DRN-4411458

The complaint

Mr M complains that Revolut Ltd didn't do enough to protect him when he fell victim to an investment scam.

What happened

Mr M received an email from a friend referring him for an investment opportunity. He provided his details to this company, who turned out to be a scam investment. Mr M built rapport with his contact at the company and opened an account with Revolut to facilitate him buying cryptocurrency to then invest. Mr M understood he was investing from early March 2023 until late May 2023, when he made several large payments to withdraw his funds but didn't receive anything back. Mr M then realised he'd been scammed.

Mr M complained to Revolut, via a representative, and said Revolut ought to have intervened on the payments. Revolut didn't uphold Mr M's complaint so he came to our service.

Our Investigator partially upheld Mr M's complaint and said Revolut should refund him 50% of his losses from the second payment made. He said the intervention Revolut did at this time wasn't sufficient and a better intervention would've unravelled the scam. But he felt Mr M had equally contributed to his loss. Mr M accepted the view, Revolut asked for an ombudsman to reconsider the case.

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 M 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. It did in this case.

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;

[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_/

- 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 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

[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"

(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 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 M was at risk of financial harm from fraud?

In this case Revolut did recognise a potential risk of harm on the second payment Mr M made. This is the same point I'd have expected it to have concerns about a financial harm risk and so intervene.

Mr M's account had been open under a week and he was trying to make a £7,050 card payment to a cryptocurrency merchant when his account opening purpose was "spend or save daily". So this wasn't in line with what he'd recently told Revolut he was doing. Revolut declined this card payment and spoke to him through in-app chat at this time.

What kind of warning should Revolut have provided? Would that have prevented the losses Mr M suffered from the second payment?

I have reviewed the questions Revolut asked and the information it did share with Mr M

when it intervened. I don't consider the questions went far enough or that the warning it gave when Mr M explained he was buying cryptocurrency was sufficient. Revolut focussed on him potentially being pressured and being told he'd receive high returns. But it didn't go into any more detail on any of the other common features of these kind of scams – which is what I would've expected it to do.

Specifically, after being told by Mr M he was investing in cryptocurrency, Revolut said: "…*Please be aware that scammers are using increasingly sophisticated techniques to gather personal information and convince customers to transfer funds in complex scams. If you have any concerns then do not proceed and let us know, we will be here to further assist you...*"

This warning doesn't give examples of the kind of complex scams happening, so Mr M could understand what it really meant. The warning is very general in nature and it's difficult to see how it would resonate with Mr M or the specific circumstances of a cryptocurrency scam. I don't think that providing the warning above was a proportionate or sufficiently specific mechanism to deal with the risk presented. I think Revolut needed to do more.

As Mr M had shared he was investing in cryptocurrency and these kind of scams were unfortunately more commonplace by March 2023, I would've expected Revolut to ask Mr M additional questions about what he was doing. For example how he found out about the investment opportunity and/or whether he was receiving any help with it. And to warn him about the common features it knew of these kind of scams, such as out of the blue contact; the use of AnyDesk; a broker who isn't regulated; and being asked to move money between accounts to buy cryptocurrency. All of these things would've directly related to Mr M's situation.

While Revolut did ask Mr M if he had recently downloaded AnyDesk, it didn't give any context for why this was important. In this case, he already had it downloaded prior to the scam, so he honestly answered "No". Had Revolut asked a question around the *use* of screensharing software such as AnyDesk, rather than about downloading it recently, I think he'd have been honest and said he was. He'd shared he was investing in bitcoin. And from the use of AnyDesk and other information it ought to have gathered, it would've been able to identify Mr M was likely being scammed.

I therefore think that if Revolut had intervened proportionately on the second payment, asking Mr M further questions and giving him a tailored warning relating to what he shared he was doing, Revolut could've prevented his losses from this point on. I think Mr M then would've realised he was being scammed and stopped contact with the scammer.

Should Mr M bear any responsibility for his losses?

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

Mr M found out about this opportunity through an unexpected email from a friend. Mr M didn't contact the friend or discuss the email further, but went ahead with the investment based on this email alone. He didn't speak to his friend until months later, after he realised he'd been scammed. Mr M's friend had been hacked and hadn't invested. Mr M said he found positive reviews online which is part of why he went ahead, but there are negative and concerning reviews available from around the time Mr M started investing.

Later in the scam Mr M considerably increased his investment and used borrowed funds towards the scam, but he didn't do any further checks or research. By this stage an FCA

warning had been published about the scammer.

Considering what happened overall, I'm satisfied that Mr M should be held equally responsible for his losses here. He could've been more proactive with the information he shared with Revolut when it spoke to him. And he ought to have done more in depth checks before investing, which should've revealed concerning information. So I consider Revolut and Mr M should equally share responsibility from the time Revolut should've intervened.

Could Revolut have done anything to recover Mr M's money?

All the payments were made by card to a cryptocurrency provider. Mr M then sent that cryptocurrency to the scammers. So, Revolut wouldn't have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that Mr M received the cryptocurrency, which he subsequently sent to the scam.

Putting things right

I require Revolut Ltd to:

- Refund Mr M the payments he made to the scam from the £7,050 payment on 9 March 2023 onwards, minus 50% for his contributory negligence
- Mr M did receive two credits after the date I'm refunding from, so Revolut can also reduce the amount it refunds him by 50% of these two credits
- Pay 8% simple interest per annum from the date of each payment until the date of settlement

My final decision

For the reasons set out above, I partially uphold Mr M's complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 7 February 2025.

Amy Osborne
Ombudsman