

Complaint

Mr P is unhappy that Revolut Ltd didn't reimburse him after he fell victim to an investment scam.

Background

In early 2022, Mr P fell victim to an investment scam. His wife and daughter had passed away and so he'd sold a property. As a result of the sale, he had a significant balance in his current account which he was looking to invest. He looked online and found a website advertising the services of a broker. He registered his interest and, shortly afterwards, was contacted by someone who claimed to be a representative of that firm. He was told that they would help him with managing his money. The investment strategy would be focused on using Contracts for Difference (CFDs) to speculate on movements of publicly listed equities. Unfortunately, that person wasn't the employee of a genuine investment firm but a scammer.

Mr P was persuaded to download remote access software to his computer so that the scammer could help him set up his trading account and, later, his account with Revolut that would be used to make transfers into it. His money was in an account with a bank I'll refer to as Bank A. Initially, Mr P attempted to make payments from his account with Bank A directly to the scammer. He first attempted to do so on 24 March 2022. Those attempts were stopped by Bank A and Mr P had to have several calls with agents of the bank who wanted to question the payment activity with him. I've transcribed a small section of two of those conversations that are relevant to the outcome here.

On 25 March, he had a conversation with an employee of Bank A that went as follows:

C: Which one are you on about? The £10,000 one?

B: The transaction we are concerned about is for £10,000 and it is going to ... Stablecoin ... something?

C: That went out this morning and that's fine.

B: May I please know the purpose of the payment, if you don't mind?

C: The purpose of the payment was for investments.

B: Ok, no problem with that – may I please know, have you invested with them before or is this the first time?

C: This is the first time.

B: Ok, no problem. And may I know, how did you receive the account details from them?

C: Talking to them.

B: Over the phone, you're saying?

C: Over the phone, yes.

B: And may I please know how did you get to know about Stablecoin? Was it through advertisement or research?

C: Advertisement.

B: Ok, no problem ... and ... did you consider making a smaller transfer first before making this £10,000 payment?

C: I did. I tried transferring £500 and yesterday I tried to do a transfer of £5,000 and, to be perfectly honest with you, I was absolutely disgusted with the amount of time and effort it took trying to get it through. I was talking to people. I couldn't understand them, I couldn't hear them. I probably lost money overnight because I was unable to purchase. Now, the £5,000 has been taken out of my account. It's not gone to theirs. It's in the cloud somewhere and it needs to go back to my account now, they won't be claiming it.

B: Ok, the £5,000 from your [Bank A] account, you're saying?

C: Yes ... It never went. It went out of my account and it was in limbo. It never went to them.

B: Ok, did you check with them for any specific reason they had not received it, because ...

C: Because the bank refused! Because the bank refused!

B: Ok ... and just to be sure, did you receive any kind of text message or any emails that you thought was from [Bank A] or any other third party?

C: Sorry?

B: Just to be sure, did you receive any text message or any emails recently that you thought was from [Bank A] or any other third party?

C: No.

B: Ok, just for future reference, please never click on any suspicious links that you receive, even if you feel that you have received any text message or any emails from [Bank A]. I would request that you validate this directly using your registered mobile application or internet banking. But never click on any links to validate any message from anywhere.

C: Right.

B: And just to be sure, did you receive any third-party phone calls recently, like Amazon, BT, HMRC ... asking you to transfer any funds.

C: No.

B: I would just request that you never believe on any of those phone calls as well because they're definitely fraudulent phone calls. And I would also request that you

never believe on any phone calls you receive from any of the banks claiming that your account has been compromised and you have to transfer all your funds to any other account or something like that. Because no bank will ever ask you to do that.

C: ... Right.

B: And may I please know, has anyone told you how to answer our questions or asked you to mislead us in any way for the purpose of this payment?

C: No, no.

B: Ok, so you never believe on anyone asking you do that either because nowadays there are a lot of fraud and scam scenarios and we are receiving cases where our customers informed that they have received a few phone calls from police and they had asked them to transfer funds otherwise there would be an arrest warrant or any kind of a charge against them ...

C: I don't understand what all of this is about! All I want to do is purchase some shares from a company from my account which I've got money in, and I have had nothing but trouble doing this. What is the problem? If I want to transfer it from my bank account across to somewhere else, what is the problem?

B: There is no problem because there are a lot of fraud and scam scenarios regarding these investments nowadays We want you to be 200% sure before making any payment anywhere.

C: Well, I'm sure. I'm an adult. I'm perfectly sure. You stopped me being able to do a transfer last night and I've had to go around to a different way of paying it to get it through. Now that should not happen with my bank account. I have money in my account, and I should be able to do what I want with it.

B: I am concerned that this might be an investment scam so you should check where you are sending the money, I would say by having double checked everything with them once again because it's the first time ...

C: Ok, thank you...

[call ends]

That £10,000 payment wasn't processed by Bank A. It had been encouraging Mr P to carry out further checks and, in his frustration, Mr P appears to have ended the call. A further conversation took place the following day:

B: I can see here that you have tried making a payment from this account for £10,000

C: Also, there was a payment before that of £5,000 and one of £500 all to the same company. I believe you stopped all of them.

B: To who are you trying to pay this amount?

C: It's to a company that's dealing with shares for me [name of broker].

B: But I see a different name over here? I can see that you've made a payment to Stable Coin.

C: That's right.

B: Who is this person to whom you're trying to pay this £10,000?

C: It's supposed to be through to the company of [broker] through a Lucas.

B: [...] But I can see a different name over here, as I mentioned ... Stable Coin? Now, what is that?

C: This whole thing started two days ago. I was trying to buy some shares and your bank has stopped my money going through. There's £5,000 in a cloud somewhere and then you stopped £10,000 thinking that it was fraud. Well, I'm not sure about it now. I just want it stopped, back into my account and no more money to go out to these people.

B: Ok, no problem – but Stable Coin is what? Is this an investing company? What exactly is it?

C: I don't know, I'm totally lost in this now. It was supposed to be buying Tesla shares.

B: Ok, did someone approach you about this? How did you get to know about this?

C: I went on the internet to look up for cryptocurrency ... [the broker] came up and when I was looking at the information, someone phoned me up.

B: Ok, are you sure it's a legitimate company where you are transferring...?

C: I'm not sure of anything anymore, I just ... I want it stopped, the money returned back if it's possible, so they can't take anything else from me again.

I understand that after this call, Mr P spoke to a member of his family who he trusted. That family member told him that the bank had been overzealous and that he shouldn't be concerned. On the advice of the scammer, he opened an account with Revolut and attempted to make a payment to it from his account at Bank A. This was questioned again by the Bank and Mr P told it that he was transferring money to his Revolut account to purchase shares.

He made payments from that account to his Revolut account. He then transferred on his funds from that account and, ultimately, via a crypto-platform to an account controlled by the fraudster. The payments Mr P made took the form of either card payments to Payee A or Faster Payments to Payee B (an FCA-authorised firm which, at the time, processed payments on behalf of Payee A). Those payments were used to purchase cryptocurrency from Payee B, which credited Mr P's own cryptocurrency wallet. From his cryptocurrency account at Payee B, Mr P sent cryptocurrency to the fraudsters.

In total, he transferred just under £270,000 between 5 April and 4 May 2022. The initial payments were made in the belief that he was putting his money under the control of someone who would invest it on his behalf and generate returns. The scammers then fabricated justifications for further payments, citing fees and taxes. At the end of the period of the scam, Mr P says he was told that he couldn't get access to his profits without paying a fee equivalent to 10% of the balance on his trading account. When he said that he didn't have access to that kind of money, the fraudsters recommended he take out a loan and lie to the bank about his reasons for doing so. It was at that point that he realised he must have fallen victim to a scam.

He made the following payments from his Revolut account:

Payment	Date	Payee	Value of payment
1	04 April 2022	A	£3,000
2	05 April 2022	A	£7,000
3	11 April 2022	B	£15,000
4	15 April 2022	B	£20,000
5	19 April 2022	B	£25,000
6	20 April 2022	B	£10,000
7	21 April 2022	B	£25,000
8	22 April 2022	B	£25,000
9	26 April 2022	B	£25,000
10	27 April 2022	B	£25,000
11	28 April 2022	B	£21,000
12	29 April 2022	B	£25,000
13	03 May 2022	B	£25,000
14	04 May 2022	B	£20,000

Revolut had concerns about payment 3. It told us that it temporarily paused that payment and showed Mr P the following warning:

Suspicious transfer detected

Our system has flagged this payment as a potential scam, are you sure you want to proceed? Please note, if you proceed with authorising the payment we may not be able to recover your money afterwards.

Mr P agreed to proceed and so was asked to specify the purpose of the payment. The header at the top of the screen would've said *"Beware, this payment might be a scam."* One of the listed options was Investment and, according to Revolut, *"after choosing the purpose of the transfer, the Customer was asked whether they are pressured to make these payments and were they called unexpectedly? And the Customer was offered either to continue talking with Revolut support or cancel the transfer in question or confirm it."*

After the payment was authorised, Revolut says Mr P would've seen the following message:

Transfer accepted. You've successfully authorised a payment which was flagged by our system as a potential scam.

Although it didn't mention it in its original submissions, Revolut later added that Mr P would've seen the following warning during this payment process:

1. *You should try to verify that this is a genuine investment company/opportunity*
2. *Scammers will typically promise significantly higher than market returns to attract you to the opportunity.*
3. *Only purchase cryptocurrencies from reputable companies.*
4. *Scammers often cold call or message with the promise of a great investment opportunity.*
5. *Revolut and other trustworthy organizations will NEVER tell you to ignore this warning.*

On 24 April 2022, Revolut queried the source of the funds Mr P was putting through his account. It asked him to provide evidence to show where the money had come from. As far as I can see, Mr P didn't respond to that request. However, on 5 May 2022, he replied on the app and said: *"I have been scammed for approx. 290000 through this account and need help as to where it has gone and if I can get it back."*

The Revolut agent replied to say that they'd open a new chat with a team that could help him with his fraud claim and asked him again to complete its source of funds verification process. On 12 May, Mr P responded to this agent and provided a brief description of the scam. He also said: *"Can you please help me in any way I am desperate and feel suicidal. I have just lost my wife and daughter and have used the money from the sale of the house to try and invest only to be totally scammed and wiped out by these people."*

The Revolut agent again said it would open a new chat with the fraud team but then reiterated that it would need Mr P to go through verification and answer its questions regarding the source of funds. Mr P said he would respond by email. Revolut then messaged him again and said that, as he'd mentioned investing in shares, could he please provide more evidence of that investment – for example, a statement from the investment manager, an investment certificate and so on.

Eventually, Mr P complained to both Revolut and Bank A that neither had done enough to protect him from fraud. His complaint about Bank A is being dealt with under separate cover. Revolut didn't agree to uphold his complaint and reimburse him. It said that it had done everything in its power to protect him and to attempt to recover his funds. It said it warned him about fraud risk. It temporarily stopped the third payment and asked Mr P what the purpose of the payment was. He selected *'investment'* and so he saw a warning that was tailored to the risks posed by investment scams.

Mr P was unhappy with that and so he referred his complaint to this service. It was looked at by an Investigator who upheld it in part. The Investigator said that Revolut needed to have systems in place to spot out of character or unusual payments that might have indicated Mr P was at risk of fraud. The Investigator concluded that the third payment in the table above was the point at which those concerns should've resulted in action on Revolut's part. He noted that it had displayed a warning to Mr P, but he didn't think it was a particularly helpful intervention in the circumstances. He considered that it should've made enquiries with Mr P before allowing the payment to be processed.

He also considered whether Mr P should bear any responsibility for his own losses but was persuaded that it wouldn't be fair and reasonable for him to do so. He recommended Revolut refund 100% of Mr P's losses from the third payment onwards.

Revolut disagreed with the Investigator's view. It made the following arguments:

- The warning was sufficiently detailed and should've been enough to prevent Mr P from going ahead with the payments.
- Mr P was making payments to his own account. It could reasonably consider those payments to be lower risk because they were going to an account in his own name.
- Mr P was making the payment to another FCA regulated business and so Revolut could reasonably have understood the risk to be lower.
- The fact that Mr P was making payments to his own account means that this incident doesn't fit the criteria for an authorised push payment (APP) scam under the DISP rules. That definition specifically requires the customer to have transferred money to someone other than themselves.
- The Investigator had mentioned the circumstances that made Mr P vulnerable, but Revolut wouldn't have had any way of knowing about his wider circumstances at the time. It's therefore unreasonable for that to be a consideration when reaching an outcome on the case.
- Mr P should've carried out more research before parting with his money, particularly when his investment appeared to be earning disproportionately good returns. He was contributorily negligent and so a deduction should be made from any award payable.

As Revolut disagreed with the Investigator's view, the complaint was passed to me to consider and come to a final decision.

I issued a provisional decision on 23 August 2024. I wrote:

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 Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- *The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.*

- *At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its customer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.*

In this case, the terms of Revolut's contract with Mr P 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 Mr P and the Payment Services Regulations to carry out their 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 authorised push payments immediately¹. Revolut could comply with the requirement to carry out these 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 2022 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;*
- *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),*

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/

“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 Code⁴, 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.*

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 2022 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*

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”

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 Mr P was at risk of financial harm from fraud?

It isn't in dispute that Mr P has fallen victim to a cruel scam here, nor that he authorised the disputed payments he made to his cryptocurrency wallets (from which his funds were subsequently transferred to the scammer). Whilst I have set out in detail in this provisional decision the circumstances which led Mr P to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr P might be the victim of fraud.

Revolut has argued that it could take comfort from the fact that the destination of these payments was an account in Mr P's own name. It's not clear to me that Revolut would have known for certain that the immediate destination of Mr P's funds was his own account – there was no positive 'Confirmation of Payee' check, for example. Nevertheless, I'm aware that cryptocurrency exchanges like the payee here 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 have likely been aware of this fact, so I accept that, as it claims, it could have reasonably assumed that all of the payments in question were to accounts in Mr P's name.

I also accept that, in general, a firm can treat payments made between accounts under a customer's control as carrying a lower fraud risk. That's particularly true where a payee is well-known and long-standing, but remains true, to a lesser extent, where the payee is new or recently created, particularly if the firm can independently verify the holder of the destination account (for example, through the Confirmation of Payee scheme) or the customer has indicated that they are paying their own account. As noted, there wasn't a Confirmation of Payee match here and Mr P didn't indicate that the payments were going to his own account. So, I think any reassurance that Revolut could have taken from its knowledge of the recipient account was already fairly limited.

In addition, it knew that the destination of the payments was a cryptocurrency provider. By the time he fell victim to this scam, firms like Revolut ought to have been aware of the risk of multi-stage scams involving cryptocurrency. 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 have continued to increase since.

So, Revolut ought fairly and reasonably to have recognised that its customers could still be at risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the customer's own name. In those circumstances, as a matter of what I consider to

have been fair and reasonable and good industry practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

I've also taken into account that Mr P opened this account specifically to make payments relating to this scam. He told Revolut at that point that the purpose of setting up the account was to "make transfers." That made Revolut's job here more difficult. It lacked a detailed payment history to serve as a basis of comparison when deciding if these payments were unusual or out of character.

The first two payments he made in connection with the scam were for £3,000 and £7,000 respectively and these payments were made by card. However, the following week, he made a payment for £15,000 to a cryptocurrency platform. He'd already transferred £10,000 to a different cryptocurrency firm the previous week. While I recognise that Mr P had specifically stated that he'd opened the account to make transfers, I think Revolut should have identified a concerning pattern of escalating payment values. It should've gone further than the written warning it provided.

Even without detailed data regarding a customer's historic payment behaviour, a payment of £15,000 is large enough to be worthy of further scrutiny. I also think it ought to have been concerned at the significant increase in the value of the payments, something which is and was a known risk signifier with investment scams like this one. It was at that point that it should've been concerned about the risk Mr P might be about to fall victim to a scam. It shouldn't have processed that payment without first making further enquiries to satisfy itself that he wasn't at risk of financial harm due to fraud.

In my view, in line with good industry practice at the time, as well as what I consider to be fair and reasonable in the circumstances of this complaint, a proportionate intervention at the time of payment 3 would've been for an employee of the firm to contact Mr P to discuss the payment before deciding whether it should be processed.

What did Revolut do to warn Mr P?

As I explained above, I think Revolut ought to have done more to warn Mr P about the risks of fraud when he asked it to make the third payment. I recognise that it did attempt to do so by displaying a warning to him during the payment process. Its content was driven by information Mr P volunteered about the purpose of the payment. The details of its intervention are described in the background section of this decision.

The warning made it clear to Mr P that its systems had determined that there was a higher-than-normal fraud risk associated with that payment. Mr P could reasonably have been expected to be aware that there was a general background risk of fraud. He was later presented with a more detailed warning in the form of a list of five items. That list is set out above.

The first item in the list said that Mr P should try to verify that the opportunity is genuine. In isolation, and given the asymmetry of knowledge between the parties, this wasn't a particularly helpful piece of advice. Recommending that a layperson verify if an opportunity is legitimate without pointing to any of the checks that they could've conducted to do so wouldn't help to protect them from fraud risk.

Points 2 and 4 highlight things that might be features of investment scams, but they weren't relevant here and so wouldn't have had any impact on Mr P's decision

making. He hadn't been promised a better return than might be typically available to a retail investor. He'd also found the broker himself, rather than being cold called. Point 3 also wasn't a particularly helpful piece of advice to Mr P, since he was purchasing cryptocurrency from a reputable firm, albeit he was then being tricked into transferring it to the scammer. Unfortunately, the warning didn't point to the key features of cryptocurrency investment scams, such as the customer being helped by a 'broker' or 'trader' managing their funds on their behalf, the use of remote access software or the relatively small initial deposit which then ramped up in value.

I recognise that a warning of this nature would not be able to cover off every circumstance that a customer finds themselves in and I don't suggest that it was inadequate because the scam features it highlighted didn't entirely match Mr P's circumstances. Nonetheless, I'm not persuaded it adequately addressed the typical features of this scam type. Having said that, I'm not persuaded that a written warning without those shortcomings would've changed what Mr P did here. There were multiple parties involved at this point (i.e., the scammers themselves and Bank A). Bank A had made some unskilful attempts to protect Mr P from the fraud risk across multiple telephone conversations. Those conversations created in Mr P a frustration at the practical obstacles being placed in his way preventing him from transferring his money as he wished, but also an inclination to view such measures as bureaucratic and unnecessary. They also did very little to enlighten him as to why those conversations were taking place at all. That hamstrung any efforts of Revolut to provide him with an impactful written warning at that time. I think his experience up until that point meant it was unlikely that he would've meaningfully engaged with and reflected on the content of a warning displayed by Revolut.

What kind of warning should Revolut have provided?

In the circumstances, I think the proportionate response to the risk was to do more than display a written warning. In this instance, I think a human interaction needed to take place.

An employee of Revolut should've made contact with Mr P to discuss the circumstances surrounding the payment request. I'm satisfied that it's more likely than not that he would've been open and honest when responding to Revolut's queries. He wasn't told that he'd need to mislead the firm if it questioned the payments with him and the fact that he was willing to be candid with the employees of Bank A backs that up.

In the circumstances, I think an employee of the firm would've uncovered that the likelihood Mr P was at risk of fraud was very high. If it had asked Mr P appropriate questions about the investment, Revolut would've discovered that he was working with a 'broker' who claimed to be acting on his behalf and that he was making payments into his 'investment' using cryptocurrency. This was something he did say to Bank A when it spoke to him about the activity on his account. It could also have uncovered that he'd been given implausible reassurances about how his account would be protected from trading losses. The situation Mr P found himself in had all the hallmarks of a cryptocurrency investment scam. Revolut should've given him an unambiguous warning that it was highly likely he was in the process of falling victim to such a scam. It's significant from those calls with Bank A that Mr P clearly had a background level of uncertainty and was worried about fraud risk and so I don't think it would've taken much to dissuade him from going ahead with the payments

Is it fair and reasonable for Revolut to be held responsible for Mr P's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut was not the effective point of loss here. Mr P made the payments to a separate business which is also a regulated firm. I've also taken on board Revolut's argument that it shouldn't be liable for any shortcomings of any other firm Mr P interacted with.

However, as I've set out above, I think that Revolut still should have recognised that Mr P might have been at risk of financial harm from fraud when he made payment 3, and in those circumstances Revolut should have made further enquiries about that payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mr P 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 Mr P's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr P'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 either the firm that is the origin of the funds or the point of loss.

Revolut has also argued that, since Mr P made these payments to an account in his own name, this doesn't constitute an APP scam as defined in the DISP rules. I'm not persuaded that's relevant to the outcome of the complaint. The DISP rules contain a definition of an APP scam for the purpose of delineating this service's jurisdiction over a specific type of complaint. I don't think it has any bearing on whether Revolut acted fairly and reasonably in its dealings with Mr P.

I've also considered that Mr P has only complained against Revolut and Bank A. He hasn't complained about Payee A or B, which are regulated businesses in their own right. 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 Mr P could instead, or in addition, have sought to complain against those firms. But he has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut and Bank A.

I'm also not persuaded it would be fair to reduce Mr P's compensation in circumstances where: the consumer has not complained to every potential respondent from which they are entitled to recover their losses in full and where it is appropriate to hold a business such as Revolut and Bank A 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 Mr P's loss from payment 3 (subject to a deduction for Mr P's own contribution which I will consider below and an apportionment of liability between Revolut and Bank A).

Should Mr P 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.

Although contributory negligence is subject to an objective test in the courts, in considering what's fair and reasonable I've factored in his vulnerability when considering the extent of any deduction that should be applied, if any. To be clear, I recognise that Revolut didn't have any knowledge of the wider circumstances that underpinned Mr P's vulnerability. Nonetheless, I think it's a relevant consideration when considering this point.

Several months prior to the scam commencing, Mr P had lost his wife and daughter in tragic circumstances. As a consequence, he was extremely isolated. He also told an employee of Bank A that his wife had been responsible for managing household finances. He suffered with severe depression and has since been given a diagnosis of bipolar disorder, a condition which has a well understood association with impaired judgement when it comes to financial decision making.

It's noteworthy that he hadn't been promised a specific return by the fraudster. He was told that the returns earned were dependent on market conditions generally and so nothing could be guaranteed. He was also persuaded by an apparently professional looking website and a fake trading platform. Mr P tells me that he took his device into Bank A's branch and showed the trading platform to a member of its staff who didn't have any obvious concerns with what they saw. I wouldn't expect an employee working in a branch to be able to spot a scam based on that kind of evidence, but it would likely have reassured Mr P that he wasn't falling victim to a scam. He found some critical reviews online and queried these with the scammer who reassured him that they were a new business and that all firms receive at least some negative reviews.

I don't think it's at all realistic to think that a person in Mr P's circumstances wouldn't find they had an impaired ability to critically assess the information that was being presented to him and judge what level of risk they were exposing themselves to. I recognise that there was no reason for Revolut to have known about the full extent of Mr P's vulnerability at the time. Nonetheless, I think it's a relevant factor when determining whether he acted reasonably in the circumstances. The combination of the fraudster's persuasiveness and Mr P's personal circumstances persuade me that he was simply the unwitting victim of an experienced fraudster. On the particular facts of this case, I'm satisfied there was no contributory negligence.

Apportionment of liability

I'm mindful of the fact that Revolut was not the only firm involved in these transfers. The process of him losing his money began when he started making transfers from his account with Bank A to his account with Revolut. As I've explained, I don't think this means Revolut shouldn't have any liability for the losses he suffered. However, I am persuaded that liability should be shared with Bank A.

Mr P has referred a complaint to this service about the actions of Bank A which will be decided separately. However, I'm satisfied that Bank A, like Revolut, had ample opportunity to protect Mr P from the risk of financial harm here, but failed to do so. For that reason, I find that the fair and reasonable way to resolve this complaint is for both Revolut and Bank A to share 50% liability each for the money Mr P lost to the scam.

Other issues

I've also considered whether Revolut needs to compensate Mr P for non-financial losses. In particular, I've looked at the way Revolut handled things when he let it

know that he'd fallen victim to the scam. It learned what had happened when Mr P responded to its message that sought to clarify the source of his funds.

He responded to say that he'd fallen victim to a scam with very significant losses and that he was suicidal. The employee of Revolut responded by directing Mr P to communicate with a different team but reiterated the need for him to provide evidence of his source of funds. In a later message, he was asked to provide more details of his investment in shares. It ought really to have been clear to Revolut that Mr P had fallen victim to a scam, and it was asking him to provide evidence of the source of all of the money he'd lost. It did this even though he'd told them falling victim to the scam had left him suicidal.

The overwhelming majority of the distress Mr P experienced as a result of the scam was caused by the fraudster. But to send him those messages at that particular time was an unfeeling response which served to rub salt in the wounds. In the circumstances, I think Revolut should pay him £400 in recognition of the distress and inconvenience caused.

Mr P responded to say that he agreed with the provisional decision. Revolut didn't respond until after the deadline of 16 September 2024. It asked for a further two weeks to respond. I asked that it ensure any further representations arrive by 2 October 2024. At the time of writing, no response has been received.

Findings

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

As no further evidence or arguments have been submitted, I don't see any reason to depart from the findings I reached in the provisional decision. I am, therefore, upholding Mr P's complaint for the reasons set out above.

Final decision

For the reasons I've explained, I uphold this complaint. If Mr P accepts my final decision, Revolut Ltd needs to:

- Pay £400 in recognition of the distress and inconvenience it caused him.
- Refund 50% of the money Mr P lost to the scam from payment 3 onwards.
- Add 8% simple interest per annum to those payments calculated to run from the date they left his Revolut account until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 31 October 2024.

James Kimmitt
Ombudsman