

The complaint

Mr S is unhappy because Monzo Bank Ltd (Monzo) did not reimburse the money he transferred to a fraudster.

What happened

What Mr S says

Mr S says that on 3 June 2020 he provided details of his account with another bank in response to an email he thought he'd received from HMRC. I'll refer to the other bank as Bank A. That evening Mr S realised the email he had responded to wasn't genuine and called Bank A to explain what had happened and asked for his account to be closed. Mr S also says he asked for a new account to be opened. Bank A cancelled Mr S's card and advised him to change his password and, Mr S says, reassured him that if he took these steps his funds would be safe.

A few days later Mr S received a call from someone who claimed to be from Bank A. Mr S didn't know it at the time, but the caller was a fraudster. He explained to Mr S that a direct debit had been set up from his account with Bank A and a payment attempted, so he needed to change his account. Mr S asked how he could verify the caller was from Bank A and was told to hang up and check the caller ID, which Mr S did. He found that the number he'd been called from was a help desk number for Bank A.

The caller told Mr S that he needed to transfer £25,000 to create a new account. As his account at Bank A had been blocked the fraudster told Mr S that he couldn't set up a new payee so needed to pay an existing payee first and then transfer the funds to the new account. There were daily limits to the amount he could transfer from his account with Bank A, so Mr S moved £24,541.39 in ten payments over two days from his account with Bank A to his Monzo account. Mr S then made the following payments from his Monzo account to a new account the fraudster provided him with details of.

Date	Amount
08/06/20	£10,000
09/06/20	£10,000
10/06/20	£5,000
Total	£25,000

This new account wasn't with Bank A or Monzo, but Mr S was told that all banks work together to combat fraud.

Mr S remembers seeing warnings when he made the payments but as he was persuaded he was dealing with Bank A and following its instructions he went ahead with the payments.

Mr S realised he was the victim of a scam when his new card arrived from Bank A. The account details were the same as previously showing that a new account hadn't been set up. He called Monzo to report the scam on 30 June 2020.

What Monzo say

Monzo isn't a signatory of the Lending Standards Board Contingent Reimbursement Model CRM Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances, but has agreed to apply its principles. Monzo say exceptions to reimbursement apply in this case. It says that Mr S ignored an effective warning when he made the payments and that Mr S didn't have a reasonable basis for believing the person he transacted with was legitimate or was providing a legitimate service.

Monzo contacted the bank that received Mr S's funds to try to recover them but was unable to recover any funds.

Our investigation so far

The investigator who considered this complaint recommended that Monzo reimburse Mr S's full loss of £25,000 together with interest. He said that the warning Monzo gave Mr S when he made the first payment wasn't effective, primarily because it didn't bring to life common features of safe account scams like number spoofing. The investigator also said Mr S had a reasonable basis for believing he was making a genuine payment because the call wasn't unexpected given the phishing email he'd contacted Bank A about, the fact the number was spoofed was persuasive and the new account was in Mr S's name. Also, the investigator felt that Monzo could have prevented the scam from taking place as the payment requests Mr S made were unusual and out of character.

Mr S agreed with the investigator's findings but Monzo didn't. In summary, it said:

- Monzo did everything it could to warn Mr S before he made the payments. An effective warning was provided when the first payment was made which clearly stated that other banks wouldn't ask a customer to transfer funds from their Monzo account. And it didn't need to go into detail about number spoofing as if it did so, the warning wouldn't be understandable. Overall, Mr S should have done more and contacted Monzo directly.
- Ms S received no match confirmation of payee results for all three payments which clearly warned that if he continued with the payments it was almost impossible for Monzo to recover the funds.
- The payments were made over several days, so Mr S had the opportunity to make further checks. This also means Mr S's funds weren't protected as quickly as they could have been, which should have caused concern.
- Banks don't work together to combat fraud in the way the fraudster told Mr S they do, and Mr S should have been aware of this as his apps for different banks varied.
- Bank A should bear some responsibility for Mr S's loss because it didn't provide appropriate scam education. Mr S noted that had Bank A warned him about number spoofing the scam wouldn't have happened.
- The CRM Code and PSRs don't require Monzo to prevent the scam payment.

I reviewed Mr S's complaint and issued my provisional decision on 28 June 2022. In my provisional decision I said:

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

In deciding what's fair and reasonable in all the circumstances of a complaint, 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.

When thinking about what is fair and reasonable in this case, I've considered whether Monzo should have reimbursed Mr S under the provisions of the CRM Code and whether it ought to have done more to protect him from the possibility of financial harm from fraud.

There's no dispute here that Mr S was tricked into making the payments. But this isn't enough for Mr S to receive a full refund of the money under the CRM Code. The Code places a level of care on Mr S too.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning
- The customer made payments without having a reasonable basis for believing that: the payee was the person the Customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate
- The customer has been grossly negligent

*The two further exceptions outlined in the CRM Code do not apply to this case.

I have carefully considered Monzo's representations about the warning it gave and whether Mr S had a reasonable basis for believing the transactions to be genuine. But they do not persuade me to reach a different view. In particular, I am not persuaded that Mr S failed to take the requisite level of care required for Monzo to choose not to reimburse under the terms of the CRM Code.

Did Monzo provide Mr S with an effective warning/warnings?

The CRM Code sets out standards for firms – that is, what firms are expected to do to protect customers from the risk of fraud and scams. Where those standards are not met, the firm may be expected to compensate its customer. One of those requirements is that, where the firm has (or should have) identified that its customer is at risk from a scam, it should provide that customer with an Effective Warning, within the meaning of the CRM code.

Monzo has provided evidence of what happened when Mr S set up a new payee to make the first payment. He was provided with a confirmation of payee no match that said,

"The details you entered don't match the account you're sending money to.

Please double-check who you're sending money to and cancel this payment if you think someone might be trying to scam you."

Mr S clicked to continue and would have seen a screen that said,

"Could someone be trying to scam you?"

If you're not sure, cancel this payment.

Once you've made a payment, it's almost impossible for us to get the money back."

Monzo then provided a warning to Mr S based on his chosen payment reason of "Transfer to a 'safe account' and saw a red screen that said,

“Stop, don’t pay

It’s very likely this is a scam”.

The following wording was in a box underneath.

“Remember:

*X Monzo will never call you without arranging by email or in-app chat first
X Other banks will never ask you to move money out of your Monzo account”.*

The warning then advises customers to call the bank on the number on the back of the card and provides a number for Monzo. A customer is required to tick a box to say that they have read all the information and want to continue. Underneath this, two boxes appear. One says, “Stop and report” and the other, “Confirm payment”.

Mr S says he doesn’t remember seeing the warning, although Monzo’s records show he viewed it for over twenty seconds before moving on.

For a warning to be effective under the provisions of the CRM Code it needs to be understandable, clear, impactful, timely and specific. The warning Monzo provided in respect of the first payment (together with the confirmation of payee no match) includes a number of important details. For example:

- It says this is very likely to be a scam;*
- It says that other banks won’t ask a customer to move funds out of their Monzo account;*
- The warning is bold and written on a red screen to draw attention to it;*
- It advises Mr S to call the Monzo number on the back of his card;*
- It warns Mr S that if he went ahead with the payment, he may not be able to get his money back.*

But I’m satisfied that the requirements of the effective warning exception were not met. I say this because I consider the warning lacks impact. An effective warning should reduce the likelihood of a scam succeeding. In this case, the warning doesn’t explain the common features of this type of scam or bring to life what a ‘safe account’ scam is. For example, it doesn’t refer to the fact fraudsters pose as banks and apply pressure to convince their victims to urgently move their money to a safe account. The warning also doesn’t mention a powerful feature of this type of scam – number spoofing. Monzo has said that if it included this detail it would mean that its warning wouldn’t be understandable, but I don’t agree.

Monzo has said that Bank A should bear some responsibility and referred to Mr S’s comment that if Bank A had advised him about number spoofing, he wouldn’t have fallen victim to this scam. I believe this shows the importance of a warning bringing to life common features of a scam so that it resonates with a customer.

Overall, while I appreciate that Monzo tried to give Mr S a warning in respect of the first payment, I’m not persuaded the warning could be considered as effective under the terms of the CRM Code.

Monzo didn’t provide a warning for the second and third payments. Monzo says it provided an effective warning in respect of the first payment and this should have been enough to prevent Mr S from making all payments. I don’t agree. To be effective, a warning needs to be timely. This means it needs to be given at a point in the payment journey where it is most

likely to have an impact on a customer's decision-making. I'm not persuaded that a warning not given in the payment journey, but one or two days before can be effective.

As Monzo didn't meet the standards required of it under the CRM Code it is liable for 50% of Mr S's losses.

Did Mr S have a reasonable basis for believing what the scammers told him?

Taking into account all of the circumstances of this case, including the characteristics of Mr S and the complexity of the scam, I think the concerns Monzo has raised about the legitimacy of the transactions Mr S made are enough to support its position that he failed to meet his requisite level of care under the CRM Code for the payments he made. I don't think he had a reasonable basis for believing the person he transacted with was legitimate. In reaching this conclusion I've taken the following into account:

- *Mr S hasn't provided an explanation as to why he considered it plausible that he needed to transfer £25,000 to a new account to activate it. Bank accounts can be opened with very small amounts.*
- *Mr S thought an agent of Bank A told him he needed to transfer funds to a 'safe account'. But he didn't question why daily transfer limits couldn't be overridden by the bank and so he needed to make multiple transfers to his Monzo account before he could move funds to a 'safe account'.*
- *On 8 June Mr S spoke to the scammer at 12.54 (for 18 minutes) and 13.14 for 30 minutes. He transferred funds at 18.30. He has explained that given the nature of his job he was unable to take more time away and so transferred funds at the earliest opportunity he could. Given this, it's clear that the scammer wasn't on the phone to Mr S or putting pressure on him at the time he made the first payment. Future payments were made the following day and the day after that. So I consider that Mr S had time to consider what the scammer had told him and take steps to check, for example, whether a direct debit had been set up from his account with Bank A or to call Monzo before making any payments.*
- *The account Mr S transferred his funds to wasn't with Bank A or Monzo. Mr S has explained that he thought banks worked together to prevent fraud, but I consider this fact, combined with the other factors I've discussed, should have been a red flag to Mr S that something wasn't right. I find it unlikely that Bank A would seek to open a new account for Mr S with a different bank.*
- *For each payment he made Mr S was provided with a confirmation of payee no match result, showing that the account he was transferring the funds to wasn't in his name. I find it surprising that Mr S would continue with the payment after being presented with a warning in these terms and believe Mr S didn't have a reasonable basis for believing he was paying the person he believed he was paying.*
- *Whilst I don't consider the warning given to Mr S when he made the first payment was effective, it does have an impact on whether he had a reasonable basis for believing he was making a genuine payment. The warning said that other banks won't ask a customer to move funds out of their Monzo account and if they did it might not be possible to recover them. Mr S thought he had been asked by another bank to move funds from his Monzo account and so I consider the warning should have resonated with him.*

It's important to note that it's the combination of the factors I have listed above that have led me to the conclusion that Mr S didn't meet the standard required of him by the CRM Code to receive a full refund.

This means that Monzo isn't responsible for the remaining 50% of Mr S's loss.

I've also considered whether Monzo did enough to protect Mr S in this case. I consider that the first payment of £10,000 was unusual and out of character given previous activity on Mr S's account and so Monzo should have intervened before making the payment. It was to a new payee and was for a significantly higher amount than previous payments. Had Monzo have asked Mr S some questions about the payment I believe the scam would have unravelled quickly when Mr S explained he was moving funds to a safe account.

I'm also mindful of the fact that, in order to see this warning, Mr S needed to categorise this as a payment to a 'safe account'. There's no such thing as a safe account outside the realm of fraud and scams. I think that once Monzo gathered this information from Mr S, it should have recognised that it was highly likely that he was making the payment in connection with a scam and prevented the payment from being made. Because I think Monzo could've done more to protect Mr S from the scam by recognising that it was a safe account scam, I think it should fairly and reasonably refund 50% of his losses in connection with that scam. I've awarded 50% of his loss because I think Mr S should also bear some responsibility for the loss he suffered – for the same reasons I've set out above.

The significance of my decision that Monzo could have prevented the scam is that it should pay interest from the date of each payment rather than from the date it decided not to reimburse Mr S under the CRM Code.

The money was taken from Mr S's current account with Bank A. It is not clear how Mr S would have used the money if Monzo had refunded it when it should have done, so Monzo should also pay interest on the money it should have refunded at 8% simple per year from the date of payment to the date of settlement.

Recovery of funds

Mr S reported his loss to Monzo at the end of June 2020. I've seen evidence which shows that Monzo contacted the bank his funds were sent to on 5 July 2020. Whilst I'd expect this to have happened sooner, it wouldn't have made a difference in this case. This is because the evidence I have seen from the bank that received Mr S's funds shows they were used up very quickly. So by the time the scam was reported, no funds remained.

Mr S accepted my provisional decision but also said that Monzo should at least have had concerns about money laundering as the payments were made within 24 hours.

Monzo didn't accept what I said. In summary, Monzo said:

- It disagrees with my conclusion that an effective warning wasn't given. Monzo said it is best placed to decide the relevant information to give to customers that doesn't lead to information overload. Monzo also referred to the Code definition of impactful in respect of an effective warning.
- Monzo said the "first" point of the CRM Code is that it shouldn't negatively affect legitimate payment journeys. So once it has sent a warning when a new payee is set up it doesn't continue to send warnings unless anything changes as, to do so, would limit the impact of the warning.
- Monzo pointed out that customers often choose an incorrect payment reason to get through the process quickly, including the safe account reason. If it froze accounts and attempted to contact customers each time that happened legitimate payments would be negatively affected.
-

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 in all the circumstances of a complaint, 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.

After reviewing the responses I have received from both parties, I have reached the same overall conclusion as I set out in my provisional decision and for the same reasons.

Although the warning Monzo gave when Mr S made the first payment included some good features, I'm still not persuaded it was effective under the CRM Code. I recognise there is a balance to be struck and a warning may lose impact if it's too long. But the warning Monzo gave to Mr S didn't explain common features of safe account scams like this one to enable Mr S to recognise that he was falling victim to a scam. So I don't think the warning positively impacted Mr S's decision making in a manner that reduced the likelihood of this type of scam happening.

As I've concluded that the warning Monzo gave in respect of the first payment wasn't effective (and no further warnings were given to Mr S when he made subsequent payments), it follows that I'm also not persuaded Monzo met its obligations when the second and third payments were made.

Monzo has said it's best placed to decide what to include in a warning. But that's not what I'm here to decide. My role is to consider whether Mr S should receive a refund under the CRM Code and to decide this I need to consider each party's obligations under it.

In its response to my provisional decision Monzo has referred to one of the overarching principles of the CRM Code – to minimise disruption to legitimate payment journeys. There are three overarching principles though, so I need to consider them as a whole. The other two are to reduce the occurrence of APP scams and to increase the proportion of customers protected from the impact of APP scams – both through reimbursement and the reduction of APP scams.

Monzo also said in its response to my provisional decision that customers choose the wrong payment reason and so to block every payment when a customer chooses paying a safe account would negatively impact legitimate payments. I accept that customers don't always get the payment reason right but, as I said in my provisional decision, there is no such thing as a safe account outside the world of fraud and scams. Given this, I consider that Monzo should fairly and reasonably have contacted Mr S when he made an out of character transaction and used the safe account payment reason.

Overall, I think both parties ought to share responsibility for the loss in this case.

My final decision

I require Monzo Bank Ltd to:

- Refund Mr S 50% of his loss (£12,500) and;
- Pay interest on 50% of the loss, at the rate of 8% simple from the date of each payment until the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 11 August 2022.

Jay Hadfield
Ombudsman