DRN-3396803

## The complaint

Mr Z complains that Monzo Bank Ltd ("Monzo") won't refund him the money he lost as the result of a scam.

## What happened

The details of this complaint are well known to both parties so I won't go into too much detail here. However, in summary, Mr Z was the victim of a scam. He received a call from someone who said they were calling from his broadband internet provider but who we now know to be a fraudster. The fraudster told him there were issues with his broadband that meant hackers might be able to use his IP address to access his bank accounts.

Mr Z has told us that the person he spoke to went through some basic verification questions with him and then asked him to install team viewer on both his laptop and mobile phone. They then directed him to a website which appeared to show hackers attempting to gain access to his online accounts. Mr Z was directed to log in to his online bank account (held with a third-party bank). Mr Z says he was shown two transactions had debited his account which he didn't recognise. We now know that the fraudsters were able to manipulate what Mr Z saw on screen to give him the impression that hackers had access to his bank accounts and were making transactions. But at the time, Mr Z thought these transactions were genuine and he's told us that this persuaded him his money was at risk of being stolen.

The fraudster then told Mr Z that the only way to keep all of his accounts secure was to make a series of payments to a 'virtual account' which would ultimately allow the hackers to be caught. Mr Z initially declined to make any payments as he didn't want to use his own funds but was reassured when the fraudster told him that they had a 'special fund' to use in these circumstances. The fraudsters told Mr Z that they would put money into his account in order to make the payments and he wouldn't have to use any of his own money.

Mr Z said the fraudster was then able to show him that £9,000 had been transferred into his account - he saw his balance increase on screen. Again, with the benefit of hindsight, we know that Mr Z's screen was being manipulated by the fraudsters to give the impression that funds had been paid into his account. In reality, this wasn't true, and the only funds available in Mr Z's account were his own.

Mr Z has told us that the fraudster then transferred £8,900 from his bank account to his Monzo account. They then transferred the same amount from his Monzo account to another Monzo account that wasn't in his name. The fraudster then told Mr Z that as a result of the transfer, a hacker had been caught and Mr Z was shown a picture of the supposed hacker on a fake Interpol page.

The fraudster then told Mr Z that a second hacker had to be caught. He was told that a further £2,500 had been paid into his account to allow him to make some further transfers

to catch them. The fraudster then transferred this £2,500 from his bank account to his Monzo account. But this time, Mr Z was told that he would need to set up an account with a third-party money remittance service so the payment could be transferred out of his Monzo account to India – where the hacker was based. For ease, throughout this decision, I'll refer to the third-party money remittance provider as "Company R".

Mr Z has told us that he provided the fraudsters with his email address so an account with Company R could be set up and once this was completed, the fraudster entered Mr Z's card details into Company R's website in order to facilitate the transfer.

At this point, Monzo sent Mr Z a passcode to enter to confirm he was authorising the transfer. Mr Z provided this code to the fraudsters and the payment debited Mr Z's Monzo account.

Mr Z had been on the call with the fraudsters for about 3 hours by this point and had to end it to go to a meeting. However, later the same afternoon, the fraudsters called back. They told Mr Z that they needed his help to catch another hacker in a foreign country. Mr Z has told us that he went through the same process again and a further £250 was transferred from his bank account to his Monzo account. The fraudsters then used Mr Z's card details to make a further payment via Company R which in turn incurred a £1.99 handling fee. At this point, the fraudsters assured Mr Z that the security process was now complete and his accounts were now secure.

Around 15 minutes later, Mr Z decided to login to his online banking to make sure everything was okay. It was at this point that he noticed that both the current and savings account he held with the third-party bank had been drained of funds. Mr Z realised he had been scammed and contacted Monzo. In total Mr Z had lost £11,651.99.

Monzo looked into Mr Z's complaint and acknowledged that he had been the victim of a scam but it declined to offer him a refund. It said Mr Z had ignored scam warnings that had popped up on his screen during the payment process. It also didn't think Mr Z had taken enough steps to check who he was paying and the reason for the payments before he allowed the payments to leave his account.

Unhappy with Monzo's response, Mr Z brought his complaint to this service and one of our investigators looked into things. She agreed with Monzo that Mr Z had proceeded to make the first payment without a reasonable basis for believing that he was speaking with his genuine broadband provider. But she didn't agree with Monzo that Mr Z had ignored effective warnings throughout the payment process and because of this, she recommended Monzo refund Mr Z 50% of the first payment plus interest. Our investigator pointed out that the following two payments had been made using Mr Z's debit card and so these had to be considered differently to the first payment, which was an online transfer. And because Mr Z had provided the fraudsters with his card details and security passcode in order to allow these transactions to be made, he had broken the terms and conditions of his account and it wouldn't be fair to hold Monzo liable for these transactions now.

Mr Z agreed with our investigator's opinion but Monzo did not. It said that as Mr Z had made payments without verifying who he was speaking to or what he was being told, it shouldn't be held liable for any of the losses at all. It pointed out that when Mr Z was asked to select the reason he was making the first payment from a drop-down list as part of its online payment process, he had selected the payment reason "something else". Monzo said that there was a more accurate payment reason available for Mr Z to select. And so, whilst it acknowledged that the warning that had popped up at this point wasn't

specific to the type of scam Mr Z fell victim to, it said this was because Mr Z hadn't select the correct reason for payment. If he had, Monzo said it would've been able to show him an 'effective warning' which may have prevented the scam from taking place. Monzo said it shouldn't be held liable for 50% of the first payment if the reason it hadn't been able to provide an effective warning was because the customer had picked the wrong payment option.

Our investigator didn't change her mind and as an agreement has not been reached the case has now been passed to me for 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.

Having done so, I am currently minded to reach the same outcome to the one reached by our investigator – in that I think the complaint should be *partially* upheld. I'll explain why in more detail below.

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

Under the Lending Standards Board's Contingent Reimbursement Model (the CRM Code), which Monzo is not a signatory of but which it has agreed to act in the spirit of, it should reimburse customers who are victims of authorised *push payment* scams, except in limited circumstances. In this case, only the first payment for £8,900 can be considered a *push payment* the following two payments were debit card payments. And so it is only payment one that I have considered under the CRM Code. I will address the card payments separately later on.

*The CRM Code - Payment 1 – (£8,900)*

In considering the first payment, 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 Mr Z from potential financial harm from fraud. The Code also places a level of care on Mr Z and so I have also considered whether Mr Z met the required level of care too.

As I've said above, The Code requires payment service providers to reimburse customers who have been the victims of authorised push payment (APP) scams, in all but limited circumstances. If Monzo declines to reimburse its customer in full, it is for Monzo to establish that its customer failed to meet the requisite level of care under one, or more, of the listed exceptions set out in The Code itself.

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

There are further exceptions within the CRM, but none of these are applicable here.

*Did Mr Z have a reasonable basis for belief?*

Under the CRM code, Monzo can choose not to reimburse Mr Z in full if it doesn't believe he took the requisite level of care to ensure he had a reasonable basis for believing that the business he was paying was legitimate. It isn't enough for Mr Z to have believed that he was paying a legitimate business, he had to have *a reasonable* basis for that belief.

I have carefully considered Monzo's representations that Mr Z did not have a reasonable basis for believing he was making a payment to his genuine broadband provider, and I agree. In particular, I'm not persuaded Mr Z did take the requisite level of care required for Monzo to reimburse him in full under the terms of the CRM Code and I'm not persuaded that he had a reasonable basis for believing he was speaking with his broadband provider or that he was making payments from his account to catch online hackers abroad. In reaching this conclusion, I've had regard to the scene that was set by the fraudsters and the impact I believe this reasonably had on Mr Z when acting 'in the moment'. I'll explain why:

- Mr Z appears to have believed what he was being told by the fraudsters without trying to independently verify the information they were giving him.
- It's unclear how any potential hackers could've used Mr Z's IP address to access his bank accounts and so its unclear why Mr Z found this story plausible.
- Mr Z's broadband provider wouldn't generally play a role in preventing crime or need access to its customers personal bank accounts. And I'm satisfied that this should have struck Mr Z as unusual. It would be his bank that dealt with any potential threats of fraud on his account, not his internet provider.
- It's unclear why Mr Z's broadband provider would need a member of the public's help to catch so called international hackers in a foreign country – and how they would do this. But Mr Z doesn't appear to have questioned this.
- Mr Z has told us that he would not and did not agree to the use of his own funds being used to catch the 'hackers'. He has told us that throughout the scam, he thought he was using funds given to him by his broadband provider for this purpose. But this suggests to me that Mr Z was cautious enough to not want to use his own money. Yet despite being somewhat cautious, he proceeded to authorise the transfers from his account by allowing the fraudster to enter the details on his behalf.
- It's not plausible that Mr Z's broadband provider would have a special fund set aside to aid members of the public in catching hackers that were based abroad. It's also unclear why it would need a member of the public to make payments from their bank account in order to catch these hackers or why Mr Z would need to set up an account to transfer money abroad. And I'm satisfied that this should have been strange enough that it should've prompted further questioning from Mr Z.

Overall, and based on the evidence I've seen, I'm not satisfied that what Mr Z was being told was plausible and yet he appears to have accepted what the fraudsters told him at face value without completing any independent verification checks of his own. Given the particular circumstances of this case, I'm not satisfied this was reasonable and I think he should've taken steps to check who he was speaking with before agreeing to make payments out of his account in order to meet the required level of care under the CRM Code, especially

considering the amount of money involved. And so I don't think Mr Z met his obligations under the code in regard to the first payment.

*Did Mr Z ignore an effective warning?*

Monzo have said that Mr Z ignored an 'effective warning' that was presented to him on screen during the payment process for the £8,900 payment. Monzo has said that during this process, Mr Z was prompted, on screen, to select a reason for the payment from a drop-down list. Monzo has said Mr Z chose "something else" from this drop-down list and was then shown a scam warning appropriate for the payment reason he had selected. Monzo has acknowledged that this warning is unlikely to have be considered 'effective' under the CRM code but it doesn't think it should be held liable for this.

Monzo has said that its obligations under the code to share an effective warning are based on customer input and in this case, it was not possible for it to provide Mr Z with a warning specific to the scam that he was about to fall victim to as he had not accurately recorded the reason for the payment he was making.

Whist I acknowledge the arguments put forward by Monzo, the fact remains that under the CRM Code, Monza has an obligation to provide its customers with an 'effective warning' should it identify an APP scam risk in the payment journey. And, in this case, as the warning provided by Monzo wasn't specific to the type of scam Mr Z ultimately fell victim to, I'm not persuaded that the warning provided to Mr Z at the time could be considered an 'effective warning' under the Code. So, I'm not satisfied Monzo has been able to establish that Mr Z should not be reimbursed on the basis that he ignored an effective warning.

*Could Monzo have done anything else to prevent the scam?*

I also think Monzo ought to have done more than it ultimately did to try and protect Mr Z from financial harm from fraud. This payment was of a relatively high value and it was being made to a new payee. Had Monzo spoken with Mr Z about the payment at the time, I think the scam would've likely come to light and Monzo would have been able tell Mr Z that it was unlikely he was speaking with his internet provider. However, that doesn't mean I think Monzo should be held entirely responsible for the loss of the first payment. As I've set out above, I don't think either Mr Z or Monzo met their requisite obligations under the CRM Code and so I'm satisfied that a fair and reasonable outcome, in all the circumstances, would be for Monzo to refund Mr Z 50% of the first payment (plus interest at the account rate) and for Mr Z to bear responsibility for the rest.

*The card payments*

The final two payments that left Mr Z's account were debit card payments and these aren't covered by the CRM code. The regulations relevant to these transactions are the Payment Services Regulations 2017 ("The PSRs") in addition to the terms and conditions of the customer's account. Under the terms and conditions of his account, Mr Z has a responsibility to protect his account from fraud. That includes keeping things like debit cards safe and not sharing his security information, such as his PIN, security codes and online banking details with anyone else. And so I now need to decide if Mr Z failed to keep his account information safe and whether he 'failed with intent' to do so.

Intent generally means an action that someone has deliberately taken. And so, alongside the terms and conditions of his account, I've thought about whether Mr Z deliberately gave away any security details which ultimately allowed the payments to leave his account.

The terms and conditions of the account set out the following:

"*Examples of when you won't be able to claim back money you've lost may include if:*

- *you gave us incorrect instructions, or we can prove that the bank we sent your payment to received it (although we'll still try to help you recover your money)*
- *you purposefully didn't keep your phone, card (including virtual card), PIN or other security details safe, you were very negligent in not keeping them safe, you gave them to someone else, or your account is overdrawn*
- *you acted fraudulently".*

In this case, it appears Mr Z shared his debit card information with the fraudsters to allow the payments to Company R to take place. He's also told us that he shared a security passcode that was sent by Monzo to his mobile phone to allow the authorisation of the first payment. Having reviewed the terms and conditions of Mr Z's account, I'm satisfied it's made clear that security credentials such as his card information and secure codes shouldn't be provided/shared with anyone. I appreciate Mr Z was under the impression that he was speaking with his genuine internet provider and what he was doing would ultimately secure his account. But ultimately sharing this information meant he (with intent) failed in his obligations to protect his security details. And this means he's breached the terms and conditions of his account.

For this reason, and in the particular circumstances of this complaint, I'm satisfied Monzo is entitled to hold Mr Z liable for the final two card transactions that left his account - £2,500 and £251.99 respectively. And so, I won't be asking Monzo to refund these payments to him now.

**My final decision**

My final decision is that this complaint should be *partially* upheld.

Monzo Bank Ltd should now reimburse Mr Z in-line with the provisions of the CRM Code by:

- Refunding him £4,450 - 50% of the loss attributed to the first payment.
- Paying him interest at the account rate on the above sum from the date the funds left the account, up until the date of refund.

- Monzo doesn't need to take any further action in relation to the final two card payments.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr Z to accept or reject my decision before 24 May 2022.
Emly Hanley
**Ombudsman**