DRN-4828471

The complaint

Miss S complains that Monzo Bank Ltd won't reimburse her after she fell victim to a scam.

What happened

The background to this complaint is well known to both parties so I won't repeat it in detail here. But to summarise, Miss S has explained that in around September 2023 she was looking to book a cosmetic procedure. She's said her ex-partner had recently paid for a weekend away for them both and had used a discount page he had found on a social media platform to get a reduced rate of £200. Miss S has explained that it was her ex-partner who found the discount page and arranged the weekend, so she has no evidence of conversations that took place and is unable to obtain these from her ex, but that she made this payment through her own account.

Miss S has explained that the social media page her ex-partner used also claimed to be offering to pay half of any bills you requested, such as mortgage payments, loans and also procedures like she was having. It also offered other 'services' such as getting any documents needed, including wage slips, bank statements and digital copies of passports or driving licenses. Miss S has said the page had around 6,000 followers and the page owner often posted positive testimonials from customers. Based on this and her previous successful experience booking a weekend away, she contacted the page and asked if it would pay towards her surgery fees. Unfortunately, unbeknownst to Miss S at the time, she was in fact corresponding with a fraudster.

The fraudster confirmed her cosmetic fee could be paid towards and Miss S asked how it worked. She was told all she needs to do is send information of the fee that needs paying. Miss S advised that the initial deposit fee was £750 and provided details of the clinic. The fraudster confirmed the fee had been paid and provided details of a bank account (belonging to the same account name as the one she'd previously sent £200 to) to transfer her portion of the costs (£375).

Miss S has explained that her clinic confirmed payment had been received. Therefore when the final balance was due days before her procedure, she contacted the fraudster again to request the bill is partially covered, which the fraudster confirmed could be done. Miss S advised the final balance was £4,445. Again, Miss S was told this had been paid, and was provided with new bank details under a different name to send her portion of the cost (£2,200).

Once she'd made the payment, the fraudster told her that their bank was questioning the source of payment and asked her to send her proof of identification which they could pass to the bank to unblock the account. At this point Miss S became suspicious that she may have fallen victim to a scam, which was confirmed when her clinic advised her the payments made had been recalled and the full balance was therefore owing. At this point Miss S contacted Monzo to raise a scam claim.

Monzo investigated Miss S' claim and considered its obligations to provide her 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), which 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 has said Miss S didn't have a reasonable basis for believing she was making a legitimate payment. However, it did acknowledge there were delays in providing Miss S with its response, and offered her £50 as an apology.

Miss S remained unhappy and referred her complaint to our service. An investigator considered the complaint but didn't uphold it. She didn't think Miss S had done enough to satisfy herself that this was a genuine deal. She also didn't think there was a requirement on Monzo to have further intervened, based on the value of the payments Miss S made.

Miss S disagreed. She clarified points that had been misunderstood in the view regarding the initial £200 payment she'd made, unrelated to the scam. She also explained she thought that Monzo ought to have done more to protect her and reclaim her money.

As Miss S remains unhappy, the complaint has been referred 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, while I'm sorry to disappoint Miss S, I'm not upholding her complaint. I'll explain why.

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 S under the provisions of the CRM Code and whether it ought to have done more to protect Miss S from the possibility of financial harm from fraud.

The CRM Code

As mentioned, Monzo has agreed to act in the spirit of the Lending Standards Board CRM Code (although it isn't a signatory). The CRM Code 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 and it is for Monzo to establish that a customer failed to meet one of the listed exceptions set out in the CRM Code.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by

failing to take appropriate action in response to such an effective warning

- The customer made payments without having 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

**Further exceptions outlined in the CRM Code do not apply to this case.*

I think Monzo has been able to establish that it may choose not to fully reimburse Miss S 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.

Taking into account all of the circumstances of this case, I don't think there is enough to support a position here that Miss S had a reasonable basis for believing she was paying a legitimate individual. I'll explain why.

First, Miss S has explained, and provided evidence, about the sorts of services the fraudster was offering. These included providing any type of financial or identity document. I think this alone is sufficient to demonstrate that this individual was providing illegitimate and likely illegal services and therefore payments made to a linked individual wouldn't be covered under the Code, based on there being a requirement to believe the individual with which a customer transacted with is 'legitimate'.

In any event, I've further considered whether I think Miss S did enough in the circumstances of the scam she fell victim to, to check the legitimacy of the deal she was being offered – and having considered everything, I don't think she did.

I appreciate Miss S had successfully used the services of this social media page before and that this would've reassured her to an extent that offers posted were legitimate, but in this case, I think the deal she was being offered was simply too good to be true. Miss S simply asked if the fraudster would pay towards her bill - without having to provide any explanation or evidence of why financial support may be required - and was led to believe this was the case. While Miss S did ask how the process 'works' the fraudster offered her no explanation on how (or why) they are able to pay bills of anyone who approaches them asking – and I don't think there's a realistic business model that would explain this. Even though Miss S' initial deposit seems to have been successfully paid by the fraudster, based on the unlikeliness of this offer, I still consider there should have been significant red flags on what 'catch' there may be to this offer – particularly considering their open advertisement of other illegitimate business avenues.

There's also no explanation provided of why Miss S has to pay a third party's private account, and why the social media page wouldn't just pay a portion of the bill and let Miss S pay the rest directly – or why it couldn't transfer the available funds directly to Miss S.

For these reasons, I don't find Miss S had a reasonable basis for believing she was paying a legitimate individual and so fell below the level of care expected of her under the CRM Code.

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

I've thought about whether Monzo did enough to protect Miss S 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 S 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). Having considered the payments Miss S made, I don't think they was so remarkable, or out of character in comparison to her usual account activity, that they should've appeared as suspicious to Monzo. I therefore don't think Monzo failed to meet its standards under the Code by not providing Miss S with an effective warning, prior to processing the payments.

Once it was made aware of the scam, Monzo contacted the recipient account that Miss S sent her payment of £2,200 to. The receiving bank have been unclear with both our service and Monzo about whether or not funds remain. Miss S may therefore wish to contact the recipient account provider directly to make further enquiries. In any event, I don't consider there is more Monzo could have done at this point in time, based on the enquiries it has made and lack of conclusive responses.

Unfortunately the recipient account where Miss S sent £375 has confirmed that all funds were removed by the account holder before Miss S had logged her claim with Monzo. Therefore any swifter action by Monzo for this payment would not have impacted its ability to recover her funds.

Overall, while I'm sorry to disappoint Miss S and don't underestimate the impact this scam would have had on her, I don't think Monzo should be held liable for Miss S' losses under the CRM Code. And so I don't intend to make an award to Miss S.

My final decision

My final decision is that I don't uphold Miss S' complaint against Monzo Bank Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 19 August 2024.

Kirsty Upton
Ombudsman