

## **The complaint**

Mrs M complains that Monzo Bank Ltd will not refund a transaction she says she did not authorise.

## **What happened**

The events that unfolded are well known to the parties, so I won't detail them again here. Instead, I'll focus on the key points and reasoning behind my final decision.

In summary, a £415 payment left Mrs M's Monzo account on 20 May 2021. It went to Binance, an online cryptocurrency exchange. Shortly afterwards, Mrs M raised this as a fraudulent transaction, claiming that she didn't authorise the payment. She explained to Monzo that she had been contacted by what she thought was a cryptocurrency broker who claimed that bitcoin needed to be paid to her bank account, which she had acquired from a trading account she had previously held. This seemed legitimate and was very convincing. They knew some of her personal details and, although Mrs M was surprised with the windfall of cryptocurrency, she did have a trading account before which made it all possible.

The fraudsters had convinced Mrs M to 'link' her Monzo account to the account where her cryptocurrency possession was being held. To facilitate this, Mrs M revealed details about herself and her Monzo account. She also allowed remote access to her computer.

Monzo investigated and declined to refund the payment, citing that it couldn't agree it was liable to reimburse Mrs M. It maintained this position when Mrs M raised a complaint.

Unhappy with Monzo's response, Mrs M brought the matter to our service. One of our investigators looked into what happened and concluded that Monzo should reimburse Mrs M's loss, which Mrs M agreed with.

Monzo does not agree. It's raised counter arguments that it should not be responsible for Mrs M's account losing this money. Including, that the bank was not the actual point of loss, considering the Binance account the payment went to was set up in Mrs M's name. Because Monzo is not in agreement, the case has been escalated 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 line with the Payment Services Regulations 2017 (PSRs), Mrs M isn't liable for payments she didn't authorise, unless she failed with gross negligence or intent to comply with the terms of the account or keep her personalised security details safe.

Accordingly, I've considered whether Mrs M authorised the payment – and so, whether she made the payment herself by carrying out all the agreed steps or whether she gave someone else permission to do this on her behalf.

*Did Mrs M make the payment herself or give permission for it to be made?*

We know Mrs M's money went to Binance via an online card payment, so I've reviewed what the agreed process was for this transaction to be made. Looking at Monzo's website, Mrs M's 16-digit card number, expiry date, and 3-digit CVC had to be input on Binance's website. Her billing address was also needed.

It's unclear how the fraudsters intercepted Mrs M's personal information, such as her name and email address (which were needed to initially contact her). This may have been from a data leak caused by a prior purchase, or the previous trading account that she held before.

Unfortunately, our service is aware of an array of different scams which involve a consumer being duped into believing they are speaking to a genuine firm or individual, on the basis that their personal information has somehow been captured and used to give a false sense of security. Such fraudulent methods can be referred to as 'phishing', which typically involves a fraudulent message (or email) being sent that is designed to trick an unwitting person into revealing sensitive information. As a bank that tackles all types of fraud for its consumers, Monzo will be familiar with this technique that fraudsters frequently employ.

Suffice to say, it's not uncommon for information to end up in the wrong hands. I'm persuaded that this is what happened to Mrs M – her details and ownership of a previous trading account were used to reassure her that the party she had been contacted by was legitimate. Everything suggests Mrs M was targeted in order to reveal certain details to permit a payment to be instructed from her account.

By her own admission, this social engineering led to Mrs M passing certain information to the fraudsters; her card details included. The sophisticated methods used led to a host of information about Mrs M and her Monzo account being acquired. Indeed, this is reinforced by the fact that the fraudsters had sufficient information about Mrs M to take out unauthorised lending in her name (with other banks/credit providers, which is therefore not subject to this complaint). That so, I have little doubt the required information was within the scammer's gift and was used to set up the payment to Binance.

What's more, I'm satisfied the fraudsters had remote access to Mrs M's computer at home, and Monzo has not presented a compelling argument to make me believe otherwise. Mrs M concedes that she granted this without appreciating the risk of doing so. Without a doubt, with the means to set up a card payment on a merchant's website, and having created a scenario to gain access to Mrs M's computer, it seems highly unlikely that the fraudsters would risk asking Mrs M to carry out the payment herself when inputting the requisite information on Binance's website was possible without her knowledge. Clearly, involving Mrs M in this part of the payment process could have unnecessarily jeopardised the scam.

Monzo has confirmed that once the payment was initiated, a feature of its security measures meant that this transaction needed to be authenticated by using the Monzo application on Mrs M's mobile phone. Mrs M's PIN, face ID, or fingerprint was needed to confirm the payment within the app before it would be let go.

It's unclear exactly what happened in regards to this mobile app authentication. Mrs M has told our service she remembers divulging some sort of code – which might have been linked or produced by her phone. I accept her explanation that the distraction of her screen being controlled and the persuasive coaching of the fraudsters at the time meant she was absentminded when it came to the role the Monzo mobile app had. I've also borne in mind that this mendacious scheme has strong similarities to lots of other scams our service has seen involving unauthorised payments, where consumers are made to be preoccupied and so do not appreciate the instructions a mobile banking app may give.

In any event, even if Mrs M did take certain steps via her Monzo app, I am not persuaded that this means she authorised the payment. In keeping with the PSRs, under these circumstances Mrs M could only be fairly said to have authorised the payment if she consented to it.

As far as I can tell, at no point did Mrs M understand that she was giving the means for a payment to go ahead. She didn't disclose her details and card information to make a payment. Conversely, everything she did was to receive a payment *into* her account. The purpose for giving her details and following the instruction of the fraudsters was to only link accounts together and not to transmit money away. I therefore cannot safely conclude that her actions amounted to giving her consent for this disputed transaction.

So, overall, I'm not persuaded that Mrs M took all of the agreed steps to make the payment herself nor did she give permission for someone else to on her behalf. It follows that I find this to be an unauthorised payment.

### Considering intent and gross negligence

Monzo could fairly hold Mrs M liable for an unauthorised payment if she failed with intent or gross negligence to comply with the terms of her account or keep her personalised security details safe.

All things considered, I'm not persuaded Mrs M intentionally failed to keep her details safe – she genuinely believed what she was doing was enabling her to receive a windfall, by connecting her Monzo account to where the supposed cryptocurrency was being held.

I'm also not convinced Mrs M failed with gross negligence. She had held a trading account in recent months, which not everyone would have experienced. This made it possible for her to have prematurely closed her holdings without realising she had made a profit. Not least, given the speculative nature of the cryptocurrency market, where considerable earnings can be made in short spaces of time (and with no real exact science or methodology).

I can see why this, together with her personal details being used in an introductory email, led her to believe she was talking to a credible party. Like most people, Mrs M is not an expert in cryptocurrency or particularly savvy with releasing investments. Without some sort of intel about her previous trading experience, I find it hard to see how else someone could use this fact to build trust. Especially, given the professional look of the email that was sent.

So, when someone in a position to understand her (albeit limited) history of trading got in touch, equipped with some of her personal details, I can see why Mrs M believed she was talking to a legitimate outfit.

I've already concluded the fraudsters gained access to Mrs M's computer. I have to bear in mind that Mrs M was, by her own admission, inexperienced with investing in cryptocurrency. Given the complexity of this investment arena, I can understand how the clever techniques of the fraudsters made her believe she needed to 'link' a crypto account to a normal bank account, which would differ from a bank-to-bank payment. Consequently, I don't think Mrs M was significantly careless in allowing this to happen.

As I've mentioned, it's not clear exactly what security details Mrs M shared in respect of her mobile banking app with Monzo. However, even if she did share her PIN or confirm her identity via biometrics, I'm not convinced this means she failed with gross negligence.

Monzo may claim it's unrealistic for a broker or representative of a cryptocurrency firm to ask for such steps to be taken. But this ignores the context of what happened – Mrs M believed she was talking with a trusted professional, one which had information about her prior trading that would otherwise be unexplained, and that was acting in her best interests by following the legal process of settling assets held in her name. In that light, I can see how someone might be duped into believing everything was above board and part of due process.

Besides, mere negligence isn't the benchmark. What I need to consider is whether Mrs M's actions fell so far below what a reasonable person would've done, to the extent that she failed with *gross negligence*. For the reasons I've set out, I do not consider she did.

### *Binance account*

Finally, I turn to the submissions Monzo has made in respect of the Binance account being in Mrs M's name. In summary, the bank claims that it should not be held liable for the payment because Mrs M's loss occurred when the funds left the Binance account, and not her Monzo one.

There's no question the Binance account belonged to Mrs M. It is arguable that, strictly speaking, she still had possession of the £415 when it was held with Binance, before it was transferred away to an account owned by the fraudsters (which cannot be traced due to the nature of cryptocurrency). To that end, I can appreciate Monzo's contention.

Still, I've determined that Mrs M did not knowingly make the payment, meaning that she would not have comprehended the whereabouts of her funds once they left Monzo. In practice, custody of the money only would remain with Mrs M if she was able to actually access it, i.e. by having the security credentials to get into her Binance account. Or, at the very least, understand where her money was. On both these fronts, Mrs M could not make sense of where or how to get to her stolen money.

Moreover, I find the degree of control to be material to whether the funds were still within Mrs M's gift, in between leaving her account with the bank and being irretrievably lost to the fraudsters. I've already described the control the fraudsters had of Mrs M's computer, armed with a host of her personal information and account details. Mrs M has always maintained that she didn't understand that the Binance account was opened, not to mention that it was created in her name. I find her version of events plausible and there's a lack of persuasive evidence to make me think that Mrs M realised that the Binance account was set up for money to be paid there from her Monzo account.

According to Binance's website, the verification of a new user's identity requires documents and information in order to register a new account. Most (if not all) of this information I'm satisfied the fraudsters possessed, and there appears to have been nothing Binance would have requested that required Mrs M to speak to them personally. Again, we know the fraudsters had enough to take out a loan in Mrs M's name without her permission – which would be all that is required to also create a trading account. On top of that, the speed of the scam was swift, meaning that there was little chance for Mrs M to take stock of what was happening.

I'm therefore satisfied that Mrs M had no ability, or at least restricted ability, to access the funds in the Binance account. Although this intermediary account may have been in her name (and therefore strictly in her possession), because she was unaware of it and had no access to the login credentials, it's unfair to find that it was Mrs M's action or inaction that was the true cause of her loss.

In other words, because I'm persuaded Mrs M could not access the funds with Binance before it was too late, I cannot reasonably say she carried out the independent act of sending money onwards to the fraudsters. Because of this, I do not find it fair for the presence of the Binance account to strip away Monzo's liability for Mrs M's loss.

It follows Mrs M isn't liable for the transaction and Monzo need to put things right – by refunding her losses from this unauthorised transaction alongside interest to compensate her for the time she's been out of pocket.

### **My final decision**

For the reasons given above, my final decision is to uphold Mrs M's complaint and I require Monzo Bank Ltd to:

- Pay Mrs M the total of the unauthorised transaction (£415) less any amount already returned.
- Pay 8% simple interest per year on this amount, from the date of the unauthorised transaction to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 23 December 2022.

Matthew Belcher  
**Ombudsman**