DRN-3328570

The complaint

Miss M is unhappy that Monzo Bank Ltd won't refund the money she's lost to a fraudster.

What's happened?

Miss M has fallen victim to a safe account scam. She says that, on 8 June 2021, she missed lots of calls from different telephone numbers whilst in a meeting at work. After the meeting, her phone rang again, and she answered it. The caller told her they worked for Ofcom – the UK's communications regulator – and her internet had been hacked. In the following order, they asked her to:

- Open her mobile banking application and check whether there had been any suspicious activity. She followed their instructions and couldn't see anything obvious.
- Download a remote support application on her phone so they could show her how many hacks had been attempted on her device – she saw that there had been 42 attempts and then closed the application.
- Re-open her mobile banking application and move her money into a specified 'safe account' so they could follow the trail of the hacker - £1,490 was paid from her current account to the 'safe account'. The caller said the money would be transferred back into Miss M's current account after 10 minutes if the hacker didn't follow the trail. She stayed on the phone for the duration, and then the call was disconnected.

Miss M says she immediately reported what had happened to Monzo. She asked if it could do anything to stop the £1,490 payment out of her account. But Monzo didn't retrieve her funds and it's declined to reimburse her under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code') because it says she ignored an effective warning it gave her during the payment journey and she didn't do enough to check who she was paying and what for.

Miss M asked this Service to consider her complaint. She said:

- She has only recently moved to the UK and she didn't know how to handle the situation. She was aware that the call may be a scam and she tried to do as many 'safety checks' as she could whilst on the phone in a pressured situation (the caller told her she only had a 10-minute window to take action).
- She entered the caller's telephone number into an internet search and nothing came up against it, but she saw that it was a UK number.
- She asked the caller why there had been calls to her mobile from multiple numbers that morning and they said it was just Ofcom's call centre trying to get in touch with her urgently.
- She conducted an internet search to check that Ofcom was a genuine business that her internet provider was associated with and found that it was. She also saw that Ofcom wasn't reporting anything about scams or fraudulent calls on its website.
- The caller told her how to find her IP address on her device, and then they confirmed they knew what it was by giving her the last digits. They asked her to look at the location of the address, and it showed as California. The caller said this demonstrated she was being hacked as it wasn't her current location.

- The caller knew the last 4 digits of her bank account number.
- She questioned why she had to move money to an account in an individual's name rather than a generic Ofcom account. The caller said the only way of catching the hacker was to follow the money. They also passed her to a 'manager' who reiterated the urgency of the situation and that there had been a number of hack attempts.

What did our investigator say?

Our investigator wasn't satisfied that the warning Monzo gave Miss M during the payment journey was impactful enough to be considered an effective warning under the CRM Code, so she didn't think Miss M had ignored an effective warning. She also thought that Miss M had a reasonable basis for belief. She concluded that Monzo should have reimbursed Miss M under the CRM Code.

Monzo didn't agree and asked for the complaint to be escalated to an ombudsman. In summary, it said:

- The warning that it gave Miss M during the payment journey was timely, impactful and relevant to the scam. Even though it doesn't mention Ofcom, it was enough to give a reasonable person pause for thought.
- If Miss M had been duly diligent, she would've concluded that she was being scammed.
- There's no reasonable basis to believe Ofcom would contact a customer to advise them they'd been hacked and ask them to move money to a 'safe account' held by a named individual.

The complaint has now been passed 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.

Monzo isn't yet a signatory of the CRM Code, but it's allowed us to apply the CRM Code's principles to complaints we consider against it which meet the relevant criteria.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Miss M has fallen victim to, in all but a limited number of circumstances. Monzo has argued that two of the exceptions apply in this case. It says that Miss M ignored an effective warning it gave during the payment journey and she made the payment without a reasonable basis for belief that the payee was the person she was expecting to pay, the payment was for genuine goods or services and/or the person or business she was transacting with was legitimate.

Effective warning

The CRM Code says:

SF1(2)(e) As a minimum, Effective Warnings should meet the following criteria

(i) Understandable – in plain language, intelligible and meaningful to the Customer

(ii) Clear – in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's [Financial Conduct Authority] *Principles for Businesses*

(iii) *Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;*

(iv) *Timely – given at points in the Payment Journey most likely to have an impact on the Customer's decision-making;*

(v) *Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*

I've considered the warning Monzo says it gave Miss M during the payment journey and I appreciate that it tried to provide an effective warning. But overall, I'm not satisfied it can reasonably be said that the requirements of the effective warning exception were met. I don't think the warning was impactful or specific enough.

It's clear to me that the warning Monzo displayed attempts to prevent safe account scams, but I don't think the warning makes the risk of falling victim to this particular type of safe account scam obvious to its customers. The warning is bright red and says *"Stop, don't pay. It's very likely this is a scam."* But then it goes on to say:

*"**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
Check with your bank
Call your bank from the number on the back of your card…"

The caller told Miss M they were calling from Ofcom, not Monzo. So, the warning is not specific to her particular circumstances or the scam she fell victim to, and I can see why she moved past it. In any event, the warning does not really bring to life what safe account scams look like. It doesn't explain that fraudsters pose as banks and other genuine companies and apply pressure to convince their victims that the funds in their account are at risk if they don't move them to a safe account with urgency. Nor does it talk about the prevalence of this type of scam or explain how sophisticated the scams can be – it doesn't for example, explain that fraudsters often know personal information about their victims and use this as a tactic to convince them that they are genuine. Finally, the warning doesn't explain the potential consequences of continuing with an irrevocable payment.

Overall, I'm not satisfied that a reasonable person in Miss M's position would fully understand the scam risk from the warning Monzo gave.

I can see from the evidence that Miss M appreciated there was some risk, and she made some effort to protect herself from financial harm. But she's said she didn't know how to protect herself so she carried out the 'safety checks' she could think of before she was ultimately persuaded by the scammer. If Monzo had really brought to life what a scam of the nature Miss M fell victim to looks like with specific information, and if it had given advice on how customers can protect themselves from this type of scam and explained the potential consequences of continuing with an irrevocable payment, then I think this would've been important contextual information that would've affected Miss M's decision making and led her to take additional steps to protect herself.

Reasonable basis for belief

I'm satisfied that Miss M had a reasonable basis for belief in this case.

I note that she was at work when she took the call from the scammer, and the pressure was

on – she's said she thought she had a 10-minute window to take action. She would no doubt have been worried about her funds, but she still tried to do some 'safety checks' in the time she thought she had. She asked the caller relevant questions and she carried out some internet searches. Ultimately, she was persuaded the scammer was genuine from the research she conducted under pressure and in a less than ideal environment, the answers the scammer gave her and the personal information they knew about her. I don't think this is unreasonable.

Monzo has pointed to some 'red flags' in the scammer's story, and said it believes Miss M could've done more checks to protect herself. I acknowledge Monzo's points but, as I've said above, I don't think it made the scam risk clear to Miss M. Overall, I think the fraud was sophisticated and I don't think it's unreasonable that it went undetected by Miss M.

Conclusions

To conclude, I'm satisfied that Monzo should have reimbursed the money Miss M lost to this scam under the terms of the CRM Code. I am not persuaded that any of the permitted exceptions to reimbursement apply in the circumstances of this case.

My final decision

For the reasons I've explained, my final decision is that I uphold this complaint and instruct Monzo Bank Ltd to:

- reimburse Miss M's loss within 28 days of receiving notification of her acceptance of my final decision; plus
- pay 8% simple interest per year from the date Miss M should have been reimbursed under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 27 April 2022.

Kyley Hanson
Ombudsman