DRN-4767103

The complaint

Mr M complains that Monzo Bank Ltd won't refund the money he lost as a result of a scam.

Mr M has used a professional representative to bring this complaint to our service and they have made submissions on his behalf. For consistency, I'll refer to Mr M throughout.

What happened

I issued my provisional decision on this complaint on 28 March 2024. I wanted to give both sides a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

Between 3 March 2022 and 21 June 2022, Mr M made 53 payments totalling £520,376 from his Monzo account towards a fake investment as a result of a scam.

Mr M, who was new to investing, was looking for investment opportunities to generate some income as he was close to retirement. He found an online trading platform (that I'll call T) who had prominent results on a search engine, and good feedback on the internet. So, he opened an account with them on 16 February 2022 in order to start trading.

Mr M's understanding was that T is an automated trading platform that represented a group of traders and brokers. On 16 February 2022, T assigned Mr M a broker (that I'll call S). T supposedly received the trading funds and distributed them to the assigned broker - S. Due to the belief Mr M held that T was a 'large, bonified and respected organisation on the internet with good reviews', he had confidence that the broker they directed him towards was reputable. It's unclear whether Mr M looked into S. On the one hand he says he visited S' website and found it to be professional, noting they had offices globally. On another occasion, Mr S told our Investigator that he didn't look into S as it had been recommended to him by T.

Mr M says that initially he was given a trial account with T, to learn and familiarise himself with the system. He says he could see graphs on T's platform showing how currencies and the markets were performing. After two weeks, he could request a live trading account from T, which he did.

Having seen online that Monzo permitted this type of investment, he opened an account with Monzo on 28 February 2022. He used three accounts in his own name, to fund his Monzo account. From Monzo, he sent the funds to an account in his own name at a cryptocurrency platform (that I'll call F). And from there, he sent this on to the fraudster.

Mr M says he was a total novice with forex trading. Of the research he did into forex trading, he found F was supposedly the largest cryptocurrency site in the global industry so he assumed all dealings with F would be professional, legal and above board. He opened an account with F, as he needed to convert his funds into cryptocurrency to fund the investment on T. Mr M says the funds were converted into USDT on F, and then sent to a

cryptocurrency wallet, which he had to apply for and obtain from T on each transactions sent.

Mr M claims he could see such deposits reflected on his account with T and having access to the trading portal with T made him feel in control of his funds. The scammer offered Mr M incentives to invest more such as company bonuses which Mr M says he could see reflected in his account. For example, on 7 March 2022, Mr M confirmed he would invest $500,000 with T because there was a reward scheme offered whereby if he invested this amount, he'd be awarded with an account bonus of around $68,000. Mr M was happy with how his investment was performing and this was his main motivation behind investing the sum he did.

Mr M says he got to a point where he had accumulated $2.8 million in his trading account, so he asked for a withdrawal into his business bank account held with another bank (Bank L). But he was met with excuses as to why he couldn't withdraw his profits. For example, he was asked to set up a different wallet and verify it by depositing $50,000 which would be refunded to him shortly after, but of course this wasn't refunded.

Mr M did open an account with another cryptocurrency platform (that I'll call C) to facilitate this. But he only made payments to this account from his account at Bank L. He says the fraudster told him step by step how to open the account with C and send funds to the wallet. He says the fraudster then accessed the wallet and took the cryptocurrency and didn't return it. Each time he requested a return, they would ask for huge release fees, so he never received any returns. He says this was the only point in which he had doubts about the investment. He was also threatened by the fraudster if he didn't make the payments. They said he would be pursued for liabilities if he didn't pay, and his credit score would be impacted. Mr M soon realised he'd been scammed as the requests for further funds continued.

Monzo closed Mr M's account on 22 June 2022. After this point, he opened another account with a different bank (Bank S) on 25 June 2022, to continue making the payments towards the investment. Mr M previously said he opened this other account with Bank S as a savings account, but he has also said the account was used to make payments to F until the scam came to light when he could not make a withdrawal from his investment.

Mr M reported the matter to Monzo on 14 July 2022. Monzo says it asked Mr M for information on multiple occasions, but he did not always respond. On 7 November 2022, Monzo declined Mr M's claim. Mr M raised a complaint in October 2022 which Monzo declined for the following reasons:

- *The payments were made intentionally by Mr M. Monzo acted in accordance with Mr M's instructions.*
- *Mr M sent the funds to F in order to purchase cryptocurrency which F successfully delivered. So, there was no loss for the transactions Monzo was involved in. Mr M should contact F for help.*
- *Monzo gave Mr M warnings and intervened on a number of payments. Mr M confirmed he was 100% confident and there was no fraud involved.*
- *Mr M didn't conduct sufficient checks and the investment was too good to be true.*

Unhappy with this response, Mr M referred his complaint to our service. In its submissions, Monzo told our service the Contingent Reimbursement Model (CRM) Code, which Monzo has agreed to abide by the principles of, was a relevant consideration in Mr M's complaint.

The CRM Code sets out that Monzo should refund victims of authorised push payment (APP) scams (like Mr M), in all but a limited number of circumstances. Monzo said Mr M

didn't have a reasonable basis for believing the person or business Mr M paid was legitimate, as he did no due diligence, and the investment was too good to be true. But it also said that the payments were out of scope of the CRM Code as the payments were made between accounts in Mr M's own name.

Our Investigator looked into things and upheld Mr M's complaint. They thought Monzo should have done more to check the legitimacy of the payments Mr M was making, but that Mr M also should share liability for acting with contributory negligence. They recommended Monzo put things right by refunding 50% of Mr M's total loss and paying 8% simple interest per year on the refund amount, from the date the transactions were made until the date of the settlement.

Mr M accepted this outcome, but Monzo did not. It said:

- *The fraud did not happen at Monzo. Mr M bought legitimate cryptocurrency from a well-known and respected merchant (F). As the funds were sent to an account in Mr M's name, there was no fraudulent transaction made from Mr M's Monzo account.*
- *Mr M would have continued with the payments even if Monzo had asked more questions.*
- *It's unreasonable to expect a bank to be able to exercise any control over how a customer uses goods that they have legitimately purchased (in this case, cryptocurrency).*
- *Monzo referenced a recent Supreme Court case in saying the basic duty of a bank is to make payments in accordance with the customer's instruction. Refusal to execute a payment in accordance with the customer's instructions could be considered a breach of mandate. As Mr M did not dispute he made the payments, Monzo acted in accordance with his payment instructions. Just because Mr M was tricked into making the payment, does not invalidate the payment instructions he gave.*
- *Monzo referenced upcoming regulatory changes on mandatory reimbursement of APP scam losses. Such regulation does not intend to cover losses such as this. So, there is no expectation for Monzo to refund the loss where the payment had been made across other payment systems (such as where the customer sends funds to their account as a cryptocurrency exchange and then sends cryptocurrency to a fraudster).*

What I've provisionally 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 doing so, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

The starting point under the relevant regulations (in this case, the Payment Services Regulations 2017) and the terms of Mr M's account is that Mr M is responsible for payments he's authorised himself. And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, banks generally 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 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, the bank 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.*

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

In this case, Monzo's December 2021 terms and conditions gave it rights (but not obligations) to:

- *Block payments if it suspects criminal activity on a customer's account. It explains if it blocks a payment it will let its customer know as soon as possible, using one of its usual channels (via it's app, email, phone or by post)*

So, the starting position at law was that:

- *Monzo was under an implied duty at law to make payments promptly.*

- *It had a contractual right not to make payments where it suspected criminal activity*

- *It could therefore block payments, or make enquiries, where it suspected criminal activity, but it was not under a contractual duty to do either of those things.*

It is not clear from this set of terms and conditions whether suspecting a payment may relate to fraud (including authorised push payment fraud) is encompassed within Monzo's definition of criminal activity. But in any event, whilst the current account terms did not oblige Monzo to make fraud checks, I do not consider any of these things (including the implied basic legal duty to make payments promptly) precluded Monzo from making fraud checks before making a payment.

And, whilst Monzo was not required or obliged under the contract to make checks, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good practice at the time, it should fairly and reasonably have been on the look-out for the possibility of APP fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances – as in practice all banks, including Monzo, do.

I am mindful in reaching my conclusions about what Monzo ought fairly and reasonably to have done that:

- *FCA regulated banks are required to conduct their "business with due skill, care and diligence" (FCA Principle for Businesses 2) and to "pay due regard to the interests of its customers" (Principle 6)[1].*

- *Banks have a longstanding regulatory duty "to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime" (SYSC 3.2.6R of the Financial Conduct*

[1] 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.

Authority Handbook, which has applied since 2001).

- *Over the years, the FSA, and its successor the FCA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by banks to counter financial crime, including various iterations of the "Financial crime: a guide for firms".[2].*

- *Regulated banks 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).*

- *The October 2017, BSI Code, 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, but in my view 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.*

- *Monzo has agreed to abide by the principles of the CRM Code. This sets out both standards for firms and situations where signatory firms will reimburse consumers The CRM Code does not cover all authorised push payments (APP) in every circumstances (and it does not apply to the circumstances of these payments for reasons I'll come on to explain), but I consider the standards for firms around the identification of transactions presenting additional scam risks and the provision of effective warnings to consumers when that is the case, represent a fair articulation of what I consider to be good industry practice generally for payment service providers carrying out any APP transactions.*

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Monzo should fairly and reasonably:

- *Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.*

---

[2] For example, both the FSA's Financial Crime Guide at 4.2.5G and the FCA's 2015 "Financial crime: a guide for firms" gave examples of good practice in relation to investment fraud saying:

"A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.

A bank contacts customers if it suspects a payment is being made to an investment fraudster.

A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules."

- *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 banks are generally more familiar with than the average customer.*
- *In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – as in practice all banks do.*
- *Have been mindful of – among other things – common scam scenarios, the evolving fraud landscape (including for example the use of multi-stage fraud by scammers) and the different risks these can present to consumers, when deciding whether to intervene.*

I've considered the circumstances of this case carefully and whilst I'm extremely sympathetic towards Mr M's circumstances, I don't find that Monzo can be fairly held liable for his loss.

Did the payments Mr M made indicate he might be at risk of financial harm?

Firms process hundreds of thousands of transactions on a daily basis, and so it would not be reasonable to expect it to intervene on each and every one. Instead it should do so where it identifies a transaction indicates the consumer might be at risk of financial harm. When deciding this, I'd expect the firm to consider whether the transaction is out of character and unusual, considering that particular customer's account usage and also pay due regard to known indicators of fraud.

Our Investigator found Monzo ought to have been concerned Mr M was at risk of being scammed, when he attempted the first payment, and it ought to have intervened and made further enquiries with Mr M before allowing the payment to be made. He said this because Monzo ought to have been on the lookout for unusually large or suspicious transactions. And the payments were going to a well-known cryptocurrency provider, so he thought this presented an APP scam risk, given the prevalence of cryptocurrency scams at the time.

I'm mindful that in this case, Mr M appears to have opened the account with Monzo for the purpose of the scam. So Monzo didn't have any prior awareness of his typical spending habits. However, I'd still expect Monzo to have taken into account the information available to it at the point the payments were made, when deciding whether the payments presented a fraud risk.

When Mr M opened his account with Monzo, he told them the intended use of the account was 'cash deposits' and the first three transactions showing on Mr M's statements are deposits from his business account with Bank L totalling £30,000. So the initial activity did align with the stated account opening reason. On 3 March 2022, Mr M made the first debit (and fourth transaction) on his account which was a £10,000 faster payment to F – a known cryptocurrency provider. I don't think this aligned with the intended account opening reason Mr M had provided Monzo, and given the value of the payment, I would have expected Monzo to provide Mr M with a warning tailored to the apparent scam risk, based on the information provided by the consumer. And when Mr M continued to make payments of £10,000 a day to F over the next three days, Monzo ought to have gone beyond an online warning and contacted Mr M, such as via the in-app chat, to ensure he wasn't at risk of financial harm, given the sums he was sending.

When Mr M set up the new payee for F, he was presented with an automated online warning which said:

"Could someone be trying to scam you?

Stop if:

- *x You were told your account is at risk, to make an unexpected payment or to take out a loan*
- *x The offer sounds too good to be true*
- *x You haven't double checked who you're paying*
- *x You were told to ignore warnings like this*

You may lose money if this is a scam

If you're at all unsure, stop and get advice."

Whilst this warning was not tailored to any particular type of scam, this doesn't automatically mean Monzo can be held liable for Mr M's loss. I have to consider whether a better intervention from Monzo would have likely made a difference to Mr M's decision to proceed with the payments.

Would an intervention from Monzo have deterred Mr M from making the payments?

It's worth me noting that Mr M referred two other complaints to our service in relation to this particular scam. So, in reaching my provisional decision on Mr M's case, I have taken into account all of the information he has provided our service with about the scam.

Having done so, I'm not persuaded that an intervention from Monzo, or likely any bank, would have deterred Mr M from proceeding with the payments. And therefore, I can't fairly and reasonably hold Monzo liable for Mr M's loss. I know this will be highly disappointing for Mr M, so I'd like to explain why I've reached this outcome.

Turning to the interventions he received from the firms involved, I am aware that he interacted with at least three firms throughout the course of the scam. I'll go into greater details about each of these interactions below.

Interactions with Bank N

Mr M opened an account with another bank (Bank N) on 18 February 2022. He says he opened this account as he already held savings with Bank N, and he could only move funds to another account with Bank N, in order to access them. On 21 February 2022, Mr M attempted to send £18,600 to F from his account with Bank N. But this was automatically blocked by Bank N.

Similarly on 27 February 2022, Mr N attempted a second payment to another cryptocurrency platform (that I'll call G) for £10,000. Again, this was blocked by Bank N. For both payments, Bank N says Mr M would have received a text message explaining that the payment was blocked due to a bank policy restricting payments to cryptocurrency providers and containing a link to further information to cryptocurrency. Mr M says he doesn't recall ever receiving such a text. However, he proceeded to send the same amount to his own business bank account held at Bank L, the following day. This suggests to me Mr M did have an understanding that Bank N was restricting payments to cryptocurrency providers.

To my knowledge, Mr M attempted to send funds to F from Bank L on 18 February 2022, but this was returned to his Bank L account on 23 February 2022 as F wouldn't accept funds from a business bank account. So Mr M opened an account with Monzo on

28 February 2022 and proceeded to move funds from Bank N to Bank L, to Monzo, and from Monzo to F.

Bank N has provided evidence of two phone calls it had with Mr M in relation to payments made to F, which Mr M has not included as part of his dispute. I've listened to two phone calls between Mr M and Bank N. The first phone call, which took place on 25 June 2022, was to discuss payments Mr M was attempting to his own account with Bank S. During this call, Mr M told Bank N that he was moving the funds to his Bank S account and on from there to his Bank L account in his business' name. Mr M confirmed he'd only opened the Bank S account within the last 24 hours and they both discussed their experience of Bank S, with the Bank N employee highly commending Bank S' customer service. During this conversation, Mr M told Bank N that he trades in cryptocurrency and that Bank N "just puts a block on everything" and "this is why I hope (Bank S) is going to be okay, I don't go mad with crypto and I know about all the risks". The Bank N advisor told Mr M that Bank N tend to stop all payments to cryptocurrency so it's better to deal with another bank.

A second call with Bank N and Mr M took place on 6 July 2022. This call was to discuss a number of payments Mr M was making to F. He told Bank N he was trying to make a payment to a company he has paid 'many, many, many' times before. Bank N confirmed the payments had been rejected automatically as they'd been deemed high risk by a fraud and scams payment profiling system. Mr M explained F is 'a receiving entity for crypto' and he'd used them since February when he started trading. He said he'd 'never had one problem with them' and has '100% confidence' in where he is sending the money and where it ends up. He explained he has a cryptocurrency site, and he is trading. He has evidence it's all there and all is fine – he is 100% sure of it. Bank N explained it has seen quite a high increase in cryptocurrency scams at that moment, not necessarily specific to F, but a lot of payments do flag and then automatically reject. Bank N explained cryptocurrency scams are on the rise which could be why the payments have automatically rejected. They explained some cryptocurrency providers come with a high risk of customers being victims of fraud. Bank N wouldn't put through the payments for Mr M and sent him an email with further information.

Mr M explained it's a fund verification amount and once cleared, he'd be getting $700,000 paid into his Bank N account. He said "I can assure you it's not a scam and I am quite confident that everything is fine on my end. I really need to get this payment away to them". Bank N confirmed they couldn't put the payment through for him, but it would send him an email with the answers to his questions. Mr M said, "I don't have any questions and I am quite confident 100% that the payment I'd like to make is 100% bonafide and secure – I've got no problem with it at all". Mr M explained he'd banked with Bank N for a number of years and couldn't understand why they wouldn't permit the payments to go through. Bank N explained the information would be shared with him via email. Mr M also asked how he could escalate and described it as 'crazy'. Mr M said, "I know you're only trying to look after my interests…but I really do have to get £4,850 away to these people".

Interactions with Monzo

In addition to the aforementioned warning Monzo gave Mr M when he set up the payee for F on 3 March 2022, Mr M had to contact Monzo via live chat on 11 March 2022 in order to increase his daily transfer limit so that he could move funds to F. He said, "Maybe ask you could you make a payment to a regular recipient of mine". When Monzo asked what the payment was for, Mr M said "The payment is for an investment and there is no documentation I can provide to you. I have an account set up with F of which I can prove to you it exists". He went on to say, "F are a trusted recipient and if you look back at my account, several payments have already been made by me to their account". Monzo approved the request.

On 13 March 2022, Mr M asked again for his payment limits to be increased. He said "I need to work to a deadline which makes this necessary to transact!...The transaction is for a [sic] investment. The people who I want to send the money to are a trusted recipient (F) who I have made many recent dealings with. Please check my account as evidence of this!". Monzo approved the request.

On 22 March 2022, he asked again for his payment limits to be increased. He said, "It's to go to my previous trusted company (F)…The money is being used as an investment exactly the same as my previous payments made to this company. The company is known to me and is safe!...I've sent the selfie and explained the payment is for an investment. I've made previous payments to F without incident as they are a trusted company. Please look back at previous payments made to this company by myself".

At this point, Monzo grew concerned Mr M might be at risk of being scammed. And it presented him with a warning in the chat which said:

> *"I'd like to assure you that legitimate organisations will never tell you to move money or take sudden action*
>
> *Remember:*
>
> *Legitimate investments will never guarantee profit*
>
> *Legitimate investments aren't arranged over social media or things like WhatsApp*
>
> *Check out the company*
>
> *See if they're a legitimate company here. Don't pay unless they're registered with the FCA and you're certain you trust them."*

It also asked Mr M to take a look at a link to a blog post on its website about scams.

In response to this, Mr M said "The F account is not registered in my name and it is used to traffic payments into my (cryptocurrency) account. All payments have been transacted by F without any problem whatsoever. The account it ends up in is registered in my name and I'm happy to provide a screenshot of this account. I'm 100% confident that all is ok and fraud is not involved whatsoever".

Monzo asked for a screenshot of his cryptocurrency account with F, which he provided. He also sent a screenshot of the trading account with T showing his existing balance and said, "As you can see things are going rather well". Monzo has provided a copy of a screenshot which appears to show the balance of a trading account at $946,239.05. I have presumed this is the screenshot Mr M sent to Monzo when he made the comment that things are going well. Given Mr M had been honest with Monzo and told them he was moving the funds to an investment, and this screenshot clearly showed it was a trading investment, I think this ought to have prompted more questions from Monzo to check the investment was legitimate. I also think the values shown within the screenshot, ought to have caused Monzo concern that what Mr M was involved in was 'too good to be true'. So, I accept that Monzo failed to provide Mr M with greater warnings when it became aware of this information. And I'll come on to explain the impact this has on my decision at a later point.

Monzo reviewed the evidence but decided it had no major scam concerns as the accounts showed as registered in Mr M's name. So it approved the request to increase his transaction limits.

On 8 April 2022, Mr M asked Monzo again to increase his daily limits. He said "I need to make a payment to my trusted service provider F. If you look back during the month of March, there has been considerable financial processes between us, so I'm happy that there is [sic] no potential fraudulent dealings to worry about." Despite Monzo's internal notes showing it referred this to an internal team due to concerns of a scam risk, it approved the request.

On 21 April 2022, Mr M asked Monzo to increase his daily limits again. He said, "would you please arrange for a payment to be made to F who are a trusted service provider of which I've used many times previously". On this occasion, Monzo had frozen Mr M's account whilst it reviewed his account usage. It was later unblocked, and Mr M continued to make further payments to F until 21 June 2022. Monzo closed his account on 22 June 2022.

Interactions with Bank S

After Monzo closed Mr M's account, Mr M opened an account with Bank S on 25 June 2022. The same day, he made a £1,000 payment to F and was presented with an online warning when he set up the payee. This warning said:

> *"Warning*
> *Always research a company and check reviews from other people. If the investment returns sound too good to be true – this could be a scam. All Financial Advisors and Financial Institutions should be FCA registered. You can check the FCA register here…"*

*Later the same day, Mr M attempted a £5,000 payment to F which was blocked by Bank S. He contacted Bank S via live chat and said "This transactions [sic] to F is a trusted service provider of which I've made may [sic] payments to in the past…Would you please release this £5k payment. It's to a service provider I've used many times before. It is but [sic] a scam, it's a trusted account that I use regularly…*Not a scam". He went on to say, "I appreciate your taking care of me and my account, but on this occasion I am 100% sure this is a trusted account as I've used them for months now without incident. I'm more than happy to accept full responsibility for this transaction".*

When asked if the payment was for cryptocurrency, Mr M said, 'It's an investment fund…It's not a scam I can assure you of that!". Bank S explained the value exceeded their account limits for cryptocurrency related transactions and confirmed if Mr M was to make smaller payments this should be okay.

On 28 June 2022, Mr M had a further interaction with Bank S when payments he was attempting to send to F were blocked. He said, "I have tried to make a payment this morning of which has been prevented. This I need to make to complete an investment I'm involved in. The payee is a trusted company who I have used many times previous."

When asked if the payment was for cryptocurrency, Mr M said, "The company is involved in crypto I understand but this is a separate investment I'm looking to make a final payment, in stages if needed of only £3500…I've made months of trusted payments which have all been received". Again, Mr M discussed lowering the value of the payments to circumvent the friction he was experiencing.

When he was still unable to make the payment, he contacted Bank S again and said, "Can you please permit this payment as it is a private investment…I'm happy to take full responsibility for the transaction".

What do these interventions mean for Mr M's complaint against Monzo

For the reasons I've explained, banks like Monzo are expected to intervene where a transaction identifies the consumer might be at risk of financial harm. I appreciate Mr M feels strongly that Monzo is at fault for failing to warn him about the payments he was making being potentially linked to a scam. However, the failure to do so, won't mean the bank is automatically presumed liable for the loss that consumer has suffered. It's crucial that I consider whether Monzo's failure to intervene, had a material impact on the success of the scam. The above listed interventions have all informed my decision on this. And I'm sorry to disappoint Mr M, but I'm satisfied that Monzo's failure to intervene had no material impact on the success of the scam.

Firstly, it's clear from the above interventions that Mr M greatly trusted the investment he was involved in was legitimate. He made a point, in almost every interaction he had with the various banks, of stating that F was a trusted recipient and that he had transacted with F many times before – often before he was asked, which I presume was to pre-empt any concern from the banks about the legitimacy of the payee. He repeatedly told the banks involved of his confidence in what he was doing, and he was certain he was not being scammed and it was a legitimate investment. When our Investigator queried this with Mr M, he explained F was trusted because it was himself that he was paying. But I don't agree that in the context of these interactions, Mr M was suggesting this was why he trusted the recipient. He made it quite clear that he trusted in the investment he was making.

With this in mind, I've thought about what would have happened if Monzo had given Mr M a much better warning about cryptocurrency investment scams. For the reasons I've already explained, Monzo knew enough information about the payments, considering their appearance, what Mr M had told it, and the screenshots Mr M shared, to be concerned he might be at risk of a cryptocurrency investment scam. So I'd have expected Monzo to have asked Mr M further questions about the nature of the investment, and how he came across it, to try to establish whether he was at risk of financial harm. From the previous interventions I've listed, it's clear Mr M was not trying to hide what he was doing – he was honest with all the firms involved that he was making an investment. So I have no reason to believe he would have misled Monzo, had it asked him more questions, which I think it ought to have done.

But I'm mindful that from the way Mr M has described the scam, it didn't necessarily carry many of the typical features one might expect to see in such a scam. For example, he sought out T himself. He wasn't cold called or approached by anyone. He had no dealings with the broker – S - until he attempted to make a withdrawal at later stages of the scam. He is adamant he was not coached, nor was he told what to say to the bank. Having reviewed the messages between him and T, I believe this to be true. And he didn't give the fraudster access to his device – he made all the transactions himself. So there does seem to be an element of him investing independently here. This isn't typically what you might expect to see in a cryptocurrency investment scam. So even if Monzo had given Mr M a warning which covered off the common features of this type of scam, I'm not persuaded it would have resonated enough with Mr M to sufficiently override the clear trust, if not certainty, he had in what he was doing.

I do acknowledge that the interactions he had with Monzo, and the other banks involved, did not go into any great level of detail about cryptocurrency investment scams or what they typically look and feel like. However I'm mindful that Mr M received a number of interventions

and warnings from various banks, and on balance I'm satisfied that there was enough brought to his attention overall to put him on notice that there was some risk that he was being defrauded when making the investment. For example, Bank N explained cryptocurrency transactions are on the rise and payments to such providers (like F) carry a greater risk of the consumer being the victim of fraud. Monzo told Mr M that WhatsApp would not be used to arrange a legitimate investment – which was the method of contact he was using in the scam. Multiple firms told Mr M to check the companies he was dealing with were regulated by the Financial Conduct Authority (FCA), which Mr M confirmed he had some knowledge of through his business dealings. And multiple firms warned him of investments which are too good to be true – and considering Mr M thought he had generated profits in the millions, I think this was likely applicable to him too. Despite this, Mr M was still happy to proceed and was adamant that what he was doing was legitimate.

By Mr M's own admission, he was new to investing. So, I would have expected him to pay due regard to the risk of cryptocurrency scams, being brought to his attention by multiple firms. His version of events about the level of due diligence he conducted into the investment opportunity, has been inconsistent at times. But I've understood he found T on the internet, and he did some research into T by looking at reviews and ratings for prior users. He trusted S because it had been recommended by T. The most he looked into S was reviewing their website – but again his version of events has been contradictory on this point. Unfortunately, evidence of S' website has not been provided so I'm unable to place much weight on how sophisticated this might have appeared to Mr M at the time. He says he did look into forex trading in general online, and this led him to find that F was a well-known cryptocurrency platform. Based on the information provided, this is the extent to which Mr M looked into the investment and the companies he was dealing with. Given the concerns being brought to his attention by multiple firms, and the limited due diligence he conducted, I'm unable to see why he didn't take heed of the warnings he was being given.

In terms of his understanding of risk when investing his funds, Mr M said "like any other investment, it's a chance you take, some may do well, and some may not. But if you do, do well, the reward outweighs the risk". So, despite him being a self-confessed novice, he does seem to have had some awareness of the risks of investing and seemed to accept the risk that came with trading. Mr M also admits he didn't seek any financial advice before making the investments. He said 'I am a managing Director of a successful Engineering company with 45 years' experience in handling financial affairs / situations etc. I felt I had the relevant experience to join a trading platform based upon my own knowledge and personal intelligence.' He also told Bank N in a phone call that he knew about all the risks of cryptocurrency. And on a couple of occasions, he told the bank(s) he was willing to accept full responsibility for the transaction. Taking these things into account, I am persuaded Mr M placed great weight on his own ability to calculate the risks involved in proceeding with the investment, and this did impact his receptiveness to any warnings he received from the multiple banks involved in the payments he made. I'm not persuaded there is anything further Monzo could have said to change Mr M's mind in proceeding with the payments.

But, even if he had been told to conduct further research into the investment, the platform he was using (T) is a legitimate software that sadly was used by a fraudster to scam Mr M, so had he been prompted to conduct further research into T, which is who he thought he was communicating with, it might not have uncovered that who he was speaking to, was a fraudster. There was also very limited information about S online, so again, it's difficult to see what he would have found had he conducted further research into S under Monzo's instructions. And by Mr M's own admission, he did not think it was necessary for him to seek advice from a financial advisor, despite having no experience in the investment, because he trusted his own understanding of how the investment worked. So I'm not persuaded Mr M likely would have been willing to conduct further checks into the investment, nor would such further checks have easily identified with any certainty that he was being scammed, which I

think would have been necessary to break the spell, given how much Mr M trusted the investment to be genuine.

Even if Monzo had taken further steps to deter Mr M from making the payments, such as through further interventions as the payments continued, I'm not persuaded this would have prevented Mr M from losing this money. I say this because the evidence suggests that when Mr M's payments were restricted by a firm, he attempted to send the funds in a different way instead to circumvent this.

Mr M has provided some information about why he opened so many accounts. He says he opened an account with Monzo because it was a cryptocurrency friendly bank. He opened an account with Bank N because it was the only way he could utilise the balance in his savings account with Bank N. He moved funds to Bank L to aid with 'cash flow' of his business. He moved funds from Bank L to Bank S because F would not permit deposits from a business bank account. And he says he opened an account with Bank S for savings purposes, but then he used it for payments to F. I've taken Mr M's version of events into account, but I've also weighed this up with the evidence presented to me as well as what I consider to have been the most likely version of events.

The evidence compels me to believe that Mr M opened the Bank N account to access his savings and move funds to F. When he was unable to move funds to F from Bank N, he sent his funds to Bank L and Monzo. When he was unable to move funds from Bank L to F, he opened an account with Monzo instead, to forward the transmission of funds to F. When Monzo blocked and closed his account, he opened an account with Bank S instead and proceeded to move funds to F via Bank S. At the same time he was experiencing friction from Bank N when paying F, so he confirmed in the phone call that he was moving his funds to Bank L, then to Bank S, then to F instead. When he was unable to send funds from Bank S to F, he tried reducing the payment values in order to deter the automated blocks he was faced with. Whilst Mr M suggested he made the payments in this manner in case he made an error, and due to daily payment limits of the banks involved, the evidence I've seen suggests this was a deliberate attempt to avoid friction from the banks transaction detection systems. This is supported by the messages he exchanged with T on 24 June 2022 which said, "My bank is restricting payment to crypto companies so I'm gonna [sic] have to slide them through in stages to sneak them through hopefully".

On the balance of probabilities, I think it's more likely than not that Mr M opened all of these accounts and made the payments in the way he has, to circumvent the restrictions the firms were placing on the payments to cryptocurrency providers. I think this was because they were preventing him from making payments to F directly as part of the investment, an investment he believed was genuine, and he confirmed this during some of the conversations with the banks involved. For example when he talked to Bank S, he enquired about sending lower amounts to avoid the friction. And when speaking to Bank N, he implied he was moving funds to Bank S because Bank N was blocking his cryptocurrency transactions. Whilst I appreciate Mr M was likely doing this because he was frustrated by the restrictions put in place around cryptocurrency transactions, as he believed he was making a legitimate investment, this did mean it was much more difficult for the firms involved to detect that Mr M was falling victim to a cryptocurrency scam.

In light of the above, I am satisfied that even if Monzo had taken further steps to intervene on the payments Mr M was making, this would not have prevented Mr M's loss. It's seems more likely than not that Mr M would have found another way to send the funds to F. So Monzo can't fairly and reasonably be held liable for Mr M's loss, when this loss seems to have been unavoidable, based on Mr M's determination to process the payments to F.

Recovery of funds

I'm not persuaded Monzo could have done anything to recover Mr M's funds. He reported the scam to Monzo on 14 July 2022, which was over three weeks after he'd made the last payment to F. Furthermore, Mr M confirmed he sent the funds to F to convert into cryptocurrency which was sent on to a wallet address provided by T. It's therefore highly unlikely any funds remained in his own account with F, at the time he reported it to Monzo.

The Contingent Reimbursement Model Code

I've also thought about whether the payments should be considered under the CRM Code which Monzo has agreed to abide by the principles of. I know this will be disappointing for Mr M, but I'm not persuaded there are any reasonable grounds to apply the provisions of the CRM Code to his case, for multiple reasons.

- *Mr M has made the payments to an account in his own name, which he had control over, at F. So, the funds have not been sent to 'another person' and therefore the definition of an APP scam under the CRM Code has not been met. The definition requires that funds be sent to 'another person'.*
- *Secondly, Mr M sent the funds to F for the onward transmission of cryptocurrency. The CRM Code only covers faster payments between GBP, UK-based accounts. The transaction from F to the fraudster was not a faster payment between GBP accounts as it's a transaction in cryptocurrency.*
- *The transaction was also a legitimate purchase of cryptocurrency from a genuine business – F.*

Therefore, I agree with Monzo that the CRM Code doesn't apply here.

So, in light of all of the above findings, there's no fair and reasonable basis under which I can ask Monzo to reimburse Mr M's loss.

My provisional decision

For the reasons I've explained above, I do not intend to uphold this complaint.

Monzo accepted my provisional decision and had nothing further to add. But Mr M did not accept the provisional decision reached. In disagreement, he said:

- The payment activity was highly unusual and bore the hallmarks of an investment scam. And in total, over £500,000 debited his account in a short space of time.
- The activity should have given rise for concern and further investigation, given the clear indicators that these payments were destined to be invested in cryptocurrency.
- Monzo did not intervene effectively. The questions and warnings were generic and basic. A member of staff ought to have flagged the activity to senior management.
- Monzo dealt with Mr M under 'business as usual' processes, rather than any value-based or risk-based exception review, despite the activity being 'ultra-rare' and 'ultra-high risk'. It should have processes in place that routed Mr M to a specialist team, including a management review of recent account activity. The payments should have been stopped and blocked.
- Mr M wants Monzo to demonstrate that they have any process to route ultra-high risk payments, in terms of value and volume, to senior colleagues for a review.
- Mr M was truthful on every occasion when questioned about the purpose of the payments.

- As I stated in my provisional decision that the trading account value was ‘too good to be true’, this should have immediately flagged for Monzo to provide further effective banking intervention, which it failed to do. It is a major red flag that Mr M doubled his money from his investment and had not received any documentation. The bank ought to have spotted these red flags and intervened, but they failed to provide Mr M with the protection and care he deserves from his bank, who are the professionals.
- Mr M believes that a useful test for a scam loss case such as this, is to reflect on the patterns of activity seen and the values lost in totality. He believes that any normal bank fraud investigator, when applying this test, would be disappointed that the scam was allowed to continue. He expects Monzo to have invested in fraud defence controls that can identify this type of loss as it is happening.
- The onus is on Monzo to identify and prevent the risk of financial harm to their customers, and for their employees to go through extensive contextualized questioning with their customers using the multitude and extensive software and tools at their disposal. This did not happen, and so this is a clear breach of BSI PAS 5.2.1, 5.4.2, 6.2, 7.2.1.1, 7.2.1.2, 7.3, and 8.3.2.

What I’ve decided – and why

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

I appreciate that this complaint concerns a considerable sum of money, and there’s no denying that the circumstances through which Mr M found himself to have lost this money, were extremely callous and cruel. However, I’ve explained that whilst Mr M has been the victim of a cruel scam, that doesn’t mean Monzo is automatically liable for refunding his losses.

It's not in dispute that Monzo ought to be on the lookout for signs that its customer might be at risk of financial harm due to fraud. And if it suspects such a risk is apparent, it ought to, fairly and reasonably, take additional steps, or make additional checks, or provide additional warnings, before processing a payment. I need to consider whether Monzo’s failure to do this, on the balance of probabilities, caused Mr M’s loss. And for the same reasons I’ve set out in my provisional decision, I don’t think it did.

Most of Mr M’s further comments are focused on the nature of the activity being highly unusual and concerning, and that this ought to have prompted an intervention from Monzo. I’ve explained in my provisional decision that I do think Monzo ought to have intervened on the first payment Mr M made, given the information known to it at the time. And, as the payments continued, it ought to have made further enquiries with Mr M about the payments he was making. So this point, as it appears, is not in dispute.

Whilst Mr M has argued the intervention from Monzo ought to have gone beyond what it did in the circumstances, (which I also agreed with in my provisional decision), his further comments do not pay due consideration to whether this would have made a difference to Mr M’s decision to proceed with the payments.

As I’ve set out within my provisional decision, whilst the warnings Monzo gave Mr M at the time did not go as far as I’d have expected them to, considering the nature of the payments and information known to it at the time, this still does not mean it is liable for Mr M’s losses.

I can appreciate and understand why now, with the knowledge that he was being tricked, Mr M feels as though a better warning from a more senior staff member at Monzo would have prevented his losses. However, I’ve considered what happened at the time, when

multiple firms did speak to Mr M about the payments, and it didn't deter Mr M from proceeding. For the reasons I've explained in my provisional decision, the evidence of the previous conversations he had with the various firms involved in the payments he made towards the scam, suggests that Mr M would more likely than not have been determined to carry on making the payments.

I do recognise that the payments Mr M made from his Monzo account, were significant in value and frequency. And Monzo was aware that these payments were for an investment because Mr M confirmed this in an intervention on 3 March 2022. So there's no dispute it ought to have tailored its warnings to cryptocurrency investment scams as the most relevant scam risk.

However, I'm also mindful that Mr M faced restrictions from multiple firms when attempting to make payments to a known cryptocurrency exchange. And such restrictions ought to have given Mr M pause for thought about the risks involving cryptocurrency related transactions.

But Mr M himself confirmed that he too was well aware of the risks of cryptocurrency transactions and had *'100% confidence'* in what he was doing, despite being '*completely new'* to investments. Bank N in particular highlighted to Mr M that it has seen a rise in cryptocurrency scams, but Mr M was '*confident that everything is fine'* and was sure it was not a scam. Whilst there is no dispute that he was honest about the reason for the transactions, he was simply not receptive to the risks being brought to his attention by multiple firms, despite the significant sum of money that he was moving, because he was certain it was a legitimate investment.

Mr M was entirely persuaded that he was making a legitimate investment and would not accept that what he was doing could be part of a sinister attempt to steal his money, despite several firms bringing this possibility to his attention. Even if Monzo had taken further steps to warn him about the risks of cryptocurrency investment scams, I'm still not convinced this would have persuaded Mr M that what he was doing wasn't legitimate. This is because it's also the case that some of the circumstances relevant to the scam Mr M found himself falling victim to, didn't mirror the typical features of a cryptocurrency investment scam. As explained in my provisional decision, Mr M sourced the investment himself, he said he had no dealings with the broker – S – until he attempted to make a withdrawal, he was not coached nor was he told what to say to the bank and he didn't give remote access to his device. Any warnings about these common features of investments scams wouldn't have resonated with him. So, I'm not persuaded Monzo could have reasonably provided a warning that would have resonated enough with Mr M, to the extent needed to break the very high degree of trust Mr M had in the fraudster.

I do acknowledge, as stated in my decision, that Monzo ought to have been concerned by some of the information known to it at the time, such as the apparent returns Mr M had made on his investment being too good to be true. But Mr M too ought to have recognised this. Despite his inexperience in investments, I do think he ought to have appreciated that he'd made a significant return on his investment, in a very short space of time and this was too good to be true. When Mr M set up the payee on his Monzo account, a warning told Mr M to *'Stop if…The offer sounds too good to be true'*. And Bank S warned Mr M *'If the investment returns sound too good to be true – this could be a scam'*. Despite the significant returns Mr M thought he was going to make, neither warning resonated with Mr M.

On 22 March 2022, Monzo warned Mr M *'Legitimate investments aren't arranged over social media or things like WhatsApp'*, which was the method of communication he was speaking to the fraudster over. But again, this didn't resonate with him.

Bank S told Mr M to *'Always research a company and check reviews from other people'* and said, '*All Financial advisors and Financial Institutions should be FCA registered'*. Monzo told him to '*Check out the company…See if they're a legitimate company here. Don't pay unless they're registered with the FCA'*. I'm mindful that neither T nor S were FCA regulated but this also didn't deter Mr M.

And whilst Mr M argued Monzo ought to have stopped and blocked the payments, I still don't agree this means his losses would have been avoided. As I've explained in my provisional decision, the evidence suggests that when Mr M's payments were restricted by a firm, he attempted to send the funds in a different way instead, such as from a different account, to circumvent this. So even if Monzo had taken further steps to intervene and prevent Mr M from proceeding with the payments, the evidence suggests that he more likely than not would have continued with the payments through other channels, and still would have lost this money.

I don't wish to blame Mr M for proceeding with the payments, considering the deceptive techniques used by the fraudster to dupe him into believing he was making a legitimate investment. But I cannot hold Monzo responsible for his loss – in full or in part - unless I think it ought reasonably to have prevented the scam. I'm not persuaded it could have done in these circumstances.

Whilst I know this will be very disappointing for Mr M and I don't doubt that he was taken in by sophisticated fraudsters, I'm afraid that his further comments haven't changed my decision on this complaint. I don't find Monzo responsible for his loss.

My final decision

For the reasons I've explained above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 17 July 2024.

Meghan Gilligan
Ombudsman