DRN-4985564

Complaint

Ms H is unhappy that Revolut Ltd didn't refund her losses after she fell victim to a scam.

Background

In December 2022, Ms H began researching different investment opportunities. She says she filled out several enquiry forms with various companies. Subsequently, she was contacted by an individual claiming to represent an investment company, which I will refer to as "F." The agent explained how the investment opportunity would work, advising Ms H to deposit money into an online account, after which they would trade funds on her behalf. She didn't know it at the time, but the agent was not a representative of a legitimate investment company but a fraudster.

The fraudster provided Ms H with a link that appeared to show F was regulated by the Financial Conduct Authority (FCA). In hindsight, it seems the fraudsters were imitating an otherwise genuine firm. After expressing her interest, Ms H was taken through a fake Know Your Customer (KYC) process, which she says reassured her that she was dealing with an authentic organisation. Ms H was informed she would need to start with a £250 deposit, which she made from an account with a different firm. The scammer directed her to their website, where she could view her "investment." The website appeared genuine to Ms H, showing real-time trading updates and significant growth in her investment.

She was asked to download remote access software so that the agent could help her with the process of making her investments. As I understand it, she made payments direct to the e-wallet of a third-party cryptocurrency exchange. Those deposited funds were then converted into cryptocurrency and transferred to an e-wallet under the control of the fraudster. Ms H isn't entirely sure how this took place, so it seems likely that the fraudsters made use of remote access software to move Ms H's funds out of her control.

In March 2023, Ms H attempted to withdraw her proceeds. She received an email, purportedly from a third-party business involved in facilitating her investment, stating her account had been flagged for enhanced anti-money laundering checks. She was told she needed to pay 50% of the value of her intended withdrawal to complete the process.

Throughout the scam, Ms H made the following payments from her Revolut account using her card:

	Date	Value
1	22 February 2023	£1,300
2	8 March 2023	£5,000
3	8 March 2023	£115

Upon realising she had fallen victim to a scam, Ms H reported the matter to Revolut. However, Revolut declined to refund her losses, stating that the payments were authorised by Ms H and that it had executed her instructions. Revolut also said there was no scope for recovering her losses through the chargeback process.

Ms H wasn't happy with that response and so she referred her complaint to this service. An Investigator reviewed the case and partially upheld it. He concluded that Revolut should have been concerned by the £5,000 payment and intervened at that point. They were persuaded that an appropriate intervention would have prevented both the £5,000 payment and the subsequent £115 payment. However, the Investigator also considered it fair and reasonable for Ms H to bear some responsibility for her losses due to contributory negligence.

Revolut disagreed with the Investigator's findings, and the complaint has now been passed to me for a final decision.

Findings

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 customer'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 Ms 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 must also 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 undertaken 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 March 2023, Revolut, where 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 function).

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 *"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

[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.

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.
- 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 undertaken 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-

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

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 Ms H was at risk of financial harm from fraud?

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that these payments would be credited to a cryptocurrency wallet held in Ms C's name.

By March 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. 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 Ms H 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'm also mindful of the fact that this was a new account. Ms H only opened the account on the advice of the fraudster. That put Revolut in a more difficult position in respect of spotting payments that might have had an associated fraud risk because there was no historical data concerning her typical account usage that could've served as a basis of comparison. Nonetheless, I agree with the Investigator's conclusions that it ought to have had concerns at the point of the payment 2. I find that the value of the payment alongside the fact that it

was being made to a third-party cryptocurrency exchange was significant enough to necessitate Revolut taking some steps to warn Ms H.

What did Revolut do to warn Ms H?

From the evidence that has been shared with me, Revolut didn't provide Ms H with a warning when making payment 2. 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 Ms C attempted to make payment 2 knowing (or strongly suspecting) that the payment was going to a cryptocurrency exchange, 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.

At this point in time, I think that such a warning should have addressed the key risks and features of the most common 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 such 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 Ms 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 Ms H suffered from the second 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 Ms H's payments, such as finding the investment through an advertisement on social media, being assisted by a broker and being asked to download remote access software.

There's no evidence to suggest Ms H was asked, or agreed to, disregard any warning provided by Revolut. Ms H tells me that the fraudster told her that this was a *"routine transaction."* On the balance of probabilities, if Revolut had provided her with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not she was genuinely dealing with the company that was regulated in the UK. I'm satisfied that a timely warning to Ms H from Revolut would very likely have caused her to do so, revealing the scam and preventing her subsequent losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that payment 2 was made to an account in Ms H's own name and that, at the point the funds left her Revolut account, she hadn't experienced any financial loss. But as I've set out in some detail above, I think that Revolut still should have recognised that she might have been at risk of financial harm from fraud when she made that payment, and in those circumstances it should have provided a tailored warning.

If it had taken those steps, I am satisfied it would have prevented the losses Ms H 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 her own account does not alter that fact and I think Revolut can fairly be held responsible for her 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 Ms C 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 she could instead, or in addition, have sought to complain against those firms. But she's not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce her compensation in circumstances where: she has only complained about one respondent from which she is entitled to recover her 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 Ms H's loss from payment 2 (subject to a deduction for her own contribution which I will consider below).

Should Ms H bear any responsibility for their losses?

I've also considered whether it would be fair and reasonable for Ms C to be considered partially responsible for her own losses here. In doing so, I've taken into account what the law says about contributory negligence while keeping in mind that I need to decide this case based on what I consider to be fair and reasonable in all the circumstances.

Having done so, I do think Ms C should be considered partially responsible here. The returns that she believed that she'd earned were extraordinary. She'd invested £1,300 and believed she was withdrawing earnings of over £10,000. The value of her investment had increased by over 600% in two weeks – or an annual equivalent of around 16,000% per year. I accept that she was inexperienced in these matters and had never invested before, but I think the returns that were promised to her were so high that she ought to have recognised that they were simply too good to be true. For that reason, I think it's fair and reasonable for Revolut to make a deduction of 50% from the redress that is payable to Ms H.

For completeness, I also considered whether Revolut did everything I'd have expected it to in terms of recovering Ms H's funds. As I explained above, it's likely that these payments went to an account set up in her own name and then moved on – so it's likely that none of

her funds were left in the receiving account when she notified Revolut that she'd fallen victim to a scam.

Final decision

For the reasons I've explained above, I uphold this complaint in part.

If Ms H accepts my final decision, Revolut Ltd need to refund 50% of payments 2 and 3. It should also add 8% simple interest per annum to those payments calculated to run from the date the payments left her account until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms H to accept or reject my decision before 20 March 2025.

James Kimmitt
Ombudsman