DRN-3617009

The complaint

Miss J is unhappy because Monzo Bank Ltd ("Monzo") did not reimburse her money she transferred to a fraudster.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. But in summary, and based on the submissions of both parties, I understand it to be as follows.

In April 2022, Miss J received a call from someone claiming to be from a well-known online retailer, whom she held an account with. The call was from a mobile number. Unbeknown to Miss J at the time she was in fact speaking with a fraudster.

Miss J was told someone was trying to purchase a membership for a service the retailer provided and a mobile phone. On checking the account she held with the retailer, she could see a mobile phone was in her basket. She told us that she tried to remove this but couldn't.

Miss J explained that she was told to delete the card details that were linked to her account, which she did.

Not long into the call, Miss J received a genuine text message from the retailer. This message included a one-time passcode (OTP) to reset her password. Miss J shared the OTP with the fraudster (as she believed at the time the caller was genuine) after they told her they'd help sort this out for her.

In helping to sort out this matter, the fraudster told Miss J she'd need to go through self-verification, and she needed to transfer £307 to the account details provided to her. Miss J explains she was told by the fraudster that she needed to believe them as they were handling both the account she held with the retailer and also her bank account, which they told her was linked to her account with the retailer. She says she was told that if she didn't deal with this matter then the person, who was trying to buy the membership and mobile phone, might go into her bank account and take all of her money.

Miss J was asked to install an app on her phone, so that the fraudster could help her. She was told she couldn't resolve it herself and that they needed to do it for her. Miss J has commented that she did wonder why the retailer would ask her to install an app, but as she wanted the issue resolved she did as they'd instructed.

Miss J set up a new payee and transferred £307 to the details given to her. She says she was told as this was for self-verification to put her name in as the recipient.

After making the payment, Miss J says she called the original phone number for the retailer. It was at this point; she was told her account was fine and she realised she'd fallen victim to a scam.

Miss J reported the scam to Monzo the same day. Monzo investigated the matter and considered its obligations to provide Miss J with a refund. Monzo has agreed to act in the spirit of the Lending Standards Board Contingent Reimbursement Model (CRM) Code, although it isn't a signatory of it. The CRM Code requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Monzo says one or more of those exceptions applies in this case.

Monzo says it doesn't feel Miss J took reasonable steps to check who she was paying and so it will not be refunding the money she's lost.

Monzo contacted the beneficiary bank to attempt to recover Miss J's money, but unfortunately no funds remained in the account.

Unhappy, Miss J referred her complaint to our service. One of our Investigators looked into the complaint and didn't think it should be upheld. She thought that, in the circumstances, Miss J ought to have had some concerns about the payment she was about to make and that further steps could have and should have been taken, in order for Miss J to meet the required level of care under the CRM Code. She also didn't think there was a requirement for Monzo to provide an effective warning, due to the value of the payment Miss J made. The investigator therefore didn't consider that Monzo needed to do anything to put things right for Miss J.

Miss J disagreed and asked for the complaint to be passed to an ombudsman 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.

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 at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

When thinking about what is fair and reasonable in this case, I've considered whether Monzo should have reimbursed Miss J in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect Miss J from the possibility of financial harm from fraud.

There's no dispute here that Miss J was tricked into making the payment. She thought she'd received a call from a retailer she held an account with and that she needed to make a payment to self-verify the account. But this isn't enough, in and of itself, for Miss J to receive a refund of the money under the CRM Code. The Code also places a level of care on Miss J.

The CRM Code

Monzo has agreed to adhere to the provisions of the Lending Standards Board Contingent Reimbursement Model (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 a 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.

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

In this case, I think Monzo has been able to establish that it may choose not to fully reimburse Miss J under the terms of the CRM Code. I'm persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies in the circumstances of this case.

Taking into account all of the circumstances of this case, including the characteristics of the customer and the complexity of the scam, I think the concerns Monzo has raised about the legitimacy of the transaction Miss J was making are enough to support its position that it's entitled to rely on exceptions to reimbursement. I don't think Miss J had a reasonable basis for believing the person with whom she transacted with was legitimate. I think Miss J should have done more than she did to satisfy herself that it was legitimate before making the payment. I will now explain why.

Miss J's told us she believed the person she'd received a call from, was from the retailer she held an account with, after she checked her account and could see that there was a mobile phone in the basket which was consistent with what she'd been told. The call Miss J received was from a mobile number and I've not been given any persuasive explanation as to why Miss J believed the mobile number was linked to the known online retailer. I'm also not persuaded that such a well-known company as this online retailer, would use mobile numbers as a method to contact its customers. I do also have to keep in mind, that after Miss J made the payment, she contacted the retailer on what she's said was the original number for it and she was told her account was fine. Given the steps Miss J took after making the payment, I think it reasonable that she could have taken these steps prior to making the payment to satisfy herself that she was speaking with the genuine retailer she held an account with.

Miss J has also said she did question/wonder why the retailer had asked her to install an app on her phone but has said as she wanted the matter resolved she did as instructed. I think this ought to have been a flag to Miss J and that it ought fairly to have prompted her to ask some more questions about what she was being told and asked to do, especially when taking into account that she herself was questioning why the retailer would ask her to download an app.

In light of the above, given the doubts that I'm persuaded Miss J had, I don't think that seeing a mobile phone in her account basket in and of itself was enough for Miss J to be satisfied the call she received was from the retailer she held an account with.

Further, I think it ought to have caused Miss J concern about the legitimacy of the person she was speaking to, when she was asked to make a payment of £307 for self-verification, with what appears to have been with no explanation as to why this was needed or why the money was needed to self-verify. I do appreciate Miss J says she was told to enter her name as the recipient for the transaction as the payment was for self-verification purposes, however, the account details provided from the payment were to a third-party account. I've not seen any plausible explanation as to why the payment was being made to a third-party account. And while I do recognise Miss J, in response to our Investigators assessment, says she was told she'd get a refund instantly; I think this also ought to have been a flag. I say this because, I've not been given any explanation as to why Miss J was asked to make a payment for such a specific amount of £307 in order to self-verify her account when she says she was told the money would be refunded instantly back to her.

I think these things ought to have prompted her to ask questions about the payment she'd been asked to make – for example, why she needed to transfer the funds to verify herself and why she needed to make the payment if it was to be returned to her straight away.

I do appreciate Miss J has said she'd not been in the country a long time and has said she was new to the UK. I've thought carefully about this. But unfortunately, I don't find this point changes my conclusions. As set out above, Miss J has indicated to our service that she did have some doubts during the call - as she did question/wondered why the online retailer would ask her to install an app. And, I have to keep in mind that Miss J did contact the online retailer on its contact number following the payment she made. I'm persuaded on balance that she had some degree of awareness about steps she could take – given those that she did take albeit after the payment was made.

With all the above in mind, in the particular circumstances of this case, I consider that Miss J ought to have had concerns about the legitimacy of the payment she was making for the purposes of self-verification. And that, in turn, ought to have led to a greater degree of checking on Miss J's part. In not carrying out sufficient checks I don't find she had a reasonable basis for believing the person with whom she transacted with was legitimate and so fell below the level of care expected of her under the CRM Code.

Should Monzo have done more to try and prevent the scam and protect Miss J?

I've thought about whether Monzo did enough to protect Miss J from financial harm.

The CRM Code says that where firms identify APP scam risks in a payment journey, they should provide Effective Warnings to their customers. The Code also says that the assessment of whether a firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the scam.

I am also mindful that when Miss J made this payment, Monzo should fairly and reasonably also 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).

Whilst I think Monzo could've provided a better warning than it did, I don't think it was required to give an effective warning under the CRM Code, in these particular circumstances. I think this because I don't think the payment Miss J made was so remarkable, in comparison to previous account activity, that Monzo should've identified the payment as a potential fraud risk. I therefore don't think Monzo failed to meet its standards under the Code by not doing so, prior to processing the payment.

Once it was made aware of the scam, Monzo tried to recover Miss J's funds, but unfortunately was advised by the beneficiary account that no funds remained. Having considered the short timeframes within which Monzo contacted the beneficiary account to make it aware of the scam, I don't think Monzo could reasonably have done anything further to recover Miss J's payment.

With the above in mind, I'm satisfied that Monzo's position on Miss J's fraud claim, and its assessment under the CRM Code, is fair and reasonable in all of the circumstances and that Monzo shouldn't be held liable for Miss J's loss. And so, I don't make an award to Miss J.

Overall

I'm sorry to hear of what's happened to Miss J and I can understand why she wants to do all that she can to try and recover the money she's lost. I do sympathise with Miss J as she's clearly been the victim of a scam and I recognise this has been upsetting for her. But the circumstances of the case and the evidence available lead me to find I'm unable to uphold this complaint.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss J to accept or reject my decision before 12 October 2022.

Staci Rowland
Ombudsman