DRN-5393648

The complaint

Mr A is unhappy that Revolut Ltd won't refund money he lost to a scam.

Mr A has brought his complaint with the help of a professional representative. For ease, I'll refer to all their submissions as being from Mr A.

What happened

Mr A says he was added to a social media messenger group with a focus on investments. He began to follow one of the individuals in the group, who made videos about his investment journey and profits. It later turned out this person was a scammer.

In line with the scammer's instructions, Mr A set up accounts with multiple 'investment' platforms. He also set up accounts with multiple cryptocurrency exchanges, including ones I'll call 'K', 'K2', 'B' and 'B1'. Using savings and a £13,000 loan taken out with a high street bank, Mr A made the relevant transactions using his existing Revolut account as set out below:

	Date and time	Payees	Method	Amount
	03 November 2023 12:28	*P*	*Credit*	*£14.20*
1	03 November 2023 12:28	K	Debit card	£10.00
	27 November 2023 19:30	*P*	*Credit*	*£98.05*
2	1 January 2024 21:28	K	Debit card	£10.00
3	10 January 2024 10:28	K	Debit card	£837.95
	15 January 2024 18:18	*P*	*Credit*	*£136.29*
4	22 January 2024 17:54	K2	Debit card	£100.00
5	27 January 2024 13:16	B	Debit card	£200.00

6	4 February 2024 09:56		Internal exchange into USDT	£50
7	4 February 2024 10:04		Crypto withdrawal to external wallet	50.00 USDT (US Dollar Tether)
8	4 February 2024 10:47	B	Transfer	£50.00
9	4 February 2024 12:51	B	Transfer	£11,900.00
10	19 February 2024 17:11	B	Transfer	£255.13
11	20 February 2024 09:19	B	Transfer	£410.50
12	15 March 2024 00:41	B1	Transfer	£119.00

Our Senior Investigator explained to Mr A that - from the evidence – it appeared that Mr A had received a refund from the scammer of £2,622.33 (in USDT) on 24 February 2024. As such, we proposed to deduct this amount from the total loss of £13,644.04, reducing Mr A's loss figure to £11,021.71 (in addition to 50 USDT to which I'll return later in this decision). Neither Mr A nor Revolut has challenged our view on the amount of Mr A's total loss.

Revolut said it recovered one payment of £119 from one of the beneficiaries (B) which cancelled out a payment to B. As such, our Senior Investigator did not include this amount in the table above – and I've not done so either.

Mr A says he realised he'd been scammed when he unsuccessfully tried to withdraw his 'profits'. He complained to Revolut saying it should have done more to protect him from the scam.

Revolut responded to Mr A's complaint to say it was not responsible for his loss. In summary, it said:

- All payments were authorised by Mr A.
- It had intervened, asked questions and provided warnings to Mr A.
- It wasn't possible for it to recover the vast majority of the funds, despite best efforts.
- It has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgment in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25. There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment 'APP' fraud.
- It should not be required to refund 'self-to-self' transactions, where it is only an intermediate link in a chain of transactions.
- It considered Mr A was grossly negligent by ignoring the warnings it gave. The Payment Services Regulation's ('PSR) mandatory reimbursement scheme will allow it to decline claims where a consumer has been grossly negligent, taking into account

any warnings it has provided.
- The withdrawal made in cryptocurrency shouldn't be considered by our Service as this is out of our jurisdiction.

Our Senior Investigator upheld Mr A's complaint in part. He said:

- The internal exchange into USDT is in our jurisdiction but given the amount he did not think Revolut should have provided any warnings to Mr A or make any refund to Mr A for the USDT. He did not think Mr A would challenge this point. He said the specific activity of withdrawing 50 USDT was outside our jurisdiction.
- Revolut should have recognised that Mr A was at risk of financial harm at the point he made payment 9 for £11,900 given Revolut knew or ought to have known the payment was going to a cryptocurrency provider with the associated elevated fraud risk.
- Revolut had intervened at payment 9, first with an automated series of questions and warnings and then with a human intervention via its in-app chat. But Revolut should have asked more questions surrounding this payment and, had it done so, it would have emerged that Mr A was being scammed. There was no evidence that Mr A was being coached by the scammer to give incorrect answers to Revolut's questions. Rather, he was up front about investing in crypto and that he'd found the investment on social media. The basic information about the 'investment' would have raised a serious red flag, based on the alleged unrealistic returns, but with no clear information about how the investment worked or returns were generated. An internet search would have shown the first investment platform (I'll call 'T') was not a legitimate investment firm.
- Although Mr A had ignored some on-screen warnings, our Senior Investigator was persuaded that stronger warnings given by a human as a result of a conversation and in the specific circumstances of his payments would have had more impact, such that Mr A would have stopped making payments. This was supported by Mr A having questioned the scammer about his concerns of losing his money so he was open to being educated about the risks.
- Given its knowledge of multi-stage scams involving cryptocurrency, Revolut should have been on the look-out for payments representing a scam risk. If it had made further enquiries at payment 9, it was likely Mr A's loss would have been prevented at that point.
- He'd taken into account that Mr A had received money from his high street bank. Mr A's bank had told this Service it didn't intervene on any of Mr A's payments. We had no power to compel Mr A to bring a complaint to us about his high street bank and he'd not done so.
- He thought Mr A should share the liability because: the returns were unrealistic, even for a cryptocurrency investment; Mr A had been scammed before recently (January 2024) via his high street bank account, so he should have been alive to scam risks for unregulated online investment platforms; he would likely have had to mislead his bank about his reasons for taking the £13,000 loan; and Revolut did provide some warnings relevant to the scam, but he proceeded despite those warnings.
- He didn't consider Revolut could reasonably have done more to recover the money Mr A had lost.
- He recommended that Revolut refund to Mr A the payments from and including Payment 12, less the £2,622.33 refund he'd received on 24 February 2024. Our Senior Investigator said Revolut could deduct 50% from the resulting amount for Mr A's contributory negligence, making a total refund of £5,031.15, plus 8% simple interest.

Mr A accepted our Senior Investigator's recommended settlement. But Revolut did not. In

summary, it said:

- This is a 'self-to-self scenario where Mr A owned and controlled the beneficiary account to which the majority of the payments were sent. So the fraudulent activity didn't occur on the Revolut account because payments were being made to perform legitimate cryptocurrency purchases to accounts in Mr A's own name. The cryptocurrency platforms were the final stage before Mr A allegedly sent the funds to the scam platform and then lost control of the funds. So the scam didn't occur on Revolut's platform.
- It has noticed that this Service's decisions often hinge on transactions being unusual or out of character, especially where they involve cryptocurrencies. But Mr A's account is not a current account and Revolut is an Electronic Money Institution ('EMI') not a bank. Typically, this type of account (the account with Revolut) is used to facilitate payments of a specific purpose and is not used as a main account. So the disputed payments were not out of character nor unexpected with the typical way in which an EMI account is used. This is particularly the case since high street banks have started restricting customers from sending money to cryptocurrency exchanges (an entirely legitimate activity) such that consumers using Revolut to send money to make investments in cryptocurrency is a common activity for Revolut accounts.
- Our reliance on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) is misconceived and amounts to a legal error. This is because it is a permission decision only and such decisions don't ordinarily create precedent, even for a court. Rather they are brief considerations of the arguability of a particular claim and don't have the same status as judgments which (by contrast) followed detailed pleadings, witness statements from both sides, and a full hearing.
- The Portal decision can't be relied on to allow this Service to abdicate responsibility for examining precisely what happened in a given case and ignoring the role of other parties – and in Portal the Ombudsman had apparently considered the firm's arguments on factual causation and loss.
- The Portal decision was in a materially different context, relating to pension transfers and opt-outs, which is a very different context to the service Revolut provides to its customers. Revolut's role is not to advise its customers at all, let alone adopt a role similar to a pensions advisor advising customers on transfers to self-invested pension plans. Referring to the Supreme Court's decision in Philipp: "it is not for the bank to concern itself with the wisdom or risks of its customer's payment decisions". It is easier to see how a pensions advisor might be held 100% responsible for loss on the facts in Portal than to see how Revolut could be 100% responsible in Mr A's case. Unlike in the Portal case, Revolut has no relationship with either upstream or downstream institutions involved in the fraud (that is, other institutions which could be said to be liable) unlike in the Portal case.
- The Ombudsman must explain their reasons for departing from English law. But Revolut has not asked the Ombudsman to analyse how damages would be apportioned in a hypothetical civil action. Revolut is asking the Ombudsman to consider all of the facts of the case before it when considering what's fair and reasonable, including the role of the other financial institutions involved.
- It is relevant to consider possible other bank interventions, as the funds that originated with Revolut came from Mr A's external bank account. This should be considered in tandem with this complaint. It is relevant to consider whether Mr A was warned by his bank as to whether he acted negligently in disregarding any such warnings.
- Revolut is not entitled to obtain information from Mr A's bank, but this Service is empowered to compel relevant disclosures from either the relevant banks or from the customer themselves under the relevant dispute resolution ('DISP') rules 3.5.11 and 3.5.12. Revolut believes that the use of such provisions might prove effective in this

scenario to establish a clearer understanding of events.
- This Service could also exercise its power under DISP 3.5.2 to inform Mr A that it could be appropriate to make a complaint against another respondent, if necessary, especially considering the sums involved.
- The above points should be considered when assessing Revolut's liability, as they play a pivotal role for a fair and reasonable outcome.

Our Senior Investigator responded to explain why Revolut's points did not change his mind. He said:

- Revolut's comments did not appear to relate specifically to the individual circumstances of this complaint. This Service had addressed many of the matters Revolut referred to in several final decisions.
- He had not made reference to or relied on the Portal judgment in his assessment of this complaint.
- While he did not fully agree with Revolut's interpretation of DISP 3.5.11 and DISP 3.5.12, he accepted the general premise that, as far as is practical, it is helpful to understand the actions of relevant third parties when considering a complaint about multi-stage fraud.
- In this case, he'd explained in his assessment that he'd contacted Mr A's main (high street) bank account provider which Mr A used to fund the payments to his Revolut account. The bank confirmed it did not intervene on any of the payments.
- He'd dealt with the issue of 'self-to-self' payments in his assessment when he considered whether Revolut should fairly and reasonably be held responsible for Mr A's loss.
- He asked Revolut to respond to the specific points in his assessment and reconsider its position, given Revolut had accepted many similar outcomes.

Revolut responded to acknowledge our Senior Investigator's feedback which it accepted had provided important context to his view on the matter. Revolut also acknowledged that many issues it had raised had been addressed in previous final decisions we had issued. But it said that this case primarily involves self-to-self payments, and so it requested a final decision.

As an agreement could not be reached, the complaint has come to me to decide.

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.

For the reasons I shall set out below, I have concluded that Revolut should have asked Mr A more probing questions about the purpose of the £11,900 payment (payment 9) that took place on 4 February 2024. Had it done so, I find that Mr A, more likely than not, would not have proceeded with that payment or the payments that followed. In those circumstances, and having considered Mr A's role in what happened, I consider it to be fair for Revolut to be held responsible for part of Mr A's loss. But I've also concluded that Mr A ought to share some responsibility for what happened and should receive a 50% reimbursement for the money lost from and including the £11,900 payment, less the credit he received of £2,622.33 on 24 February 2024.

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 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 A 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 A 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 payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should, in the period November 2023 to March 2024 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:

---

[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).

- 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), "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).
- 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[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).
- Since 31 July 2023, under the FCA's Consumer Duty[4], 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

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

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"[5].

- 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 the period November 2023 to March 2024 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.

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

It isn't in dispute that Mr A has fallen victim to a cruel scam here, nor that he authorised the payments he made by card and transfer to third parties and to cryptocurrency exchanges (from where cryptocurrency was subsequently transferred to the scammer).

Whilst I explained the circumstances which led Mr A to make the payments using his Revolut account and the process by which the money ultimately fell into the hands of the scammer, I am mindful that, at the time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr A might be the victim of a scam.

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

I'm aware that cryptocurrency exchanges like B 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 to cryptocurrency exchanges would be credited to a cryptocurrency wallet held in Mr A's name.

In the period November 2023 to March 2024, when the payments took place, 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.

As Revolut itself has observed, 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 the period of November 2023 to March 2024, when these payments took place, further restrictions were in place[7]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

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 a significant majority of cryptocurrency purchases made using the 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, a fact that Revolut is aware of.

So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Mr A made in the period November 2023 to March 2024, 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.

To be clear, I'm not suggesting that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in the period November 2023 to March 2024 when the disputed transactions took place that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings

---

[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.

before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

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

So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr A might be at heightened risk of fraud that merited its intervention.

The payments prior to payment 9 were all fairly modest in value. In addition, the payment pattern – with the payments being made over a period of four months - was not such that I think Revolut should reasonably have suspected they were being made as part of a scam. The payments were in line with Mr A's stated account opening purposes of 'transfers' and 'crypto'.

But payment 9 was significantly larger in value at £11,900, being around ten times the combined amounts of the relevant disputed payments to date. Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr A was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

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 (combined with the fact the payment went to a cryptocurrency platform) which ought to have prompted a warning.

Revolut argues that cryptocurrency transactions are common for its customers, particularly since high street banks have started to restrict this type of transaction. So it disputes that such payments are typically unusual or out of character. But as I have explained, I don't suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by November 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

Turning to payments 10, 11 and 12 I've noted that they were to a cryptocurrency exchange. But the payments were relatively low value and were not made in quick succession. I don't consider, of themselves, the payments were sufficiently suspicious as to require a warning. But I will explain below why I think it's unlikely Mr A would have proceeded with payments 10, 11 or 12 had Revolut provided Mr A with a proportionate and effective warning at payment 9.

What did Revolut do to warn Mr A?

Revolut said it provided a warning to Mr A when he set up the transfer to a new beneficiary. The warning said:

> *"Do you know and trust this payee?*

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

I will focus on disputed payment 9 of £11,900.

When he made the payment of £11,900, Revolut took Mr A through a process of on screen warnings and questions, and I've set out the key points here:

- Revolut showed a screen which said "We think you're being scammed – your transaction is unusual and was flagged as a potential scam. 99.2% higher risk than typical transaction".
- Mr A disclosed the following information while answering Revolut's automated questions about the payment purpose:
    - He was not being assisted through the questionnaire.
    - He was making the transfer as part of an investment – for gains from cryptocurrency.
    - He wasn't asked to install any software.
    - He found the opportunity online or via social media adverts.
    - He'd invested in crypto before.
    - He'd researched the company.
    - He was sending funds to his existing account.
- Revolut then showed Mr A some cryptocurrency investment scam warnings which covered:
    - The risk of high returns in short time periods and the scammer's use of professional-looking online platforms.
    - The risk of social media promotions promoting fake investment opportunities.
    - The risk of using screen-sharing software.
    - The need to research the investment platform, with the FCA and for online reviews.
    - Not to be rushed or pressured.

Revolut then asked Mr A to engage in an in-app chat with one of its staff, and I consider the key parts of that interaction are as follows:

- Revolut said "Our security system has paused your transfer of 11,900.00 GBP to [B] to protect you from a potential scam. I see you've already answered some questions before coming to chat. Based on your answers, we think there's a high chance that your money might be at risk if you make this transfer. To help us keep your money safe, we're going to check some additional details – this will take about 10 minutes. In the meantime, could you please give us some more additional details about why you are making this transaction?"
    - Mr A said "I am just buying some crypto to make a few investments".
- Revolut said "Thank you for letting me know. Scammers may impersonate Revolut, another bank or the police and pressure you to make a payment urgently, telling you to ignore our alerts. Never ignore these alerts, even if someone tells you to. Please stop and let us know if you are concerned for your account safety. It seems like this isn't a case where someone is instructing you what to do, which can be a red flag for scams. Could you confirm that you aren't being guided to make this transaction in any way?"

    - Mr A responded by saying “I can confirm I am not being guided by anyone else to make this transaction”.

- Revolut said “Thank you for your patience. Make sure any research you do is your own – fraudsters create convincing-looking posts on social media, or share articles about investing. If someone says you need to send money as a tax or fee to access your funds, you are being scammed. Are you comfortable with proceeding with this transaction?”
    - Mr A said “Yes I am. Thank you for your concerns but all is OK”.

I appreciate that Revolut went beyond its tailored written warning about cryptocurrency scam risks here. It made an additional, human intervention to ask Mr A some further questions about the payment, which it had flagged as highly suspicious.

But having considered all the circumstances, overall I can’t agree that the warnings provided went far enough or were proportionate to the risk that payment 9 presented, being for £11,900 to a cryptocurrency platform. While I accept that Revolut has attempted some steps to prevent harm from fraud, the warnings it gave were too generic to have an impact.

In this case, Mr A said that he was buying some crypto to make “a few investments”. But Revolut’s human intervention was, in my opinion, insufficient to understand the features of the investment Mr A was making. Revolut was aware from Mr A’s previous answers that he’d found the investment online or on social media and was making the transfer for cryptocurrency. But Revolut accepted Mr A’s answer about making a few investments at face value. I think Revolut should properly have asked more open and probing questions to include how Mr A believed the investments worked, the returns he’d been promised and any likely risks.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr A suffered from and after payment 9?

I can see the warnings given by Revolut were tailored to cryptocurrency scams, including that scammers might provide convincing-looking posts on social media and share articles about investments (as had happened in this case). But I can see that Mr A was answering questions honestly and I’ve not seen any evidence to suggest he was being coached either to ignore Revolut’s warnings or to lie to Revolut in his responses.

Despite the interventions being human, they had a generic quality to them. Revolut had obvious concerns around the transaction, but it failed to make any real enquiries about the circumstances surrounding the payment. It accepted Mr A’s one line response about the purpose of the payment (information it had already been given), rather than seeking to explore why he was investing in cryptocurrency. The second and third ‘questions’ just take the form of advice and don’t attempt to understand what was happening.

Had Revolut asked more probing questions, it seems to me that Mr A’s answers about the scam would likely have given a competent fraud analyst serious cause for concern. The returns he’d been promised of 1.5% compounded daily over 30 days with zero risk would clearly seem implausible. I don’t think Mr A could have explained how the investment worked, given his own questions to the scammer in their communications. Mr A had said he was concerned about losing his money when discussing the investment with the scammer, so I think he’d more likely than not have responded to being educated by Revolut about the high risk this was a scam. He was sending the cryptocurrency to an investment platform, that was not legitimate based on an internet search.

I can see that Mr A did ignore some of the earlier warnings. But I share our Senior

Investigator's view that Revolut could have uncovered the scam by careful questioning of Mr A and giving him strong and tailored scam warnings. I think that such warnings delivered by a human would likely have resonated with Mr A and he'd have stopped both payment 9 and the payments that followed (payments 10 to 12).

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

Revolut has addressed an Administrative Court judgment. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on the judgment. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved. I've done so in this case, for the reasons I'll set out below.

Revolut makes the point that this is a 'self-to-self' scenario where Mr A owned and controlled the beneficiary accounts to which the majority of the payments were sent. So the fraudulent activity didn't occur on Mr A's Revolut account but rather at the cryptocurrency platforms before he sent the money to the scammers and lost control of the funds.

I've carefully considered Revolut's view that in a multi-stage fraud, a complaint should properly be considered only against either the firm that is a) the 'point of loss' – the last point in 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.

In reaching my decision, I have taken into account that payment 9 was made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from Mr A's account with a high street bank.

But as I've set out above, I think that Revolut still should have recognised that Mr A might have been at risk of financial harm from fraud when he made payment 9, and in those circumstances Revolut should have declined the payment and made further enquiries before processing it. If it had done that, I am satisfied it would have prevented the losses Mr A suffered including and after payment 9. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to B does not alter the fact that I think Revolut can fairly be held responsible for Mr A's loss in those 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.

I've also considered that Mr A has only complained about Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr A could instead, or in addition, have sought to complain against those firms. But Mr A has not chosen to do that and, ultimately, I can't compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr A's compensation in circumstances where: Mr A has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm, and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr A's loss from payment 9, subject to a deduction for his own contribution which I will consider below).

Revolut appears to accept Mr A has only brought a complaint against it. But it says it is relevant to consider possible other bank interventions, as the funds that originated with Revolut came from his high street bank account.

Our Senior Investigator has correctly explained to Revolut that he made enquiries of Mr A's bank, which told us that it did not intervene in any of the payments Mr A made from his bank account to Revolut. So, on the evidence I can't fairly find that Mr A ignored warnings because his bank says they didn't give Mr A any warnings.

Should Mr A bear any responsibility for his losses?

Mr A has accepted our Senior Investigator's assessment that Mr A should bear 50% of his losses from and including payment 9. But for completeness, I'll set out why I think that's a fair deduction.

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 Mr A watched the scammer post his investment journey, 'profits' and the companies and platforms he was using, and the scammer was part of the group chat to which Mr A had been added. Mr A saw that the investment accounts he'd opened showed 'profits'. So I can see that this did reassure him that his money was being invested successfully.

But Mr A himself seems to have questioned the unrealistic returns he'd been offered, which included a daily profit of 1.5% for 30 days, together with other implausible returns offered on an hourly or weekly basis. I recognise this was a cryptocurrency investment, but I think the returns would reasonably have been considered to be too good to be true.

Sadly, Mr A had already fallen victim to a scam through his high street bank which he reported in early 2024. Although it's well known that fraudsters often target individuals who've already fallen victim to a fraud, I think that given the timing of events Mr A should reasonably have thought more carefully about the investments he was making, not least as he funded it through a loan from his high street bank – and I think it's unlikely he told the bank the correct reason for taking out the loan. Also, Revolut had given Mr A some relevant warnings. While I have explained why I don't think Revolut went far enough to warn Mr A, I also think he should reasonably share some responsibility for his decision to proceed.

Having reviewed all the circumstances, I think it's fair that liability be shared equally between Mr A and Revolut.

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

I don't consider Revolut could reasonably have done anything to recover Mr A's money for the following reasons:

- The only recovery mechanism for a debit card payment is the chargeback scheme. I don't consider any chargeback attempt would have been successful in this case because the 'service (of loading funds into cryptocurrency exchange accounts) would have been provided by each of the cryptocurrency exchanges involved.

- Mr A transferred funds to legitimate cryptocurrency accounts in his own name. From there he purchased cryptocurrency and moved it into a wallet address of his choosing (albeit on the scammers' instructions). If Revolut had tried to recover the funds, it could only have tried to do so from Mr A's own account and it appears all the money had already been moved on and, if not, anything that was left would still have been available to him to access.

Putting things right

Mr A's loss from the fraud (being payments 9, 10, 11 and 12) is £12,684.63. He received a credit from the scammers of £2,622.33. So his loss is £10,062.30. Revolut must pay 50% of this amount.

I require Revolut Ltd to:

- Refund to Mr A £5,031.15; and
- Add interest* to £5,031.15 at the simple rate of 8% per year from the dates payments 9, 10, 11 and 12 respectively were made to the date of settlement.

**If Revolut Ltd considers that it's required by HM Revenue & Customs to take off income tax from that interest it should tell Mr A how much it's taken off. It should also give Mr A a certificate showing this if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint in part and I require Revolut Ltd to take the steps set out in the 'Putting things right' section above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 6 June 2025.

Amanda Maycock
Ombudsman