DRN-4979803

The complaint

Mrs C complains that Revolut Ltd didn't do enough to protect her from the financial harm caused by an investment scam, or to help her recover the money once she'd reported the scam to it.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

In December 2022, Mrs C saw an advert on social media for an investment company which I'll refer to as "R", which was endorsed by a well-known celebrity. The advert claimed that Mrs C could make money by investing in cryptocurrency, and so she completed an online form and paid £250 to register with R.

Mrs C was then contacted by someone who I'll refer to as "the scammer" who said she would be her account manager. She said she'd been working in finance and cryptocurrency for years and would make trades on Mrs C's behalf using an expert AI algorithm.

Mrs C checked R's website, which appeared legitimate and featured photographs of stock trades showing cryptocurrency values which correlated with the current state of the market, and various tabs for 'support,' 'contact us' and 'learning.'

The scammer advised her to download AnyDesk onto her device to enable her to place the trades and to open an account on R's trading platform, which required her to provide ID. The scammer also told Mrs C to open accounts with cryptocurrency exchange companies, which I'll refer to as "B" and "M".

The broker asked her to first purchase cryptocurrency through B and then load it onto an online wallet. She transferred funds from Bank L to her Revolut account (which she opened on 12 August 2022), and between 8 December 2022 and 31 March 2023, she made sixteen payments to B and M totalling £73,876.26 using her Revolut card. She didn't make any withdrawals during the period and four payments were reverted by the merchant.

When she logged into the account, Mrs C could see the scammer place trades on her behalf, and she was receptive when her encouraged her to invest more. She asked to withdraw her funds in February 2023, and in March 2023 she was told she'd have to pay withdrawal fees, which she agreed to pay.

On 31 March 2023 Mrs C was contacted by someone claiming to her new account manager who said the previous manager had broken the law by putting her own funds into Mrs C's Revolut wallet. He said that before she could make a withdrawal, she'd need to pay tax on her profits. Mrs C paid £46,000 over eight payments, funded partly by a loan which the scammer had encouraged her to take out. Mrs C realised she'd been scammed when she was asked to pay yet more fees, at which point she spoke to a family member who advised her that the investment was a scam.

Mrs C complained to Revolut with the assistance of a representative who argued that it should have intervened on 23 February 2023 because even though there was no spending history on the account, Mrs C had sent £4,426.26 to a new payee which was a high-risk cryptocurrency merchant. They said it should have questioned her about the payments and provided effective warnings, explaining how investment scams can look and feel, and the consequences of proceeding with the payments should she ignore the advice. Specifically, it should have contacted her either via phone or its live-chat facility and asked her why she was making the payment, who she was trading with, how she found out about the company, whether she'd checked the Financial Conduct Authority ("FCA") website, whether she'd been promised unrealistic returns and whether she'd been pressured to make the payment.

They argued that, had it done so, Mrs C hadn't been prompted to give false answers and so she'd have disclosed the existence of the broker and it would have realised the investment had the hallmarks of a scam. It could then have advised her on how to check the investment company was genuine, and the scam would have been detected.

Revolut refused to refund any of the money Mrs C had lost. It said she'd contacted it a month and a half after the scam and filed fraud chargeback claims on 15 May 2023 for nine of the transactions. It said all the transactions were authenticated via 3DS, so they weren't valid for chargeback. It explained that a new chargeback claim was later raised under the dispute category, but the claim was out of time.

Mrs C wasn't satisfied and so she complained to this service with the assistance of a representative who said Revolut failed to provide effective warnings which would have prevented her from making the payments.

Revolut said the funds didn't originate from the account, and there was no spending history to compare the payments with. It said it's common for customers to use Revolut to send funds to cryptocurrency merchants, so the activity wasn't seen as suspicious. And when she opened the account, she stated that the purpose of the account was 'crypto', so the payments matched the accounts intended purpose.

It said Mrs C wasn't presented with any warnings and there was no reason to suspect there were any issues because Mrs C was paying an account in her own name, so the transactions from Revolut weren't fraudulent. It also said the external bank probably had a better overall view of her spending behaviour and the relevant transactions would likely have been objectively more suspicious when leaving that account.

It also said she'd taken out a loan on the advice of someone she'd met on social media, and had sent the funds on the promise of unrealistic returns, yet she didn't complete any due diligence.

Our investigator thought the complaint should be upheld. She said that even though Mrs C hadn't used her account for a long time, Revolut knew she was making payments to a cryptocurrency merchant, so it should have recognised the payments carried a higher risk of fraud. She thought it should have flagged the £10,500 payment on 20 March 2023 because it was high value.

She explained that a proportionate response would have been for Revolut to provide a written warning covering some of the key features of cryptocurrency-related investment scams, including the fact victims are usually targeted via social media or email, scammers will utilise fake positive reviews from other individuals, or fake celebrity endorsements, fake online trading platforms can appear professional and legitimate and genuine investment platforms won't require customers to pay fees to withdraw funds.

Had it done so, she was satisfied Mrs C would've identified the similarities between the investment and the content of the warning, the scam could've been uncovered, and her loss would have been prevented. So, she thought Revolut should refund the money Mrs C had lost from 20 March 2023 onwards.

Our investigator explained that the WhatsApp messages between Mrs C and the scammer showed she had concerns about the investment before she made any payments, but there wasn't much information available online about R at the time, and the reviews were mostly positive. However, on 27 February 2023, she messaged the scammer several times with concerns around her request to withdraw funds. Our investigator noted that by this time, there were several negative reviews from others claiming they'd been scammed and as this represented a missed opportunity to have prevented the scam, she thought the settlement should be reduced by 50% for contributory negligence.

Finally, our investigator explained Mrs C would have received a service from the cryptocurrency exchange, so she didn't think Revolut had acted unfairly when it considered the chargeback claim, and she didn't think she was entitled to any compensation.

Revolut asked for the complaint to be reviewed by an Ombudsman, explaining that, typically, this type of account is opened and used to facilitate payments for a specific purpose and often not used as a main account. It argued that the payments were self-to- self transactions, so the fraudulent activity didn't occur on the Revolut platform. And to effectively apply the reimbursement rules is an error of law and such transactions are distinguishable from transactions subject to the regulatory regime concerning APP fraud.

My provisional findings

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 Mrs C 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 was 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 considered 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 was 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;

• 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, 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 was 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).

• 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 Code3, 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 considered 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 was 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 consumer was at risk of financial harm from fraud?

The payments didn't flag as suspicious on Revolut's systems. The first three successful payments were relatively low value, Mrs C was paying a legitimate cryptocurrency exchange, and the payments were in line with the account opening purpose of 'crypto', so I wouldn't have expected Revolut to intervene. However, by the time Mrs C made the second payment on 23 February 2023, the cumulative total for the day was £4,426.26 and she was paying a high-risk cryptocurrency merchant, so it ought to have intervened.

What kind of warning should Revolut have provided?

I thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I took into account that many payments that look very similar to this one will be entirely genuine. I explained that I'd given due consideration to Revolut's duty to make payments promptly, as well as what I considered to have been good industry practice at the time this payment was made.

Taking that into account, I thought Revolut ought, when Mrs C attempted to make the second payment on 23 February 2023 payment, knowing (or strongly suspecting) 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 recognised 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 thought 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 recognised that a warning of that kind could not have covered off all scenarios. But I thought it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mrs C 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 cryptocurrency investment scam warning, would that have prevented the losses Mrs C incurred after that point?

I 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 thought it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs C'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 open cryptocurrency wallets.

I hadn't seen any evidence that Mrs C was asked, or agreed, to disregard any warning provided by Revolut. I'd seen no indication that she expressed mistrust of Revolut or financial firms in general. And at the point I said Revolut ought to have intervened, she wasn't yet paying fees to access her investment. Further, I looked at messages between Mrs C and the scammer and they didn't demonstrate a closeness of relationship that Revolut would have found difficult to counter through a warning.

The weight of evidence that I had outlined persuaded me that Mrs C was not so taken in by the fraudsters that she wouldn't have listened to the advice of Revolut and she wasn't provided with warnings by other firms. Therefore, on the balance of probabilities, had Revolut provided Mrs C with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believed it would have resonated with her. She could have paused and looked more closely into the scammer before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the scammer was regulated in the UK or abroad.

I was satisfied that a timely warning to Mrs C from Revolut would very likely have caused her to take the steps she did take later – revealing the scam and preventing her further losses.

Is it fair and reasonable for Revolut to be held responsible for Mrs C's loss?

I thought that Revolut should have recognised that Mrs C might have been at risk of financial harm from fraud when she made the payment on 23 February 2023 and provide a tailored written warning relevant to cryptocurrency investment scams. Had it done so, I was satisfied it would have prevented the losses Mrs C suffered.

The fact the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mrs C's own account does not alter that fact and I thought Revolut could fairly be held responsible for Mrs C's loss in such circumstances. I didn'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 also considered that Mrs C had only complained against Revolut. I accepted 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 consumer could instead, or in addition, have sought to complain against those firms. But consumer has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I was also not persuaded it would be fair to reduce Mrs C's compensation in circumstances where: she had 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 set out above, I was minded to hold Revolut responsible for Mrs C's loss from the 23 February 2023 payment.

Should Mrs C bear any responsibility for her losses?

In recent years instances of individuals making large amounts of money by trading in cryptocurrency have been highly publicised to the extent that I didn't think it was unreasonable for Mrs C to have believed what she was told by the broker in terms of the returns she was told were possible.

She hadn't invested in cryptocurrency before and so this was an area with which she was unfamiliar. She didn't know the returns were unrealistic, how to check the information she'd been given, or that celebrity endorsements are a red flag for fraud. This unfamiliarity was compounded by the sophisticated nature of the scam, the fact she trusted the scammer and the fact she believed the trading platform was genuine and was reflecting the fact her investments were doing well.

It's significant that there wouldn't have been any negative information about R if she'd done some due diligence before deciding to go ahead with the investment. I accepted a targeted search concerning the celebrity endorsement would have revealed some information related to the use of the celebrity's name in scams, but as she initially thought the investment was genuine, I didn't think it's unreasonable that she didn't do this.

However, the messages between Mrs C and the scammer show she asked repeatedly when she would make a withdrawal on 27 February 2023, and after being told she'd need to make further payments into the account, she took funds from her pension and paid out £10,000 and £5,000 to the scam on 20 March 2023 and 21 March 2023. I thought Mrs C ought reasonably to have asked more questions around why she was being required to make payments into her account before being permitted to withdraw her funds and, had she done some further checks at this point, she might have seen some negative reviews suggesting R was operating a scam. I agreed with our investigator that this might have prevented her loss, so I was minded to direct that the settlement for the payments she made from 20 March 2023 onwards point should be reduced by 50% for contributory negligence.

Recovery

I thought about whether Revolut could have done more to recover Mrs C's payments when she reported the scam to it.

Mrs C has described that she paid an account in her own name and from there the funds were moved to an online wallet in the scammer's control, so I was satisfied there was no prospect of a successful recovery.

Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Revolut) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mrs C).

Mrs C's own testimony supports that she used cryptocurrency exchanges to facilitate the transfers. Its only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mrs C's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I was satisfied that Revolut's decision not to raise a chargeback request against either of the cryptocurrency exchange companies was fair.

Further, the scheme sets the rules and there are specific time limits that must be applied. Those rules state that a claim can be brought no later than 120 days than the date of the transaction. In Mrs C's case, the second claim was referred after this time.

Compensation

The main cause for the upset was the scammer who persuaded Mrs C to part with her funds. I haven't found any errors or delays to Revolut's investigation, so I didn't think she was entitled to any compensation.

Developments

Mrs C has said she accepts my provisional findings, and Revolut hasn't responded.

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.

Because neither party has made any additional comments or submitted any additional evidence, the findings in my final decision will be the same as the findings in my final decision.

My final decision

My final decision is that Revolut Ltd should:

• refund the money Mrs C lost from the second payment on 23 February 2023 onwards.
• the settlement for the payments from 20 March 2023 onwards should be reduced by 50% to reflect contributory negligence.
• pay 8% simple interest*, per year, from the respective dates of loss to the date of settlement.

*If Revolut deducts tax in relation to the interest element of this award it should provide Mrs C with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs C to accept or reject my decision before 6 January 2025.

Carolyn Bonnell
Ombudsman