DRN-5108848

The complaint

Ms M is unhappy that Revolut Ltd won't reimburse money she lost to a scam.

The complaint is brought on Ms M's behalf by a professional representative.

What happened

The background to this complaint is well known to both parties, so I won't repeat everything here. In summary, Ms M has explained that in November 2023 she made several payments from her Revolut account to buy cryptocurrency which she ultimately lost to an investment scam.

Payment number	Date	Type of Transaction	Amount
1	6 November 2023	Debit card payment to cryptocurrency account at C	£2,950
2	9 November 2023	Debit card payment to cryptocurrency account at C	£4,970
3	14 November 2023	Debit card payment to cryptocurrency account at C	£4,469.77
		Total	**12,389.77**

Ms M has said she saw an advert on social media promoting a cryptocurrency investment with a company I will refer to as "S". She said she looked through reviews on S and found that they were positive. She has also explained she was impressed by S's website and platform. She made contact with S, and believing it was a legitimate investment she paid an initial fee of £200 from an external account to start investing. She also told us she opened an account on its platform.

Ms M said the scammer told her to use her Revolut account to send payments. The payments Ms M made from Revolut went to a legitimate cryptocurrency firm – "C". From C, Ms M's funds were converted into cryptocurrency and sent to cryptocurrency wallets controlled by the scammers.

Ms M has said after making a few payments the scammer urged her to increase her investments pushing her to take out a loan. When Ms M refused the scammer became aggressive. Shortly after this point she realised she had been scammed. Ms M reported she had been scammed to Revolut.

Ms M raised a complaint with Revolut. Revolut investigated the complaint but didn't uphold it. It didn't think it had done anything wrong by allowing the payments to go through. So, Ms M brought her complaint to our service.

One of our Investigators looked into the complaint and upheld it in part. He thought that Revolut should have identified that the second payment was concerning and should have questioned Ms M about it before it debited her account. If Revolut had done this, the

Investigator thought that the scam would have come to light and Ms M's further losses would have been prevented.

Our Investigator however thought that Ms M ought to take some responsibility for her loss too. He didn't think there were many positive reviews on S, which Ms M should have thought about before sending the payments. The Investigator also thought the profits were too good to be true and that Ms M should have realised something was wrong from the pressure the scammer was applying for her to invest more and more. The Investigator thought that a fair deduction to the amount reimbursed would be 50%.

Ms M accepted the refund recommended by our Investigator. Revolut didn't agree. I've summarised its main points:

- The Payment Service Regulator's ("PSR") mandatory reimbursement scheme will not require it to refund 'self to self' transactions.
- 'Self-to-self' payments don't meet either the Dispute Resolution Rules ("DISP Rules") or the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) definition of an Authorised Push Payment (APP) scam.
- As an Electronic Money Institution (EMI) rather than a bank its accounts are typically set up to facilitate payments for a specific purpose rather than a main account and so the transactions weren't unexpected or unusual for how its customers use their accounts.
- Ms M's loss did not take place from her Revolut account as she made payments to her own account at another regulated EMI before converting her money into cryptocurrency and transferring that cryptocurrency to the fraudster. It's unfair and irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions.
- It is relevant to consider the actions of other firms involved in the chain as the source of the funds lost to this scam originated from a firm other than Revolut.
- It may be relevant for this service to exercise its power to inform Ms M that it may be appropriate to make a complaint against another firm involved.

As no agreement could be reached, the case was 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.

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.

In broad terms, the starting position at law is that an 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 Ms M 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*".

In this respect, section 19 of the terms and conditions said:

> *"**19. When we will refuse or delay a payment***
> *We may refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
> - *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 Ms M and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in November 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And, I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and

depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp*.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst its terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, it could only decline ('refuse') the payment.

But 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 November 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 do 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 from October 2023, Revolut operated a process whereby if it identified a scam risk associated with a card payment through its automated systems, it might initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat). If Revolut was satisfied with the response to those questions and/or it provided a relevant warning, the consumer could use the card again to instruct the same payment and Revolut would then make the payment.

I am also mindful that:

- EMIs 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] 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_/

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 Code[2], 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).
- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[4].*
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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.

---

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

[3] Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

- 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 November 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in November 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Ms M has fallen victim to a cruel scam here. Ms M has also authorised the disputed payments she made to a cryptocurrency wallet (where her funds were subsequently transferred to the scammer). But I've thought about whether Revolut should have reasonably intervened and if so, what impact this intervention would have had.

Whilst I have set out in this decision the circumstances which led Ms M to make the payments using her Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Ms M might be the victim of a scam.

I'm aware that cryptocurrency exchanges like C 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 the payments would be credited to a cryptocurrency wallet held in Ms M's name.

By November 2023, when these transactions started, 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[6]. And by November 2023, when these payments took place, further restrictions were in place[7].

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 the vast 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.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Ms M made in November 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. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Ms M's own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Ms M might be at a heightened risk of fraud.

Should Revolut have identified that Ms M might be at a heightened risk of fraud?

While Revolut should have identified the payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), Payment 1 was low in value. So, I don't think there would have been enough reason for Revolut to suspect that it might have

---

[6] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.
NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.
[7] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

been made in relation to a scam. I also need to take into account that Revolut needs to strike a balance between protecting customers against fraud and not unduly hindering legitimate transactions, so I don't think Revolut ought to have been so concerned about this payment that it ought to have provided specific warnings to Ms M at this point.

However, Payment 2 was significantly higher than the previous payment. Ms M had only used the account for fairly low value transactions up until November 2023, and in my view, this payment was a clear escalation in value and had the potential to cause significant financial harm to Ms M. Taken together with the earlier payment, I consider Revolut ought reasonably to have identified that a pattern had developed that could indicate Ms M was at risk of financial harm from fraud.

So, when Ms M attempted to make Payment 2, taking into account what I've said about the increased risk that cryptocurrency transactions presented, I think Revolut ought fairly and reasonably to have recognised the risk had increased and there was a heightened possibility that the transaction was linked to a cryptocurrency scam. In line with the good industry practice that I've set out above, I think Revolut should have provided a specific and impactful warning, before allowing this payment to go ahead.

Revolut haven't given us any information to suggest a warning was provided at the time, so I'm satisfied a warning wasn't shown to Ms M. To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (and the one which came before it) that, together with the fact the payment went to a cryptocurrency provider, that ought to have given Revolut sufficient cause for concern that Ms M could be at risk of suffering financial harm from fraud when she attempted to make Payment 2. In those circumstances, it should fairly and reasonably have taken additional, proportionate, steps before completing the payment.

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 primary duty to make payments promptly.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by November 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. As I explained earlier in this decision, I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to decline payment instructions in order to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment if they decided to proceed with the payment by instructing it again after reading the warning.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by November 2023, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, Revolut knew that Payment 2 was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. Revolut should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I am satisfied that, by November 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Ms M made Payment 2, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Ms S was at risk from.

In this case, Ms M was falling victim to a cryptocurrency investment scam – she believed she was making trades which would generate profits. As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Ms M gave. I'd expect any such warning to have covered off key features of such a scam, such as referring to: an advertisement on social media, an 'account manager', 'broker' or 'trader' acting on their behalf, pressure tactics being used to encourage investments, the use of remote access software, a small initial deposit which quickly increases in value and having to pay increasingly large sums without being able to withdraw money. I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Ms M wouldn't have done so here.

Revolut states that, as a matter of fact, it cannot delay a card payment – it can either decline or accept the payment. As I've set out, I accept that under the relevant card scheme rules it cannot delay a card payment, but in the circumstances of this case, I think Revolut ought to have initially declined Payment 2 to make further enquiries with a view to providing a specific scam warning, of the type I've described. Only after that scam warning had been given, if Ms M renewed the payment, should it have been made.

And as I've set out above (and as Revolut has not disputed) it did have systems in place by November 2023 to decline card payments and provide warnings of a similar nature to the type I've described. So, it could give such a warning and, as a matter of fact, was providing such warnings at the relevant time.

If Revolut had provided a warning of the type described, would that have prevented the losses Ms M suffered from Payment 2?

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, such as finding the investment through a social media platform, being assisted by a broker and being asked to download

remote access software so S could help her transfer funds to its platform. She was initially asked to set up the account with a small payment and convinced to invest more after early success on her investment. The scammer described the profits as guaranteed, which is typical in these types of scams.

From the messages it's clear that the scammer was pressuring her into investing large sums of money which she didn't want to do. Ms M explained in her chats with the scammer that she wasn't confident in dealing with cryptocurrency so wanted to start with smaller amounts. This confirms she already had some concerns with the investment. Overall, on the balance of probabilities had Revolut provided Ms M 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. So, I'm satisfied that a timely warning to Ms M from Revolut would have very likely caused her to have sufficient doubt to not go ahead with Payment 2 and the subsequent payment that followed.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Ms M purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

Revolut's primary argument is that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

I have taken into account that the payments were made to another financial business (a cryptocurrency exchange based) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out in some detail I think that Revolut still should have recognised that Ms M might have been at risk of financial harm from fraud when she made Payment 2 and, in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Ms M 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 C does not alter that fact and I think Revolut can fairly be held responsible for Ms M's loss in such circumstances.

In the alternative, Revolut argues that if we conclude it can be held responsible for a customer's loss in circumstances where it is only an intermediate link in a chain of transactions, then it is irrational to only consider its role in what happened. Instead consideration must be given to the other parties involved in the multi-stage fraud to determine overall responsibility for the loss suffered by Ms M.

I have considered those representations carefully, but I am not persuaded by them.

Ms M has only complained against Revolut. It's possible, but by no means certain (for example because the other firm – unlike Revolut – would not have known the payment was being made to a cryptocurrency firm) that the other firm might also have missed the

opportunity to intervene or failed to act fairly and reasonably in some other way, and Ms M could instead, or in addition, have sort to complain against it. But she has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only consider the extent to which Revolut itself can fairly be held responsible for her losses. As I have explained I am satisfied it can, and in those circumstances, I think it's fair to require it to compensate Ms M for the losses it could have prevented by taking reasonable steps.

Whilst it is open to me to inform the complainant it might be appropriate to complain against another respondent, I do not consider it necessary or appropriate for me to do that in this case since Revolut is an appropriate respondent from whom Ms M can seek compensation; Ms M is aware that she could also have attempted to complain against her own bank; Revolut could itself have informed Ms M that another firm might also be responsible and why when she first complained (see DISP 1.7.1R); and C is not a potential respondent to a complaint.

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 M's loss from Payment 2 (subject to a deduction for Ms M's own contribution which I will consider below). As I have explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice and as a step to comply with its regulatory requirements, I consider Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

Revolut has argued that the CRM Code does not apply to Ms M's payments. I do not seek to treat Revolut as if it were a signatory to the CRM Code. I've explained in some detail why I think it fair and reasonable that Revolut ought to have identified that Ms M may have been at risk of financial harm from fraud and the steps it should have taken before allowing the final payment to leave Ms M's account.

I'm also aware that the Payment Service Regulator's ("PSR") proposed mandatory reimbursement scheme would not require Revolut to reimburse Ms M.

However, the PSR's proposals are not relevant to my decision about what is fair and reasonable in this complaint and, in any event, will not apply to card payments. I do not consider the fact that the PSR does not propose to make it compulsory for payment service providers to reimburse consumers who transfer money to accounts held in their own name or who convert their funds into cryptocurrency before transferring that cryptocurrency to a fraudster, as part of a multi-stage fraud, means that Revolut should not compensate Ms M in circumstances when it failed to act fairly and reasonably, as I have found was the case here.

Indeed, the PSR has recently reminded firms that fraud victims have a right to make complaints and refer them to the Financial Ombudsman Service that exists separately from the intended reimbursement rights and that APP scam victims will still be able to bring complaints where they believe that the conduct of a firm has caused their loss (in addition to any claim under the reimbursement rules)[8].

[8] "The reimbursement rules and their award limit differ from the rules which govern complaints under the Financial Ombudsman Service's dispute resolution rules (DISP). PSPs should therefore inform victims of APP scams that, in addition to their right to seek reimbursement under the reimbursement rules, they have the right to bring complaints against sending and receiving PSPs if they are dissatisfied with their conduct and consider this has caused their loss. Such complaints may ultimately be referred to the Financial Ombudsman Service." PSR PS23/4 7.18

I do not consider it to be relevant that the circumstances here do not fall under the specific definition of an APP scam set out in the CRM Code and DISP rules. Those definitions define the scope of the CRM Code and eligibility of payers to complain about a payee's payment service provider respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made Payment 2 without providing a warning to Ms M.

Overall, considering what is fair and reasonable in all the circumstances, I'm satisfied Revolut should have made further enquiries and provided a tailored scam warning before processing the Payment 2. If it had, it is more likely than not that the scam would have been exposed, and Ms M would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Ms M's loss.

Should Ms M bear any responsibility for her losses?

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

I recognise that, as a layperson, there were aspects to the scam that would have appeared convincing. Ms M was impressed by the website, she was asked to provide identification documents and the scammer, who she describes as extremely professional, was knowledgeable and built a rapport with her.

I've also taken into account the provision of the trading platform (which, I understand, would have used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that fraudsters used the apparent success of early trades to encourage increasingly large deposits and that they built a rapport with her during phone calls. So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Ms M to be reduced. I think it should be.

Ms M was told her initial investment of £200 had increased to £700 in a very short period of time. These returns were too good to be true and such a high return should have led her to have some concerns about the legitimacy of the scheme. Ms M has described the scammer showing her reasonable and believable profits being made on her money, but such returns should have put Ms M on notice that something might not have been right, and she should have made further enquiries, certainly before making Payment 2.

Ms M was being asked to invest increasing amounts over a short period of time. She was having multiple calls with the scammer and her messages with him suggest she was being pressured to invest more and more. This is not something you would expect from a professional company and should have put Ms M on notice that the company may not be genuine. Ms M should also have been concerned when the scammer advised she should download a screen sharing app and exchange her personal details with him. Despite not being confident in investing she should have been concerned with the level of information she was being asked to share with the scammer.

For the avoidance of doubt, it is not my finding that Ms M knew that she was likely falling victim to a scam and went ahead anyway. Rather my finding is that she seems – to some extent – to have had concerns about making further payments. In those circumstances it would not be fair to require Revolut to compensate her for the full amount of her losses.

Taking all of the above into account I think that Revolut can fairly reduce the amount it pays to Ms M because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Ms M has also requested compensation in addition to a refund of the scam payments made. But I can't see any reason which would suggest compensation is warranted in the circumstances of the complaint as I have not found anything to suggest Revolut have acted incorrectly in addition to what I have described above.

Could Revolut have done anything else to recover Ms M's money?

There are industry standards around attempting recovery of funds where a scam is reported. So, I've also thought about whether Revolut could have done more to recover the funds after Ms M reported the fraud.

It's possible to dispute a debit card payment through a process called chargeback, which can sometimes be attempted if something has gone wrong with a debit card purchase, subject to the relevant card scheme's rules. Revolut didn't proceed with Ms M's chargeback, but I don't think it would have had a reasonable chance of being successful, even if it had been attempted. This is because Ms M received the service she'd paid for in purchasing cryptocurrency.

So, I don't think there was anything more Revolut could have done to recover Ms M's money in these circumstances.

Interest

Ms M has been deprived of the use of her funds on Payment 2 and 3. So, Revolut should pay 8% simple interest yearly to the 50% refund on those transactions (calculated from the date of the transactions until the date of settlement). She may have used these funds in a variety of different ways if they had remained available to her. I think 8% simple is a fair interest rate in these circumstances.

My final decision

For the reasons given above, I uphold in part this complaint and require Revolut Ltd to pay Ms M:

- 50% of Payments 2 and 3 – a total of £4,719.89
- 8% simple interest per year on that amount from the date of each payment to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms M to accept or reject my decision before 1 July 2025.

Aleya Khanom
Ombudsman