The complaint

Mr K complains that Monzo Bank Ltd ("Monzo") have failed to refund money he lost as part of a scam.

What happened

Mr K holds a bank account with Monzo. He made a payment of £1,000 on 28 May 2020 to an individual that was promoting an investment opportunity via social media. He had been told that an initial investment of £600 he had made (from an account with another bank) had made a £15,919 profit, for which he was required to pay a £3,183 'release fee'. However, Mr K didn't have this money, so he agreed with the fraudster to pay £1,000 instead, which he paid from his Monzo account.

Mr K eventually realised he had been scammed when he didn't receive any money and the fraudster blocked him on social media, so he reported the scam to Monzo on 29 May 2020. Unfortunately, the funds had already been withdrawn from the beneficiary account within a few minutes of it being transferred, with just £5.46 remaining (which was returned to Mr K on 9 June 2020).

Monzo refused to refund the remaining £999.54 Mr K had lost as they didn't think he had taken enough steps to verify who he was paying, or that he had a reasonable basis for believing the payment was for genuine goods or services. They also said he had ignored effective warnings issued through their banking app both when he set up a new payee and immediately before making the payment.

Our investigator didn't uphold the complaint. He was satisfied that Monzo had assessed Mr K's fraud claim fairly as he didn't think he had a reasonable basis for believing that the payment he was making was for a genuine service. Mr K disagreed, so the matter has been escalated to me to determine.

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, I agree with the conclusions reached by the investigator and have decided not to uphold it.

Monzo is a signatory of the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code). This requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams, in all but a limited number of circumstances.

A firm 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.

- The customer had been grossly negligent.

There are additional exceptions set out in the CRM Code, however they do not apply in these circumstances, so I have not listed them.

In the particular circumstances of this case, I'm not persuaded that Mr K had a reasonable basis for believing the payment he made was for a genuine investment with a legitimate individual for these reasons:

- Mr K has said that the fraudster followed him on Instagram, and that they were posting about successful investments and trading. They subsequently sent him a direct message on his Instagram account and encouraged him to speak to them through WhatsApp messenger, where they sent further messages showing him how much he could make (such as guaranteed returns of £3,000 based on an investment of £600). He was also told by the scammer that they operated a no loss guarantee, such that he would get his money back even if the investment didn't work out. This isn't something that can ever really be promised with genuine investments. So, in these circumstances, I think it ought to have been apparent that it sounded too good to be true – i.e. investing in a scheme that promised significant returns in a few hours with absolutely no risk of losing the capital invested. The guarantee Mr K was given is also in stark contrast to the warning displayed on the website that Mr K said he visited, which stated that 77% of investors lose money.

- The nature of the investment proposed by the scammer seems implausible, as they said the profit was made by buying the US dollar for a third of its normal value – but there was no further explanation or context behind how they were able to purchase currency at what is objectively an unrealistically low rate.

- Mr K said he researched the investment company by checking google and Companies House but says he didn't find anything suspicious. However, I note that the website he visited (XM.com) was for a Cypriot based investment firm, yet the entry he looked up on Companies House (XM Solutions Limited) is an IT consultancy based in Leeds. So it ought to have been apparent that this wasn't the same company. Mr K says he did question this with the scammer he was messaging and was told it was due to their staff working from home (mainly in Leeds). But I think this ought to have raised concerns, as it doesn't sound plausible that an investment company registered overseas would later register its company in Leeds just because it had some people working there remotely. In any event, there was little basis to believe that the individual Mr K was talking to was even from any of the companies he had researched, as they'd provided no evidence or credentials to demonstrate this, and all he had seen of this individual was an Instagram account.

- Once Mr K had invested his money, he was told that he had made over £3,000 in just one hour, which then turned into over £15,000 in just four hours. Again, given that he had only invested £600, I think a reasonable person ought to have had some concerns about whether this was realistic, and whether the investment and/or the person he was dealing with were in fact legitimate – particularly when contacted by a supposed investment company out of the blue as was the situation here.

- Mr K was originally told by the scammer that investments under £1,000 were tax free, however he was later told that he had to pay over £3,000 as a ‘release fee’ in order to obtain the money. I appreciate that he questioned this with the scammer and was provided with a ‘company policy’ document. But given that he hadn’t been forewarned of this charge (and had even been told it was tax free) and also taking into account the significant amount of money Mr K was told he had made in just a few hours, I think he ought to have made additional enquiries before transferring the ‘release fee’ to the fraudster. He hadn’t been given any access to any trading platform, for example, to be able to see the gains for himself and was instead reliant on the messages and screenshots he was getting from the scammer on WhatsApp. It also doesn’t appear to have struck Mr K as odd that the company that originally required over £3,000 in order to release his profits would take just a few minutes to accept £1,000 instead. If indeed the ‘release fee’ was a legitimate fee or a tax, it’s highly unlikely that a legitimate investment company would be able to accept such a significant amount less than what was owed.

Overall, I think Mr K ought reasonably to have had some concerns about the risks associated with the payment he was making. I appreciate that he questioned certain things, but in the circumstances, I’m not persuaded there was enough reasonable basis for him to believe that he was making a payment towards a genuine investment and/or that the individual he was talking to had any link to a legitimate trading company. So I don’t think Monzo have acted unfairly by relying on this exception to not reimburse him under the provisions of the CRM Code.

Should Monzo have done more to try and prevent the scam and protect Mr K?

I’ve also thought about whether Monzo did enough to protect Mr K 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. In the circumstances, I don’t think that any warning would have made a difference here. It seems that Mr K was convinced enough by the rudimentary research he’d carried out and the screenshots he had been shown, so I’m not persuaded that any warning from Monzo about fraud would have stopped him from making the payment.

I am also mindful that when Mr K made this payment, Monzo should’ve fairly and reasonably had systems in place to look out for unusual transactions or other signs that might indicate that their customers were at risk of fraud (among other things).

I’ve considered the £1,000 payment Mr K made to the scammer and I don’t think it stood out as being uncharacteristic or unusual enough for Monzo to have been concerned that he was at risk of financial fraud at the time he made it, so I don’t think Monzo were under any obligation to stop the payment.

Overall, I’m satisfied that Monzo’s position on Mr K’s fraud claim, and their assessment under the CRM Code, is fair and reasonable in all of the circumstances. I appreciate this isn’t the outcome Mr K will have been hoping for – but I won’t be asking Monzo to take any further action.

My final decision

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr K to accept or reject my decision before 13 October 2021.

Jack Ferris
Ombudsman