DRN-3367943

The complaint

Miss M is unhappy that Monzo Bank Ltd won't refund her money that she lost as a result of a fraud.

What happened

In late 2020, Miss M received an unexpected automated call claiming to be from her communications provider. The message informed Miss M that her internet would be turned off due to illegal activity being detected on it. The message prompted Miss M to press a button, which she did, and was transferred to a person who claimed to be representative of the company. Unfortunately, it later transpired that Miss M was in fact talking to a fraudster.

Miss M says that the fraudster knew personal information about her, such as customer ID, address, telephone number and full name. The fraudster then told Miss M that she was currently in the process of being hacked and that she had to act as a matter of urgency.

She was instructed to download an application to her phone and was provided an elaborate story regarding a known criminal who was intent on stealing her money unless specific instructions were followed.

The fraudster instructed Miss M to transfer £9,999 from a bank account she held with another provider to her Monzo account. She was then instructed to send this to another third-party account so that it could be kept safe. Miss M followed the instructions and transferred the funds to the account details provided.

The fraudster continued to attempt to extract further funds from Miss M through her accounts held by other providers until she was asked to contact her bank and discovered she'd been defrauded. Miss M contacted Monzo and raised concerns regarding its lack of protection.

Monzo responded to Miss M's claim applying the Contingent Reimbursement Model (CRM); a voluntary code it has agreed to adhere to. Under the CRM code, the starting principle is that a business should reimburse a customer who is the victim of an APP fraud except in limited circumstances. The exceptions where a business may choose not to reimburse include where the customer:

- Ignored an 'effective warning'.
- Made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payments was for genuine goods or services; and/or that the person or business with whom they transacted with was legitimate.

Monzo has argued that both of these exceptions apply in this complaint. Therefore, it didn't offer to reimburse Miss M the money lost as a result of the fraud.

Miss M remained unhappy with the outcome of her complaint, so she came to our service to independently assess her complaint.

An Investigator considered the evidence provided by both parties but concluded Monzo should have fully reimbursed under the code. They found:

- The warning provided prior to the payment being made didn't meet the definition of an 'effective warning' as set out in the code.
- Due to the complexities of the fraud, and Miss M's vulnerabilities, they felt Miss M did have a reasonable basis for believing she was legitimately dealing with, and making payment to, the communications provider.

For the above reasons, the Investigator found that Miss M had met her requisite level of care. Therefore, Monzo were unable to decline reimbursement under the code.

Monzo disagreed with the Investigator's assessment. It said:

- It's unable to list all potential organisations that may be impersonated in any warning as this list would be exhaustive and render the warning ineffective.
- It remained confident that Miss M didn't have a reasonable basis for believing she was legitimately dealing with her communications provider.
- There was no reasonable basis for believing a communications provider would instruct a customer on how to run or manage their bank account, as there is no link between the two.

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.

Did Miss M ignore an 'effective warning'?

Miss M has argued that no warnings were shown prior to authorising the payment. But Monzo has been able to evidence that its warnings were activated for the specific payment subject to this complaint. This is supported by the fact that Miss M chose the option that specifies she was making payment to a 'safe account'.

It's possible that Miss M doesn't recall seeing this warning due to the passage of time or the high level of pressure and stress she was under at the time. But I find it more likely than not from the evidence presented that a warning was given prior to making the payment.

Monzo has supplied a copy of the warning. This instructs the payer to not proceed with the payment and highlights that Monzo—or any other bank—would not ask a customer to move their money out of their account. However, that wasn't specific to the fraud Miss M had fallen victim to.

While Miss M was intending on transferring the money to a 'safe account', she wasn't being instructed to do so by a bank. So, it's understandable why this warning didn't have the impact it was intended to give as it wasn't relevant to the situation or scam. Nor did it go into any other detail about how 'safe account' scams are typically committed or any common features to look out for.

The CRM code sets out that in order for a warning to be deemed effective it should be, among other things, impactful and specific to the APP scam risk identified. And I'm not persuaded here that the warning Monzo provided meets these requirements. I therefore do

not find Miss M to have ignored an ‘effective warning’.

Did Miss M have a reasonable basis for belief?

The fraud committed against Miss M began with a phone call purporting to be from her genuine communications provider. While Miss M is unable to verify the number she was called on as genuine, she says she was persuaded by the level of information the caller knew about her that they were legitimate.

The caller greeted Miss M by her name, knew her account ID and address. Miss M has told our service that as her landline telephone number is only known to one other person and isn’t held on any online or public records, she was convinced the caller was genuine.

Furthermore, I’ve also considered the tactics used in these types of frauds. Miss M was placed into a position where she was being told her money was at risk. The caller deployed a number of social engineering tactics to put her on the back foot, embed fear and place urgency on the measures Miss M had to take to mitigate her losses. She was told her network had been hacked, showed her that her internet address had been changed to a geographical location abroad and pointed out a potential hacker on a third-party website that was responsible for the breach.

While this may appear to a person adept in financial and cyber crime to be a standard tactic used by fraudsters—and suspicious in the circumstances—, to the layman, this would have proven a convincing combination. And this factored in with the personal information known by the caller, which Miss M says wasn’t readily available, I find it would have given her a reasonable basis for believing the caller was genuine.

Monzo has submitted that the link between Miss M’s communications provider and her bank are so tenuous that it can’t see how she was convinced by the caller. But the caller wasn’t claiming to have access or control of her bank account, they were claiming Miss M’s network had been hacked and that this was putting her bank accounts at risk.

Miss M followed the instruction of the caller to transfer money to an account to keep it safe from the hacker. But prior to doing so, she did try to challenge the caller as to why she was moving the money between accounts if they were compromised. This shows that Miss M was attempting to understand the logic behind the requests she was being given, but the fraudster claimed that the accounts she was transferring them to were also discovered to be at risk. And Miss M has told our service that the caller began raising their voice and aggressively telling her that she’d lose her money if she didn’t act immediately.

This no doubt caused an immense amount of panic, fear and anxiety in Miss M, and she’s told our service that this was exacerbated by recent traumatic events she’d experienced as a result of an abusive relationship. So, overall, I don’t think Monzo has been able to persuasively argue that Miss M made the transfers without a reasonable basis for belief. And so it follows that it can’t rely on this for exemption for reimbursement.

Putting things right

Monzo should now go ahead and reimburse Miss M the full amount lost.

I’ve also considered the appropriate amount of interest to pay Miss M for deprivation of those funds.

Monzo has agreed that it intervened in the payment by displaying the appropriate warning before Miss M proceeded with the payment. But I think it missed an opportunity here under

its regular obligations, outside of those in the CRM code, to protect Miss M from financial harm.

Miss M clicked on the 'safe account' option when selecting what the payment was being made for. This is a clear and concerning indicator that its customer is in the process of being defrauded as there are few legitimate reasons why a customer may be transferring their funds for this purpose.

Further, Miss M was transferring almost the entirety of the balance of her account and the payment was significantly higher than any transaction she'd made prior. I think this presented Monzo with a number of concerning signs and I think it missed an opportunity to engage in a meaningful intervention in the payment journey.

Had it done so, it's likely it could have stopped the payment from being made considering the circumstances to a person adept in financial crime were clearly that of fraud. For those reasons, I feel it fair that Monzo pays 8% simple interest per annum from the date the payment was made to the date it settles with Miss M.

My final decision

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

- Reimburse Miss M the £9,999 lost
- Pay 8% simple annual interest on this amount from the date of payment 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 24 August 2022.

Stephen Westlake
Ombudsman