DRN-3819809

The complaint

Mr H is unhappy because Metro Bank PLC ('Metro') did not reimburse the money he transferred to a fraudster.

What happened

Mr H is represented in this case but for ease, I'll refer to Mr H throughout this decision.

Mr H says that he was contacted on social media by someone I'll refer to as A who said they traded in stocks and shares and were FCA regulated. Although he didn't know at the time, A was a scammer. Mr H made enquiries with A in 2020 but at the time didn't go any further. He says he saw daily posts and testimonials from satisfied customers who had received life-changing profits and was saving for his wedding, so in February 2021 he contacted A again and decided to invest. A suggested an initial investment of £800 to see how things went and agreed to trade on Mr H's behalf for a small commission. Mr H believed this first payment was to A's accountant. After he made the payment, Mr H received confirmation of his payment by email.

After a few days A told Mr H the investment had done well and that he needed to pay a fee of £2,000 to withdraw his profits. The fee would be refunded with Mr H's profits and didn't come as a surprise to him as A discussed this with Mr H before he invested. Mr H transferred £2,000 to a different individual in two separate payments. A then told Mr H that the £2,000 had mistakenly been invested and his profits were now greater. As a result, Mr H was asked to pay another fee of £2,000. This payment was also split into two payments and the last one was made to a third payee.

I have set out in the table below the payments Mr H made to the scammer. Mr H says that he didn't receive any warnings or messages from Metro when he set the new payees up.

Date	Amount	Payee
05/11/21	£800	1
08/11/21	£1,100	2
08/11/21	£900	2
08/11/21	£1,050	2
09/11/21	£950	3
TOTAL	**£4,800**	

Mr H didn't receive any documentation (other than the email confirmation) but got regular updates on a messaging platform. In anger and frustration, he deleted the messages though, so I've not been able to see them. He says A sounded professional and knowledgeable.

A kept reassuring Mr H he'd receive his funds, but this didn't happen, and Mr H contacted Metro to report the scam on 10 November 2021.

Metro is a signatory of the Lending Standards Board Contingent Reimbursement Model CRM Code (the CRM Code) and has considered Mr H's claim under it. It says that it provided Mr H with warnings at the time the payments were made and that he didn't complete enough checks to ensure the investment was legitimate. Metro also said that it contacted the banks that received Mr H's funds in an effort to recover them but was advised that none remained.

Our investigation so far

The investigator who considered this complaint didn't recommend that it be upheld. She said there were numerous red flags that Mr H ought reasonably to have questioned and that he hadn't completed any checks before deciding to invest. The investment was arranged over social media and a messaging service, Mr H received an email from a personal account, he made payment to multiple individual payees rather than to a company and it seemed likely the rate of return was unrealistic given that Mr H was asked to pay a £2,000 withdrawal fee.

Mr H didn't agree with the investigator's findings and asked for a decision, so his complaint has been passed to me. In summary, he said that Metro ought to have picked up on the unusual activity on his account and intervened. This is because Mr H made five higher value payments to three new payees over four days.

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.

When thinking about what is fair and reasonable in this case, I've considered whether Metro should have reimbursed Mr H under the provisions of the CRM Code and whether it ought to have done more to protect them from the possibility of financial harm from fraud.

There's no dispute here that Mr H was tricked into making the payments. But this isn't enough for Mr H to receive a refund of the money he lost under 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
- The customer has been grossly negligent.

*Further exceptions are outlined in the CRM Code, but they do not apply to this case.

Taking into account all of the circumstances of this case, including the characteristics of Mr H and the complexity of the scam, I think the concerns Metro has raised about the legitimacy of the transactions Mr H made are enough to support it can rely on an exclusion to reimbursement set out in the CRM Code. I don't think he had a reasonable basis for believing the payments were for genuine services or that the person he transacted with was legitimate and will explain why. I should also say that it's the combination of these factors that lead me to believe Mr H didn't have a reasonable basis for belief and that none of them can be considered alone.

- Mr H contacted someone from a social media site after seeing the investment opportunity. Social media is not an investment platform.
- All contact between A and Mr H was via a social media site and messaging service, which isn't what I'd expect if A was a genuine broker working for a genuine company.
- It seems from Mr H's discussion with Metro's fraud department that A claimed to be from a company, but he couldn't remember the name of it. Mr H hasn't suggested that he completed any research into this company or checked its FCA registration. I consider that Mr H ought reasonably to have at least looked at the company's website.
- Mr H wasn't provided with a contract or any documentation other than an email to confirm his initial investment. This email was from a personal account which I think ought reasonably to have concerned Mr H and led him to take additional steps before making any further payment. Genuine brokers would set out the terms agreed in writing.
- Mr H says he can't remember the rate of return he was offered and no longer has the messages from A. But it's clear that A offered a quick return (as Mr H was asked to pay a fee after three days). I consider it likely the return was high given that Mr H was prepared to send £2,000 to withdraw it and the email confirmation he received said a fee was payable if profits exceeded £3,000. So, Mr H must have made substantial profit in a few days on his £800 investment. An unrealistic rate of return is a sign that something is amiss. And all investment involves an element of risk and forex trading is particularly risky, but Mr H was told that if the trade failed, he'd receive a full refund. I think these factors ought reasonably to have led Mr H to be cautious.
- Mr H paid three different individual payees, none of whom were A. This is not what I'd expect if he was investing through a genuine company. Mr H seems to have questioned the reason for this when he made the initial investment but not after that when he was asked to pay two other payees. If Mr H was investing through a legitimate company all payments should have been made to that company. So I think this was another sign that the investment and broker weren't genuine.
- A provided Mr H with a screenshot that showed her full name and an FCA registration number. Whilst Mr H says the name on the screenshot was the same as on social media, there was nothing to show that A was the individual registered with the FCA. And if Mr H had checked A on the FCA website he'd have seen that the number on the messages he received from A didn't match her official details.

Metro says that each time Mr H set up a new beneficiary and payment he was provided with a warning. But it hasn't been able to evidence the payment reason Mr H chose or which warning he saw. If Mr H had chosen a financial opportunity as the payment reason, he'd have been given some advice about out of the blue contact likely being a scam, to check the FCA website through a link provided, and not to make the payment unless you know the money is going to the right place. I don't consider the warning was effective as it didn't bring to life what a social media investment scam looks like, but I think Mr H should have been alive to the possibility that A wasn't offering a genuine investment opportunity.

Overall, I consider Metro acted reasonably in relying on an exception to reimbursement set out in the CRM Code.

Should Metro have done more to try to prevent the scam and protect Mr H?

I'm also mindful that when Mr H made these payments, Metro 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. So I've also considered whether the payments Mr H made were unusual or suspicious.

I don’t believe the payments Mr H made were so unusual and out of character that Metro ought reasonably to have intervened and asked him questions about them. I accept that Mr H made a series of payments over a few days and set up three new payees. But the amount of each payment was relatively low, Mr H’s balance wasn’t depleted, and he had previously made faster payments. It seems that the scammer asked Mr H to make smaller payments to avoid them being picked up by Metro’s systems.

There’s a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. Whilst banks have obligations to be alert to fraud and scams and to act in their customers’ best interests, they can’t reasonably be involved in every transaction. I appreciate the loss has had an impact on Mr H, but I don’t believe it would be reasonable to expect Metro to have taken any additional steps when the payments were made.

I note that Mr H’s representative has referred to previous decisions this service has published and upheld. Each case is considered on its own merits and whether a payment is unusual will depend on an individual customer’s account activity. I did note though that the amounts transferred were significantly greater in the cases Mr H’s representative has drawn this service’s attention to.

Did Metro do enough to recover Mr H’s funds?

I’ve also considered Metro’s actions once it was made aware of the scam. Mr H reported the scam on 10 November 2021. On the same day, Metro contacted most of the banks that received Mr H’s funds to see if any funds remained. Each of the banks that Metro contracted on 10 November confirmed that no funds remained, so there was nothing more Metro could have done.

Metro appears to have made an error and not contacted the bank that received the first payment of £800 until January 2022 so we contacted this bank to see if the delay had an impact on the recovery of funds. I’ve been provided with evidence that demonstrates the funds were removed very soon after they entered the receiving account, meaning they had been removed by the time Mr H reported the scam to Metro. In the circumstances, I don’t consider Metro’s delay had any impact on Mr H.

Overall, I’m really sorry that Mr H has lost money in a cruel scam, but I can’t fairly ask Metro to refund him.

My final decision

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

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr H to accept or reject my decision before 27 February 2023.

Jay Hadfield
Ombudsman