

The complaint

Mr Z is unhappy that Monzo Bank Ltd won't refund him money that he lost as a result of fraud.

What happened

The details of this case have been clearly set out by our investigator. As such, the facts are well-known to both parties, so I don't need to repeat them at length here.

In summary, Mr Z fell victim to an impersonation/ safe account scam and transferred £4,400 in December 2020.

Mr Z says on 17 December 2020, he received a call from someone purporting to be from another bank, who he held an account with. He said he was told his account had been compromised with unusual activity. Mr Z recollects going through security on this call – where he was asked to confirm his date of birth, address and full name. He was asked to confirm if he'd made specific transactions on his account and after being placed on hold, he says he was told all seemed fine.

He recollects around an hour later he received another call from someone claiming to be from Monzo. Unbeknown to Mr Z, he was in fact speaking with a fraudster. Mr Z said the caller knew his name and went on to ask him security questions which he answered. Mr Z was told his account had been compromised. He was told his account had been blocked but to make sure his money was safe he needed to send his funds to a new account which would be activated once he was sent a new card.

Mr Z was given the new account details and he proceeded to send £4,400 to this account.

Mr Z says he was panicked on receiving this second call. He was worried about his Monzo account as this held his savings. The day before, on 16 December 2020, Mr Z requested a withdrawal from his savings account with Monzo to his current account. Mr Z said this was intended to be sent to a close family member to help make a payment for a specific purpose.

It was later the same day that Mr Z said he started to worry and question what had happened. He said on thinking back he realised the bank wouldn't ask him to move his money to a safe account. He adds that he checked the account details he sent his money to and saw it was not an account with Monzo. It was at this point, Mr Z realised he'd been the victim of a scam.

That evening Mr Z contacted Monzo on the in-app chat function to raise the scam claim. Based on the initial information, it appears Monzo asked questions in relation to an account takeover. But after asking further questions, it was the early hours of 18 December 2020 that Monzo recognised he'd fallen victim to a scam. Monzo reached out to the receiving bank to see if any funds could be recovered. Unfortunately, it received a response to say no funds remained.

Monzo responded to Mr Z's claim and said it couldn't refund the money he'd lost. Monzo said it felt Mr Z didn't take enough steps to check who he was paying and for what.

Unhappy, Mr Z brought his complaint to our service. One of our Investigators considered the evidence provided by both parties but concluded Monzo should have fully reimbursed him under the Contingent Reimbursement Model (the CRM Code).

In summary:

- She said the warning provided prior to the payment didn't meet the definition of an 'effective warning' as set out in the CRM Code. When considering the warning Monzo said Mr Z would've seen had he selected the correct reason for transferring the money, she also didn't think this warning was effective even if he'd seen it. So, she wasn't satisfied Monzo had established Mr Z shouldn't be reimbursed on the basis that he ignored an effective warning.
- She also didn't think Monzo had been able to establish Mr Z didn't have a reasonable basis for believing that he was making a legitimate payment to his own, newly set up Monzo account.

For the above reasons, the Investigator found that Mr Z had met his requisite level of care. Therefore, Monzo were unable to decline reimbursement under the CRM Code. For completeness, our Investigator also considered the payment Mr Z made to be an out of character payment for his account. She felt Monzo should have stopped and questioned the payment and if it had done so, the loss could've been prevented.

Monzo disagreed with the Investigator's assessment. Monzo remained of the opinion that Mr Z isn't entitled to a refund under the CRM Code because:

- Mr Z was shown a 'high friction' warning at the time the payment was made. It considers Mr Z ignored the warnings which it feels shows Mr Z was grossly negligent.
- It added Mr Z had a confirmation of payee (CoP) mismatch which meant he would've had a message to check who he was paying.

Our Investigator's position having considered Monzo's further points remained the same. As Monzo disagreed with the Investigator's assessment, the complaint has been passed to me to make a final decision.

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.

In broad terms, the starting position is that a payment service provider is expected to process payments that its customer authorises, in accordance with the Payment Services Regulations 2017 (PSRs), which apply to this complaint, and account terms and conditions. But where a customer made a payment as a result of the actions of a scammer, it may sometimes be fair and reasonable for a payment service provider to reimburse its customer, even though the payment was authorised.

In considering this, I have taken account of whether Monzo ought to have reimbursed Mr Z under the provisions of the CRM code, and whether it ought to have done more to protect him from potential financial harm from fraud. The Code also places a level of care on Mr Z, and so I have considered whether he met this.

The CRM Code

Monzo has agreed to adhere to the provisions of the Lending Standards Board Contingent Reimbursement Model Code (the CRM Code) which requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances.

It is for Monzo to establish that a customer failed to meet their requisite level of care under one or more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- The customer ignored an effective warning in relation to the payment being made.
- The customer made the payment without 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

There are further exceptions within the CRM Code, but they do not apply in this case.

Monzo has argued that Mr Z has been grossly negligent. It says that he didn't have reasonable grounds to believe that the reason to move the money was genuine. This is because the call length was too brief and wouldn't have built up enough of a relationship to make him believe this was a legitimate call.

But I don't think Monzo has been able to establish that it may choose to not fully reimburse the payment Mr Z made under the terms of the CRM Code. I'm not persuaded any of the listed exceptions to reimbursement under the provisions of the CRM Code apply in the circumstances of this case.

Was there an effective warning?

The CRM Code sets out that an effective warning should enable a customer to understand what actions they need to take to address risk and the consequences of not doing so. As a minimum the CRM Code sets out that an effective warning should be understandable, clear, impactful, timely and specific.

I've looked carefully at Monzo's 'high friction' warning screens that it says would have been shown to Mr Z at the time he was making the payment to decide whether he ignored an effective warning.

Monzo say Mr Z confirmed that he didn't fully read the warning due to being pressured and, it also says he didn't select the correct reason for making the payment. Mr Z told our Investigator that whilst he wasn't told by the fraudster what to select, he felt selecting 'something else' was the best option. He also said he always uses the option 'something else' when making a payment. Whilst Mr Z might wish to give this more consideration in the

future when making payments, I can't say this in and of itself is enough to show that Mr Z seriously disregarded an obvious risk and was grossly negligent.

By selecting the payment purpose as 'something else', this does mean that Mr Z did not see the warning most relevant to his circumstances. But in any event, even if Mr Z had seen the warning in full, I'm not satisfied that the requirements of the effective warning exception were met in the circumstances of this case. I'll explain why.

The information that was presented to Mr Z at the top of the "something else" warning prompted him to think about whether a deal seemed too good to be true or not. This wouldn't have resonated with Mr Z at the time as it did not apply to the particular scam, he was falling victim to. I do note the 'something else' warning also says that the name and phone number of legitimate companies can be 'spoofed' or faked. Whilst Mr Z has said he doesn't recall seeing this particular part of the warning because he was stressed, I'm not persuaded the warning would reasonably have prompted Mr Z to reconsider the payment as a result.

In short, I don't think the information in the warning brings to life what safe account scams look and feel like. The warning doesn't explain that fraudsters pose as banks and other genuine companies and apply pressure to convince their victims that the money in their account is at risk if they don't move them to a safe account. Nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be. For example, it doesn't explain that fraudsters often know personal information and mimic the bank's processes as a method to convince them that they are genuine.

I'm also mindful that in order for the warning to meet the CRM Code's minimum requirements of an 'effective warning' it should clearly set out the consequences of continuing with an irrevocable payment. I don't find the warning explains this or makes this sufficiently clear.

Overall, I don't consider the warning given was an effective warning as defined by the CRM Code. It follows that Monzo has not established it can fairly apply the exception to reimbursement relating to 'ignoring an effective warning'.

Did Mr Z make the payment without a reasonable basis for belief?

I have also carefully thought about Monzo's representations about whether Mr Z had a reasonable basis for belief. But they do not persuade me to reach a different view. I say that because:

- Prior to the scam call, Mr Z had received a call from someone claiming to be from another bank (who he held an account with). Mr Z has said this earlier call was similar to previous calls he'd received from this bank about activity on his account – he was asked security questions and asked about specific transactions on that account. Mr Z also recollects being placed on hold and hearing 'hold music' – mimicking a bank's processes in this call. When Mr Z received the second call, he's explained he was again asked his name and asked to answer security questions. I appreciate Monzo feels Mr Z didn't do enough to verify the person he was speaking with was from the bank. But in light that Mr Z's experience was similar in both calls, I think this likely would've added to his belief that this was a legitimate call with his bank.
- I'm also mindful that in these types of scams, they are designed to generate and instil panic in consumers. Taking into account Mr Z had already received a call in relation to another of his accounts being compromised that day, I think the second call would've caused Mr Z concern and added to his belief that his accounts were/might

be compromised. Mr Z, himself, has said because of the first call he panicked and thought his money was at risk. I don't find this unreasonable in the circumstances.

- Mr Z made a withdrawal from his Monzo saving account to his current account the day before the scam call. This meant at the time of the scam call from Monzo, Mr Z was mindful of the higher balance in his account. Because of this, I don't think it unreasonable that Mr Z felt his Monzo account was more likely to be at risk of fraud and that this would've added to him believing his account may have been compromised. I'm persuaded his awareness of the savings he'd recently moved into his account, likely would've added to his panic and his urgency to protect his money.
- I note Monzo's concerns about the duration of the call between the fraudster and Mr Z – that the length of the call was brief and so it doesn't think there would've been enough time to have built up a relationship to believe this was a legitimate call. The duration of the call was under 20 minutes and the payment was made in under 10 minutes into the call. I've carefully considered this. However, I'm mindful that these comments/findings are made with the benefit of hindsight. Mr Z had received two calls in the same day telling him that his accounts might be at risk. I have to keep in mind that the convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day they might not otherwise take. In the moment and amongst the panic that his money might be at risk, I don't think it unreasonable that Mr Z believed he was speaking with his genuine bank.
- The fraudster told Mr Z that he was moving his money to another Monzo account in his name which would be activated once he received the new card. He was asked to put his name as the payment instruction and to use his mother's maiden name as the reference. Mr Z has told us that this was one of the answers to his security questions on his account, which further persuaded him that he was speaking with the genuine Monzo. Monzo has said when Mr Z entered the payee details, he was shown a CoP warning that said the payment details were a mismatch. That he would've been given a message to check who he was paying. The evidence provided, indicates CoP was not supported by the receiving bank. Within Monzo's submissions it said Mr Z likely would've seen a message stating it couldn't match the account. Monzo feel Mr Z should've attempted to check the account details. I've thought carefully about this point, but I don't consider a message stating it could not match the account details to be the same as a messaging telling Mr Z that the account details 'did not match'. In the absence of any other factors, such as, being asked to make a payment to an account in a different name, I'm not persuaded Mr Z missed an obvious red flag here.
- The evidence provided by Mr Z shows the number he was called from when making the payment to the fraudster was a spoofed number for the other bank, he has an account with and not Monzo. Mr Z has said he didn't check the number at the time of the call but later that day when he started to question what had happened. Mr Z isn't clear how this is the case and maintains at the time of the call he believed he was speaking with Monzo. I accept that this might have been a factor that ought to have given Mr Z a pause for thought, but as I've said above, these types of scam can be convincing in nature and can often impact a person's thought process. It follows that I don't think this aspect in isolation is enough to say Mr Z didn't have a reasonable basis for believing he was speaking with his genuine bank when combined with the aspects I've already set out above.

When weighing everything up, on balance, I'm not persuaded Monzo has established Mr Z didn't have a reasonable basis for belief that he was making a legitimate payment. It follows

that I'm not persuaded the exception for reasonable basis for belief applies to the payment Mr Z authorised and that Monzo can choose not to reimburse him.

Has Mr Z been grossly negligent?

Monzo considered Mr Z was grossly negligent. A finding of gross negligence would require a very significant degree of carelessness on Mr Z's part. Having considered everything I've seen and been told; I'm not satisfied Mr Z's actions or inaction in this case goes far enough to meet that very high bar. I don't think he disregarded or acted with indifference towards the risk of his bank account being compromised and money being stolen. Mr Z believed he was speaking with his bank and that he had to move his money to a safe account in order to protect his funds. For the reasons I've explained above, I don't think Mr Z's belief was unreasonable in the circumstances.

Could Monzo have done more to prevent the scam?

I'm mindful that when Mr Z made this payment, Monzo should fairly and reasonably 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).

Our Investigator, having reviewed Mr Z's bank statements considered the payment of £4,400 to be out of character for his account and noted the payment cleared the majority of the available balance. Because of this, she thought Monzo ought to have got in touch and asked Mr Z about the payment. Had it done so, she thought the scam could've been prevented.

I've thought carefully about this point. The effect of making a finding on this point is limited, given I'm upholding the complaint. It primarily affects whether Monzo should pay interest on an award. In this case, Mr Z told us he moved the money from his savings account with Monzo into his Monzo current account as he was intending to send the money to a close family member. So, had Mr Z not lost this money as part of the scam – the money still would have left his account as he intended to make the payment to his family member. With this in mind, I don't make an interest award recommendation on the money to be refunded to Mr Z. And because of this, I don't think I need to make a finding as to whether Monzo should have intervened to stop this payment, as I'm satisfied it should reimburse Mr Z under the provisions of the CRM Code.

Recovery of funds

Our Investigator, as part of her investigation into this complaint, contacted the receiving bank. Following this, she explained £34.23 remained in the receiving account which should've been returned to Mr Z. £2.55 of this amount was returned to Monzo. Monzo refunded this amount on 1 November 2022. Our Investigator arranged for the difference of £31.68 to be refunded to Mr Z directly by the receiving bank, which has now been paid to him.

My final decision

For the reasons I've given above, I uphold this complaint and direct Monzo Bank Ltd to;

- Reimburse Mr Z the money he lost as part of this scam - £4,400 minus the amount recovered of £2.55 and the subsequent further payment of £31.68 which has been paid directly to Mr Z by the receiving bank.

- There was a delay in returning the £2.55 to Mr Z. So Monzo should pay 8% simple interest on this amount from the date it ought to have been refunded to Mr Z to the date it was paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr Z to accept or reject my decision before 2 December 2022.

Staci Rowland
Ombudsman