to make was in fact likely going to a scam.

I consider Mr L wouldn't have reattempted the payment and would've ceased contact with the scammer at this time. While our Investigator wasn't persuaded the last set of payments Mr L made were because of this same scam, I consider it most likely they were. Considering what the caller knew about Mr L and his 'investment' it seems likely all contact came from the same group of scammers. But this reinforces the overall finding reached, that a warning on the second payment would've prevented Mr L making any of the later reported scam payments.

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

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

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the payments were made to a cryptocurrency merchant and that the payments that funded the scam were made from other accounts at regulated financial businesses (including from accounts not in Mr L's name). But as I've set out in some detail above, I think that Revolut still should have recognised that Mr L might have been at risk of financial harm from fraud when he made the second payment, and in those circumstances it should have declined the payment and made further enquiries.

If it had taken those steps, I am satisfied it would have prevented the losses Mr L has 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 L's own account does not alter that fact and I think Revolut can fairly be held responsible for his loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

Should Mr L bear any responsibility for their losses?

Our Investigator set out why she considered Mr L should also share liability for his losses and Mr L accepted the Investigator's assessment. But for completeness I will also address this here and why I agree with this deduction.

I've considered this scam as a whole and what Mr L understood he was doing and why. Mr L found out about this opportunity through a celebrity endorsement online and says found positive reviews about the company. But having done searches myself for the information available around the time Mr L invested, I haven't been able to find these. Mr L didn't receive any paperwork for the investment and the messages came through personal numbers on Whatsapp. Looking at the information he held, I'm not persuaded that Mr L had enough for him to be confident this was a genuine opportunity.

Later in the scam Mr L considerably increased his investment and used borrowed funds towards the scam, both from his friend and his business. And some of this was to get a return of nearly double the amount he was being asked to invest. I consider this should've

seemed too good to be true and been a red flag for him. And I'm aware the last set of payments Mr L made were due to an unexpected call from a different person. They got him to download AnyDesk and set up a new wallet elsewhere. It doesn't seem Mr L carried out any additional research or checks at this time, including with the original scammer to confirm if what this person said was true. I know when Mr L contacted them after making the payment, they said it wasn't. Instead, he followed the instructions of this unknown party, resulting in a further loss.

Considering what happened overall, I'm satisfied that Mr L should be held equally responsible for his losses here. He ought to have done more in depth checks before sending funds and there were red flags that ought to have concerned him. So I consider Revolut and Mr L should equally share responsibility from the time Revolut should've intervened.

Putting things right

As some of the funds Mr L sent came from money he borrowed, I've considered what the correct redress is in this case. Mr L has confirmed he has to repay his father and the two amounts involving his business. And that he has already repaid the friend he borrowed the funds from. Due to this, I'm satisfied it is fair for Revolut's refund to Mr L to include the borrowed funds.

I direct Revolut Ltd to:

- Refund Mr L the payments he made due to this scam from the £3,000 payment on 23 March 2023 onwards, minus 50% for his contributory negligence
- Mr L did receive three credits after the date I'm refunding from, so Revolut can also reduce the amount it refunds him by 50% of these credits
- Pay 8% simple interest per annum on the refunded amounts from the date of each payment until the date of settlement

My final decision

For the reasons set out above, I uphold in part this complaint and require Revolut Ltd to pay Mr L the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 28 February 2025.

Amy Osborne
Ombudsman