DRN-5175793

The complaint

Mr K complains that Revolut Ltd didn't do enough when he fell victim to an impersonation scam.

What happened

In January 2023, Mr K received a phone call from someone purporting to be Revolut. They explained that several purchases had been attempted on his account and he needed to move his funds to keep them safe. He moved money from his savings pot to his main account. He believes he accidentally shared his card details with the scammer, and he recalls sharing a code with the caller which enabled them to set up ApplePay on their device. The caller explained Mr K's funds would be secure and that his balance would go to zero, but his funds would come back after this. Payments to a cryptocurrency merchant then started being made on Mr K's account. He saw this happening and moved funds to his partner to prevent further payments.

Mr K realised he'd been scammed and contacted Revolut. At this point, five payments had been attempted with four of these being successful. The scammer had taken payments for £1,200; £1,400; £1,800 and £1,400. Revolut advised Mr K to put in a chargeback claim for the payments, but then explained it wouldn't pursue this as the payments had gone to a genuine cryptocurrency merchant. Mr K raised a complaint about this and Revolut not protecting him, asking for all the money back. Revolut didn't uphold his complaint.

Mr K came to our service and our investigator partially upheld his complaint. They considered Revolut should've intervened on the 4th payment that was made and had it done so, the scam would've unravelled. But she held Mr K jointly liable for his losses. Revolut accepted the view, Mr K disagreed and said he wanted all the funds refunded. He said that all payments to the cryptocurrency merchant should've been scrutinised. And that the payments were all out of character for his account. So the complaint has been passed to me for a decision.

I issued a provisional decision in early November 2024. My findings were as follows:

> *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.*
>
> *Mr K has confirmed he knew that money would leave his account temporarily as part of this scam. He understood that, due to the steps he was taking and the information he was sharing in this call, his account balance would go to zero. I accept this was due to being misled by the identity of the scammer, but the fact he knew that through*

his interaction, the caller would be able to move his funds and that money would be leaving his account is enough to say, under the PSRs, that these payments were authorised by him. But I've thought about what other responsibility Revolut still holds.

In Phillip, 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 K 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 January 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- *using algorithms to identify transactions presenting an increased risk of fraud;*[1]
- *requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;*
- *using the confirmation of payee system for authorised push payments;*
- *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 January 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*

[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.

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).*
- *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 January 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

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

requirements that were in place in January 2023, Revolut should in any event have taken these steps.

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

I think Revolut should have identified that payments 1 and 2 were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), but considering the payment value, I don't think Revolut should reasonably have suspected that they might be part of a scam. The amounts sent weren't out of character with other spending on Mr K's account and not all payments to cryptocurrency providers are scams. So I don't consider they indicated Mr K was at risk of financial harm.

However, payment 3 was also going to the same cryptocurrency provider; and was the third payment to this merchant and meant Mr K had attempted to send £4,400 out of his account for purchasing cryptocurrency in one minute.

Given what Revolut knew about the destination of the payment and the amount and frequency of payments, I think that the circumstances at this point should have led Revolut to consider that Mr K was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this 3rd payment went ahead.

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 the third payment was attempted, knowing that the payment was going to a cryptocurrency provider, to have provided an automated warning that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. I accept Mr K wasn't falling victim to this kind of scam, but the information Revolut had should've indicated he might've been.

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 K by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

I note that in some situations Revolut wouldn't provide an automated warning but instead would ask the consumer the purpose of their payment from a drop-down list. If it had done this, it should have assessed the purpose Mr K selected against the known destination of the funds. Mr K wouldn't have selected cryptocurrency as he believed his money was going to be moved to Safe Account. But considering the situation, I think it's likely the purpose would have been concerning and/or contradicted known information, so Revolut then ought to have spoken to Mr K, as this should've indicated he may be at risk of financial harm.

If Revolut had provided a cryptocurrency investment scam warning, or spoken to Mr K in its in-app chat, would that have prevented the losses he suffered from the £1,800 payment onwards?

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.

Mr K was falling victim to an impersonation scam. And we're aware that it was seeing payments leave his account and go to cryptocurrency merchant that uncovered the scam and prompted his contact with Revolut. He recognised the cryptocurrency merchant name and realised he'd been scammed. So had Revolut stopped this payment and required Mr K to go into his app at that time, I'm satisfied the scam would've unravelled. Had it shown him the attempted payment information, I'm persuaded he would have taken steps to alert Revolut to the scam and protect his account. I note he did move his funds to his partner's account to prevent further payments once he saw the cryptocurrency transactions. And I'm satisfied if Revolut had blocked his card, he wouldn't have unblocked it.

In this case, I'm satisfied that by presenting Mr K with the attempted payment information this scam would've been unravelled. So had Revolut shown Mr K this and asked him for the payment purpose, regardless of the purpose he selected he wouldn't have wanted to make the payment and would have been able to tell Revolut he'd been scammed – whether this was by in-app chat if the payment purpose automatically directed him there. Or he'd have taken steps to immediately protect his remaining funds and speak to an agent in the app after seeing the warning. So I'm satisfied that an intervention by Revolut would've prevented the third and fourth payments in this case.

Should Mr K 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'm in agreement with our investigator that it would be fair to share liability in this case.

I accept this was a sophisticated scam and Mr K was tricked into sharing his details with the scammer. However, I am satisfied the text message he received to set up ApplePay on the scammer's device was clearly worded and should've concerned him, considering the situation he was in. It indicated that he shouldn't share the code with anyone, even if they claimed to be Revolut. And it told him his card would be added to another device. In this case, I haven't seen anything which would persuade me it reasonable for Mr K to have acted against the information that the message set out

This is also because the scammer needed Mr K's full card information to set up ApplePay, which Mr K has said he believed he shared by accident. This information must've been shared prior to Mr K getting that text, so I think the warning in it should've been more concerning to him considering he'd already shared this information.

If Mr K had headed the warning in the text and not shared the code, ApplePay couldn't have been set up. We can't know what else the scammer would've tried, but they wouldn't have been able to make payments in the way they did. And Mr K could've then contacted Revolut to discuss the call and with Revolut's support, taken steps to protect his account.

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

I can see that Revolut did explain to Mr K he should wait for the payments to be processed and then put in a chargeback claim. I understand they were still showing as "pending" when Mr K reported the scam. But then it didn't pursue the chargeback claim for him, which caused him frustration.

I'm satisfied that Revolut couldn't stop the payments after they had been made. I accept they didn't show as completed when he contacted Revolut, but the remaining steps to complete the payment were to be done at the merchant's end, not Revolut's. It couldn't do anything to stop the payments at this point, as it had already processed them. So I don't think it did anything wrong here, as it couldn't cancel the payments, for example.

In relation to chargeback, I'm mindful that the payments made have gone to a genuine seller of cryptocurrency that wasn't involved in the scam. So Revolut is very unlikely to have been able to recover the funds, as the merchant would've supplied the cryptocurrency paid for, just not to Mr K. And the chargeback process wasn't designed for scams.

I appreciate Mr K's frustration as Revolut suggested the chargeback process and then wouldn't take his claim forward. But chargeback is generally the correct avenue to recover payments made on card, so this wasn't incorrect advice. The advisor wouldn't have assessed the validity of Mr K's claim at this time, just set out the process to follow so the correct department could then do this. So I don't find that Revolut has done something wrong here.

Revolut didn't respond to the provisional decision. Mr K explained that it was difficult to establish what was genuinely Revolut and what was the scammer in the texts he received. He was unhappy Revolut allowed payments to the cryptocurrency merchant and had hoped we'd ask Revolut to at least give him half his money back as it was a multi-million-pound corporation. The case has now been returned to me for review.

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.

I've reviewed the further comments submitted. I accept that the scammer was able to input text messages into Mr K's genuine chat with Revolut. But considering the overall context of the scam here; including the content of the genuine messages and how clear they were around what the code was for, I'm still persuaded Mr K should be held equally liable for the payments after Revolut should've intervened.

I accept that it could've initially seemed as if Mr K was speaking to Revolut, but then there was no reason for it to request he set up ApplePay on someone else's device. The genuine text message from Revolut effectively told him it wouldn't be Revolut if he was asked to share the code and this text message also didn't fit with the situation he understood was happening. So while I appreciate his confusion, it doesn't change my decision.

It's also not for our service to dictate how Revolut operates or who is allows its customers to send money to, we aren't the regulator or involved in how a firm operates. So while I appreciate for a period of time it didn't allow the cryptocurrency exchange used in this scam, that wasn't the case when Mr K approved the payments. And as an impartial service, it wouldn't be appropriate for our service to direct a business to refund a customer only because the complainant is a person and the respondent is a more wealthy business. So neither of these points change my outcome on this case.

While I have considered Mr K's further evidence, I see no reason to depart from my provisional findings. I consider Revolut should've intervened on payment 3 and this would've unravelled the scam, preventing this payment and payment 4. I accept Mr K has been the victim of a cruel scam, but for the reasons already outlined in my provisional decision, I still consider it appropriate to reduce the refund for his contributory negligence.

Putting things right

Revolut Ltd should refund payments 3 and 4, but reduce this figure by 50% for Mr K's contributory negligence. It should also pay 8% simple interest per year on that amount from the date of each transaction to the date of settlement.

My final decision

For the reasons set out above, I partially uphold Mr K's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 30 December 2024.

Amy Osborne
Ombudsman