DRN-4460707

The complaint

Miss C complains that Revolut Ltd hasn't protected her from losing money to a safe account scam.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, Miss C has explained that on 17 April 2023 she received a call from a scammer purporting to be from Revolut's fraud team, and she was tricked into falsely believing both her Revolut account, and another account she held with a third-party bank ("H"), had been compromised. As a result, Miss C was tricked into first transferring £25,000 from her account with H to her Revolut account, and, then, into sending £24,990 from her Revolut account to a 'safe account' (the scammer's account held with Revolut).

Miss C subsequently realised she'd been scammed and got in touch with Revolut. Ultimately, Revolut didn't reimburse Miss C's lost funds, and Miss C referred her complaint about Revolut to us concerning both Revolut's role as Miss C's sending payment service provider ("PSP") *and* its separate role as the receiving PSP (the scammer's account provider). As our Investigator couldn't resolve matters informally, the case has been passed to me for a decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

This decision concerns both Revolut's role as Miss C's sending PSP, and its separate role as the receiving PSP (the scammer's account provider). I'll address these in turn.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

Revolut as the sending PSP

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 Miss C modified the starting position described in *Philipp,* by 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*".

So Revolut was required by the implied terms of its contract with Miss C and The Payment Services Regulations to carry out her instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in April 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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 do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- 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] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

[2] 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, 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)[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 Code[4], 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.

---

[3] 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.

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

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 April 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.

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

Miss C opened her account with Revolut in 2020. And I agree with what our Investigator said about this. Miss C used her Revolut account for relatively small transactions on a regular basis. From 2020 up until the date of this payment, there were few transactions which exceeded £200. She certainly had never before made a payment from her Revolut account of anywhere close to £24,990. And being for such an amount, and to a new payee, I'm satisfied that Revolut should have been on alert, when Miss C instructed this payment, that she was at risk of financial harm from fraud.

Our Investigator also noted that "Confirmation of Payee" was in place when Miss C instructed this payment. Confirmation of Payee is a system by which, when instructing a payment, the actual name of the recipient account holder is cross-referenced with the details input by the payer (here, Miss C). Revolut has provided information showing Confirmation of Payee, in this instance, showed the result of not matched, meaning the actual name of the recipient account holder appeared not to match Miss C's intended recipient based on the details for the payment instruction she entered. But, in any event, I'm satisfied that because of the size of the payment, it's unusualness for Miss C's account, and the fact it was to a new payee, Revolut ought to have been on alert anyway that Miss C was at risk of financial harm from fraud. But I agree with the Investigator that the fact that Confirmation of Payee didn't match is a further reason here also.

What did Revolut do to warn Miss C?

Revolut has explained that:

- Because Confirmation of Payee showed a result of not matched, Miss C would have, in-app, been shown a warning which stated, *"Account name doesn't match. The recipient's bank said name you entered is not the name on account. Please double check the details and only continue if you're sure the recipient is trustworthy"*.

- Miss C nonetheless clicked to continue with the payment anyway, and she would then have been redirected to in-app screens which said that:

  "Do you know and trust this payee? If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others, and we will never ask you to make a payment"

  and…

  "Please beware if you've been: (1) Instructed by someone you don't know or have recently met to move money from your account. (2) Told your account is at risk, to move funds to a safe account or to take out a loan. (3) Threatened with additional fines or being arrested. (4) Given an offer that seems too good to be true. You risk losing money that we may not be able to recover".

- The payment was then automatically set to pending on its systems. And, in-app, it asked Miss C about the purpose of the payment, from which Miss C could choose from a selection of:

  "Transfer to a 'Safe Account'"
  "Payment for Goods and Services"
  "Investment"
  "Paying HMRC or Tax Authority"
  "Paying Revolut"
  "Something Else"

  Revolut has provided information showing Miss C, from these options, selected *"Payment for Goods and Services"*. And that, consequently, she would then have been shown a screen, in-app, that warned her:

  "Beware, there is a high probability that this payment is a scam. Before sending your money, please beware that: (1) Scammers will typically offer a price below market value to attract your attention. (2) You should not pay via bank transfer when card payment options are available. (3) Social media has become an easy way for scammers to advertise their goods and services. (4) Do lots of research when buying from a retailer for the first time – Are there many negative reviews? (5) Revolut and other trustworthy organisations will NEVER tell you to ignore this warning".

- Revolut has also said that, as part of these warnings in-app, Miss C would also have been offered to chat, in-app, to its customer support specialists before proceeding, and that she would also have been provided with a link to its blog where it educates its customers on different types of possible scams in further detail.

What kind of warning should Revolut have provided?

Revolut's warnings did contain some information relevant to Miss C's circumstances. For example: they said: *"Remember, fraudsters can impersonate others, and we will never ask you to make a payment"*; to *"Please beware if you've been:…Told your account is at risk, to move funds to a safe account…"*. And Miss C appears to have said the reason for her payment was *"Payment for Goods and Services"*, instead of the correct option which would have been *"Transfer to a 'Safe Account'"*. But we asked Miss C about these warnings and she said that she doesn't recall seeing them, although she does remember the scammer was 'overseeing' things and told her to select *"Payment for Goods and Services"* as the purpose of her payment. I don't find this particularly surprising. Given the pressure Miss C would have felt under to act with urgency – and her genuine belief that it was Revolut on the phone helping her – I'm not surprised if these warnings lacked sufficient context or impact in the circumstances of this case for Miss C to realise she was being scammed. The Confirmation of Payee result also wasn't designed to provide a specific scam warning, and doesn't do so. Miss C was convinced her funds were at risk and that she was on the phone to Revolut, so I don't think these warnings would have been impactful enough for her to be concerned.

So, overall, given the level of unusualness of Miss C's payment – and its size – I can't agree that any of these warnings were a proportionate response to the risk that Miss C's payment presented. I accept Revolut attempted some steps to prevent harm from fraud, but I think the warnings it provided were too generic to have the necessary impact, unless Miss C already had doubts about who she was speaking to (and I haven't seen any evidence suggesting that she did). Instead, I think a proportionate response to the risk here would have been for Revolut to have attempted to establish more context around the circumstances surrounding the payment before allowing it to debit Miss C's account. I think it should have done this, for example, by requiring Miss C to discuss the payment with it in the in-app chat before it allowed it to debit her account.

If Revolut had provided a warning of the type described, would that have prevented the loss Miss C suffered from this payment?

I agree with what our Investigator concluded about this. We asked H whether it intervened in the £25,000 payment Miss C made from her account with H into her Revolut account (which funded the payment of £24,990 out of her Revolut account). H has said that it didn't. I accept that it's *possible* that Miss C may still have gone ahead with the payment even if Revolut had discussed it with her in the in-app chat before allowing it to debit her account. But where I can't be certain about something, I need to make up my mind based on the balance of probabilities – in other words, based on what I think more likely than not would have happened. And here, I can see no sufficiently good reason to believe that Miss C wouldn't have responded positively to Revolut's in-app intervention. In deciding this I'm aware, of course, that Miss C didn't give an accurate response to Revolut's prior question about the purpose of her payment and that she's said this was on the instructions of the scammer. But I think that in-app discussion about the payment would have been more contextual, with it being much harder, even assuming the scammer would and could have done this, for the scammer to have directed Miss C to mislead Revolut without giving the game away, particularly bearing in mind that Miss C did think something was wrong in the scammer's behaviour on the phone after the payment had been made. So, on balance here, I'm persuaded that had Revolut directed Miss C to an in-app chat before it executed the payment instruction, it's most likely, from Revolut's interaction and warnings there-in, that Miss C would have been concerned. After all, £24,990 would be an extremely large amount of money for her to lose, and her actions were being driven by the very desire to protect her funds. So I think most likely she would have opened up and most likely, with proper handling

from Revolut, the scam would have been uncovered and Miss C would not have proceeded with the payment and her loss would have been avoided.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss C first moved £25,000 from her account with H to her Revolut account before sending £24,990 of this onto the scammers from there.

But as I've set out above, I think that Revolut still should have recognised that Miss C might have been at risk of financial harm from fraud when she made this payment, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the loss Miss C suffered. The fact that the money used to fund the scam came from elsewhere does not alter that fact and I think Revolut can fairly be held responsible for Miss C'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 the firm that is the origin of the funds.

I've also considered that Miss 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 Miss C could instead, or in addition, have sought to complain against those firms. But Miss C has 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 Miss C'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 Miss C's loss of this payment.

Should Miss C bear any responsibility for her loss?

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.

In this case, I think it's fair to say Miss C was put under pressure to act quickly, was genuinely tricked by resourceful and clever scammers, and was driven by a reasonable desire to protect her money. I'm aware that Miss C has said that the scammer asked her to download remote access software so they could guide her to safely transfer her money. And that Revolut has said that when Miss C downloaded this, she would have been shown warnings by the remote access software such as, *"Another person would like to access your device. If you accept, this person can do everything you can do on your device (e.g. sending money, reading text messages and emails, etc). Not every supporter has good intentions. If you have any doubts, please deny this request and inform yourself in our help article"*; and that, to proceed with the use of the remote access software, Miss C would have needed to click on the option *"I am aware of the risks"*. But Miss C has said that the scammer knew her personal information and explained there were fraudulent transactions taking place (which she seemed to be able to see). She's also said that she queried the number the scammer was calling from, and the scammer said it was a special internal number for the 'bank'

specific to fraud, not the general call lines. She has also plausibly said that at certain stages she had to phone the number back (and I can see from the call log screenshot Miss C provided to Revolut in the in-app chat – after the scam had occurred – that this shows outgoings calls to the number after incoming ones, backing this up) and that they explained they had wait times and it seemed very much like a bank would have. So I can understand how Miss C was tricked, bearing in mind she wouldn't know about scams like this like Revolut would. So, bearing in mind she was unwittingly tricked by the scam into thinking her account was at risk, I can't fairly say she acted with such carelessness, or disregard, that a deduction for contributory negligence would be appropriate here. So whilst there may be cases where a reduction for contributory negligence is appropriate, I'm satisfied this isn't one of them.

Recovery (by Revolut as Miss C's sending PSP)

When Miss C notified Revolut she'd been scammed it should have acted right away to notify the receiving PSP (here, this was Revolut too) to try to recover her funds. Like our Investigator, I'm unable to see any evidence that Revolut acted unreasonably at this point, as the sending PSP, in attempting to recover the funds.

Revolut as the receiving PSP

I've explained above why I think Revolut as the sending PSP can and should fairly and reasonably be held responsible for Miss C's loss of her £24,990. So there isn't any real need for me to address Revolut's separate role as the receiving PSP – because I think Revolut should fully compensate Miss C anyway (because of its actions as her sending PSP). For completeness, however, like our Investigator, I will address Revolut's role as the receiving PSP.

Revolut has shared relevant information with this service about the recipient account in confidence to allow us to discharge our investigatory functions and has provided that which is necessary for the determination of this complaint. But I'm also limited to how much of this I can share for the same reasons as Revolut. But I'd like to assure Miss C I've carefully reviewed everything before reaching my decision.

I've reached the same conclusions about this as our Investigator and for the same reasons. That is:

- **Account opening**: An account later found to have been utilised to misappropriate funds doesn't automatically entitle the payer (victim) to a refund nor does it mean that the recipient PSP unreasonably failed to prevent the loss. What I need to consider is whether at the time of opening the account Revolut ought reasonably to have known that the account being opened would later be used fraudulently. And in the circumstances of this complaint, there wasn't anything at the time that I think reasonably could've alerted Revolut that the account it was opening would later be used to misappropriate funds. So, I'm satisfied it didn't miss an opportunity to prevent the fraud when opening the account.

- **Monitoring**: I've also considered whether there was anything prior to when Revolut was notified Miss C had been scammed that ought to have alerted Revolut to the possibility of fraud. In this case, I don't think what our Investigator concluded was unreasonable. Within just 20 minutes of receipt of Miss C's funds, the recipient had spent materially all of the funds by way of card payments to a cryptocurrency-related merchant. I think the rapid spending of Miss C's money was suspicious activity. And I agree with our Investigator that Revolut reasonably ought to have blocked the recipient's fifth payment to the cryptocurrency-related merchant (which was for

£2,500) and enquired with its customer about the purpose of the account activity. Miss C's scam notification came in just a short while later so it's likely, if Revolut had done this, that remaining funds of £16,139.23 would have been recoverable.

- **Response to the fraud notification**: Once Revolut was notified of the scam I think it took appropriate actions to secure the account and no further funds were allowed to leave the account. Unfortunately, however, the vast majority of Miss C's funds were spent before her first contact with Revolut about the scam – less than £20 remained available for recovery. I can't see, however, that Revolut returned this amount (of less than £20), in circumstances where I think it should have. So whilst I don't think the pace at which Revolut acted was wrong or caused any loss, I do think Revolut failed to return to Miss C the residual amount (of less than £20), when it reasonably ought to have refunded her this amount.

Putting things right

I've explained above why I'm persuaded that if Revolut had done what it reasonably should have done, Miss C wouldn't have lost this money. I'm therefore satisfied that the fair outcome to this complaint is that Revolut pays Miss C £24,990. To compensate Miss C for having been deprived of this money, Revolut should also pay Miss C interest on this amount calculated at 8% simple per year from 17 April 2023 to the date of settlement.

My final decision

For the reasons explained, I uphold this complaint and I direct Revolut Ltd to pay Miss C:

- £24,990; plus
- interest on this amount calculated at 8% simple per year from 17 April 2023 to the date of settlement (if Revolut deducts tax from this interest, it should send Miss C the appropriate tax deduction certificate).

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 11 October 2024.

Neil Bridge
Ombudsman