DRN-5207884

The complaint

Mr H complains that Revolut Ltd ("Revolut") didn't do enough to protect him when he fell victim to a scam.

What happened

The details of this complaint are well known to both parties, so I won't repeat them again here. Instead, I'll summarise what happened and focus on the reasons for my decision.

Between June and July 2023, Mr H lost almost £35,000 to a scammer, believing he was investing in a legitimate company. The payments were all made to a cryptocurrency exchange using his debit card.

After realising he'd been scammed, Mr H complained to Revolut. It wasn't able to recover his money and it didn't uphold his complaint. In short, it said that Mr H had authorised the payments, hadn't taken enough care to ensure the investment was genuine and said the returns were unrealistic.

Unhappy with this, Mr H brought his complaint to us. Our investigator concluded that Revolut ought to have recognised that Mr H was at risk of financial harm from his first payment which was significant, out of character and identifiably being paid to a cryptocurrency exchange. He thinks Revolut should have provided a tailored written warning and that this would have exposed the scam. But he also felt that Mr H should share liability equally due to contributory negligence.

Mr H agreed but Revolut didn't. It said Mr H had made payments to his own cryptocurrency account and felt that any interventions by other providers, from where Mr H's lost funds originated, should be considered.

So the complaint has been passed to me to decide.

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.

Having done so, I'm upholding this complaint in part, as our investigator did – I'll explain why.

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 H 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 June 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 EMIs like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in June 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

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

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

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

practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 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 June 2023, Revolut should in any event have taken these steps.

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

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

I'm aware that cryptocurrency exchanges, such as that which Mr H paid, generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of

the account holder. Revolut would likely have been aware of this fact too. So it could reasonably have assumed that all of the payments would be credited to a cryptocurrency wallet held in Mr H's name.

By June 2023, when these transactions started to take 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. And by the end of 2022, many high street banks had taken steps to limit their customer's ability to purchase cryptocurrency using their bank accounts, on increase friction in relation to cryptocurrency related payments. And by June 2023, when these payments took place, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our Service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr H made in June 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.

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 H's own name should have led Revolut to believe there wasn't a risk of fraud.

I think Revolut should have identified that Mr H was at risk from the point of the first payment. This payment was for £3,000 which was significantly higher than payments made in the preceding 12 months and was identifiably being paid to a cryptocurrency exchange, which Mr H hadn't previously done. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr H was at heightened risk of financial harm from fraud.

What did Revolut do to warn Mr H?

Based on the evidence I've seen, Revolut didn't provide any warnings to Mr H. And, for completeness, I note here that information from third party banks suggests that the banks from where funds originated also didn't provide any warnings.

I note that Revolut has shown warnings which it says Mr H would have seen at the point of using a screen-sharing application. These state that another person would like access to his device and, by accepting, that person can do everything he can on the device, such as sending money.

But, while I don't discount this warning entirely, I don't consider that it's sufficient to rely on this warning from the screen-sharing application. It's very general in nature and it's difficult to see how it would have resonated with Mr H – he would have already been aware that

someone wanted to access his device as the intention was for the 'agent' to demonstrate how to make a withdrawal. So it wouldn't have given any suggestion that the investment wasn't legitimate.

So, in summary, Revolut didn't sufficiently warn Mr H – it needed to 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 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.

Taking that into account, I think Revolut ought, when Mr H attempted to make the first payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning 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 and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr H by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

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

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr H's payments, such as finding the investment through an advertisement endorsed by a public figure, being assisted by a broker and being asked to download remote access software so they could help him with the withdrawal process.

Mr H has told us he communicated with the scammer over the telephone, so I've not been able to review the conversations between them. But he told our Service that he wasn't asked to respond to his banks in a particular way, just that he was advised to make payments in smaller increments.

So, I'm not persuaded that Mr H was asked, or agreed to, disregard any warning provided by Revolut. I've also not been given any indication that Mr H expressed mistrust of Revolut or financial firms in general. In fact, he received an email that appeared to be from Revolut shortly after the final payment, talking about the need to 'mirror' payments. It's clear this was an attempt from the scammer to obtain further funds from Mr H. So it's unlikely that the

scammer would have used an email from Revolut to try to obtain further funds if it had given Mr H the impression he shouldn't trust Revolut.

I've not seen evidence to persuade me that Mr H wouldn't have listened to the advice of Revolut. And the bank from which the funds used for the scam appear to have originated has said it didn't provide any warnings.

Therefore, on the balance of probabilities, had Revolut provided Mr H with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I think it likely it would have resonated with him. He could have paused and looked more closely into the company he was investing in before proceeding. I'm persuaded that a timely warning to Mr H from Revolut would very likely have prevented his losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr H paid money using his Revolut account to another account in his own name, rather than directly to the fraudster.

But as I've set out above, I think that Revolut still should have recognised that Mr H might have been at risk of financial harm from fraud from the first payment. And, in those circumstances, it should have made further enquiries. If it had done so, I'm satisfied it would have prevented the losses Mr H suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr H's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr H'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 H 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 H could instead, or in addition, have sought to complain against those firms. But Mr H 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 H'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 H's loss from the first payment (subject to a deduction for consumer's own contribution which I will consider below).

Should Mr H bear any responsibility for his losses?

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

I recognise that Mr H was an inexperienced investor and had seen an advert appearing to show a well-known celebrity endorsing the investment. While I've not seen the advert, I'm

aware these can be convincing. I also know that, as appears to have been the case here, scammers often use the apparent success of early trades and the apparent ability to withdraw funds to encourage increasingly large deposits. So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr H to be reduced. And I think it should.

Mr H said he'd researched the company before investing. But there was a published warning, prior to the first payment made, on the Financial Conduct Authority's website noting the company was unauthorised and may be providing financial services or products without permission. This should have been uncovered from relatively limited researching of the company. I also note that the supposed rate of returns of the investment looks to have been too good to be true. Though Mr H has mentioned the withdrawal of returns, which provided him with reassurance, it looks as though he only received one withdrawal to his own account – of a modest amount – before committing significant funds to the investment. So I think Mr H has contributed to his own losses.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr H 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

For the reasons given above, I uphold this complaint in part and direct Revolut Ltd to pay Mr H:

- 50% of his losses from the first payment onwards;
- 8% simple interest per year on that amount from the dates of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 15 April 2025.

Melanie Roberts
Ombudsman