DRN-4833909

Complaint

Miss L is unhappy that Monzo Bank Ltd didn't pay her a refund after she told it she'd fallen victim to a scam.

Background

Miss L was the victim of an impersonation scam that took place in July 2023. She was in the process of purchasing a home and had transferred funds to her solicitor to cover the cost of the deposit. She initially made a legitimate transfer of £10,000 to the solicitor's client account. However, she then received an email, purportedly from her solicitor, advising her to transfer the remaining funds to a different account. She says she was told that the prior account was being audited and so temporarily couldn't receive funds. She didn't realise it at the time, but this email was sent by fraudsters who had created an email address that was nearly identical to that of her solicitor.

As a result, Miss L made several payments from her Monzo account to an account controlled by the fraudster. Some of the funds were returned, but her net loss amounted to £19,000. Once she realised she'd fallen victim to a scam, she notified Monzo via her representatives. Monzo looked into things but didn't agree to refund her. It says she should've carried out checks to make sure that she was paying the right person. It also said she failed to take appropriate action when warned that the name on the account did not match the intended recipient (via the Confirmation of Payee process). Monzo also doubted whether Miss L's email account had been compromised and suggested that her failure to provide the email evidence obstructed their investigation.

Miss L wasn't happy with the response she received from Monzo and so she referred her complaint to this service. It was looked at by an Investigator who considered it by applying the terms of the Lending Standards Board's Contingent Reimbursement Model (CRM) Code. He found that Miss L had made these payments with a reasonable basis to believe that they were genuinely at the request of her solicitor. Under the terms of the CRM Code, this meant it needed to refund Miss L's losses.

Monzo disagreed with the Investigator's opinion. It said that Miss L should've been more careful when she was warned about the Confirmation of Payee discrepancy. It also noted that Miss L had said the fraudster had deleted most of the relevant emails from her inbox. It said this meant there was no real evidence that she'd fallen victim to a scam. It thought she should be expected to prove that her email account had indeed been compromised by a third-party and that her failure to provide copies of the emails was cause for concern.

As Monzo disagreed with the Investigator's opinion, the complaint has been passed to me to consider and come to a final decision.

Findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

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 (in this case, the 2017 regulations) and the terms and conditions of the customer's account. However, that isn't the end of the story. Monzo has agreed to follow the Lending Standards Board's Contingent Reimbursement Model Code ("the CRM code"). This code requires firms to reimburse customers who have been the victim of authorised push payment ("APP") scams in all but a limited number of circumstances.

For Monzo to choose not to reimburse Miss L, it needs to establish that an exception to reimbursement applies. Monzo has identified two specific exceptions that it considers are applicable here - those at R2(1)(b) and (c). In other words, Monzo says that Miss L made this payment *"without a reasonable basis for believing that … the payee was the person the Customer was expecting to pay."* It also says that Miss L did not take appropriate actions following a clear negative Confirmation of Payee result. It also considers it relevant that the CRM Code says that consideration should be given to whether *"during the process of assessing whether the Customer should be reimbursed, the Customer has acted dishonestly or obstructively in a material aspect."*

After reviewing the evidence, I am satisfied that Miss L was the victim of an impersonation scam. She has demonstrated that the fraudster used an email address almost identical to her solicitor's and was aware of specific details of her transaction, which suggests that the fraudster had access to the relevant communications. Miss L has also provided a copy of an email that bounced back after she attempted to respond to the fake email address. The Investigator also obtained information from the receiving bank, confirming that the funds were quickly transferred out of the receiving account to an account belonging to a dissolved company.

Monzo has also said that Miss L needs to show that her email account was compromised. Her email provider makes it quite straightforward to see the IP address used to access the account for the last ten log-ins. If Monzo had asked her to gather this evidence at the time she reported the scam, it might have still shown the IP address used by the fraudster. It didn't do so, which is unfortunate given how significant it now says that evidence is. I've considered whether Miss L should be expected to obtain the historical data. As far as I can see, the company that provides her email account won't make that data accessible without a court order. I don't think it would be reasonable to expect Miss L to go through those steps, or to pay the legal costs associated with making sure the formalities of such a request were carried out correctly.

Overall, while Monzo expressed doubt that a scam occurred, there's nothing far-fetched about what Miss L has said happened and the available evidence supports her.

Does an exception to reimbursement apply?

The Investigator concluded that Miss L had a reasonable basis for believing she was paying her solicitor, and I agree. The fraudster used an email address closely resembling the solicitor's and, according to Miss L, the emails contained transaction details that would have reassured her that the communications were genuine. Given the circumstances, it is not surprising that she did not identify the subtle discrepancy between the two email addresses.

Monzo contends that Miss L's failure to produce the emails sent by the fraudster weakens her case. It speculates that there might be potential red flags in those emails which Miss L missed. I agree it would've been helpful to have seen them. Nonetheless, I'm mindful of the fact that impersonation scams of this kind are very common. I don't think it would've been particularly difficult for a fraudster to create a credible fake email in these circumstances.

Miss L has explained that the fraudster deleted the emails from her account. She said this when she reported the scam to Monzo and has consistently said so throughout the investigation into this case. Monzo says it finds it unlikely that a fraudster would bother to delete the emails. I'm not sure I understand the scepticism on this point. If, as Miss L says, her email account was compromised and someone had hacked into it, deleting the emails would take mere seconds. It's also theoretically possible that doing so might cause a small delay in reporting the scam which might make it easier for the fraudulently obtained funds to be transferred on from the receiving account.

Monzo has also placed significant weight on the fact that Miss L moved past the CoP warning when she attempted to make the payments. The warning indicated that the account name did not match the intended recipient, and Miss L was advised to cancel the payment if she suspected fraud.

Miss L has explained that she had seen similar warnings before and had successfully completed transactions despite the mismatch. I find her reasoning understandable. In addition to that, the text of the warning relied on Miss L's judgement as to whether there was a fraud risk – if she considered that there was, it advised that she carry out additional checks. However, in this case, Miss L didn't have any specific reason to question the legitimacy of the payment instructions. The fraudster had successfully gained her cooperation and Miss L still believed she was dealing directly with her solicitor. In light of this, I do not consider it unreasonable that Miss L proceeded with the payment despite the CoP warning.

Overall, I'm satisfied that Monzo hasn't demonstrated that an exception to reimbursement applies here and that it should have reimbursed her under the CRM Code when she made her original claim.

Final decision

For the reasons I've set out above, I uphold this complaint.

If Miss L accepts my final decision, Monzo Bank Ltd should refund the payments she made in connection with the scam, less the amount that was recovered. It should also add 8% simple interest per annum to those payments calculated to run from the date it declined to refund her (4 November 2023) until the date any settlement is paid.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss L to accept or reject my decision before 13 November 2024.

James Kimmitt
Ombudsman