

## **The complaint**

Mrs M is unhappy Starling Bank Limited ('Starling') hasn't refunded her the money she lost after falling victim to an authorised push payment ('APP') investment scam.

## **What happened**

The details of this case are well-known to both parties, so I don't need to repeat them at length here. In summary, Mrs M fell victim to a cryptocurrency investment scam.

Mrs M was contacted through a well-known social media platform by whom she thought was an acquaintance / friend. It appears the friend's account had been hacked – and it was a scammer messaging Mrs M. The scammer persuaded Mrs M to invest, advising that they had got back £12,000 after investing £1,000.

Mrs M made a payment of £1,800, on 24 November 2023, from her account with Starling to another person's individual account details that she had been provided by the scammer. Mrs M then made further payments (from a different bank account she held with another firm) in order to withdraw her profits. Unable to withdraw her profits, Mrs M realised she had fallen victim to a scam.

Mrs M contacted Starling (and her other banking provider), on 28 November 2023, to report the matter and to see whether her funds could be recovered or re-imbursed.

Mrs M's other bank ultimately re-imbursed her for the payments she had made.

Starling considered the case under the 'Contingent Reimbursement Model Code' ('CRM Code'). This is a voluntary code which Starling is a signatory of. 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.

Starling declined reimbursing Mrs M, as it said one of the exceptions in the CRM Code applies, in that it believes Mrs M didn't take reasonable steps to check if the payment was genuine.

Starling also contacted the receiving bank (the bank where Mrs M paid her funds to) but advised Mrs M that it hadn't been informed of an outcome that they were able to recover the amount sent.

Mrs M, unhappy with Starling's response, brought her complaint to this service. One of our Investigator's considered the complaint. In short, they agreed that Mrs M had acted without a reasonable basis for belief when making the payment. They considered the returns being promised, were too good to be true, and to such an extent that it should have given Mrs M cause for concern that all wasn't as it seemed. And given the value of the payment they didn't consider, under the CRM Code, that Starling was required to display an effective warning as part of the payment process. So, our Investigator agreed Starling had acted fairly and reasonably in choosing to decline reimbursement under the CRM Code.

Mrs M didn't accept the Investigator's opinion and so the complaint has been passed 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.

I'm sorry to disappoint Mrs M but I'm not upholding her complaint. I know she's been the victim of a scam. But I don't believe Starling has acted unfairly or unreasonably in its answering of the complaint. I'll explain why.

There's no dispute that Mrs M authorised the payment that is the subject of this complaint, even though she did so as a result of being deceived by a fraudster. Broadly speaking, under the account terms and conditions and the Payment Service Regulations 2017, she would normally be liable for it. But that isn't the end of the story.

Where a customer has been the victim of a scam it may be appropriate for the bank to reimburse the customer, even though payments have been properly authorised. Of particular relevance to the question of what is fair and reasonable in this case is the CRM Code.

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 and it is for Starling to establish that a customer failed to meet their requisite level of care under one of the listed exceptions set out in the CRM Code.

Under the CRM Code, a Sending Firm (in this case Starling) may choose not to reimburse a customer if it can establish that\*:

- ...The customer made payment 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 ignored what the CRM Code refers to as an 'Effective Warning' by failing to take appropriate action in response to such an effective warning.

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

In this case, I think Starling has been able to establish that it may choose not to reimburse Mrs M 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, including the characteristics and complexity of the scam, I don't think Mrs M had a reasonable basis for believing the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.

In order to determine whether this exception to reimbursement applies, I must ask if she made the payment she did whilst having a reasonable basis for belief that all was genuine. Having carefully reviewed everything I'm afraid I don't find that's the case. I'll explain why.

Mrs M received contact from an acquaintance / friend. While Mrs M sought to ensure that the person was indeed who they claimed to be, by requesting proof of identity – and received an image of the acquaintance's driving license – I also have to bear in mind what was being asked of Mrs M, in terms of being advised to invest and also – what was promised to her in regard to the investment.

Overall, having looked at the evidence and testimony provided by both parties, I consider there to have been enough warning signs that ought to have caused Mrs M concern that she was being scammed, which she does not appear to have reasonably acknowledged or acted upon.

It seems to me that Mrs M took what she was being told at face value. Mrs M was told by the acquaintance, through social media messaging, that they had invested £1,000 and got back £12,000 (so had made £11,000 in profit) and had seemingly achieved this in a very short space of time. Mrs M was also told the investment was 100% legitimate and was guaranteed. These returns are simply too good to be true. And I can't see that Mrs M questioned how such high levels of returns could be guaranteed or realised and within such a short time frame also. Mrs M also doesn't appear to have carried out any checks. I note Mrs M, in making the initial payment from Starling, made the payment to an individual / personal account – which to my mind is questionable and ought to have given her pause for thought. I say this because I think it is reasonable to suggest that if it was a legitimate investment firm or trading platform – then Mrs M would be making payments either to an account in a firm's name or to an account in her own name if a legitimate trading platform.

As a result, I'm satisfied Mrs M should've had reasonable cause for concern that things might not be as they seem at the time she made the initial payment from Starling. But it doesn't appear that she made adequate enquiries into the legitimacy of things or what she was being told. I might understand how in isolation any one of these things may not have prevented Mrs M from proceeding. But when taken collectively I think there were sufficient red flags here that reasonably ought to have led Mrs M to have acted far more cautiously than she did.

So, I think Starling can fairly rely on one of the exceptions to reimbursement – that Mrs M made the payment without a reasonable basis for believing that the payment was for genuine goods or services and/or the person or business with whom she transacted with was legitimate.

*Should Starling have done anything else to prevent the scam?*

Good industry practice requires that regulated firms such as Starling engage in the monitoring of customer accounts and to be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. And under the CRM Code, where it identified a risk of a customer falling victim to an APP scam, it was required to provide that customer with an 'effective warning'.

We now know, with the benefit of hindsight, that Mrs M was falling victim to a scam. But based on the information that was available to it at the time, I don't consider Starling would've had any reasonable basis for coming to that conclusion. I say this because the payment wouldn't have appeared out of character or unusual. The payment wasn't particularly large or remarkable. So, I don't think the CRM Code required that Starling display an effective warning as part of the payment process, and I'm not persuaded it would've had any grounds for intervening to question the payment further with Mrs M before allowing it to be processed.

### Recovery of funds

I have also considered whether Starling did all it could to try and recover the money Mrs M lost. Starling was limited in terms of what it could do here; it could only ask the Receiving Firm to return any money that remained in the recipient account. It needed to make enquiries quickly for the best chance of recovery. The evidence I've seen persuades me Starling did act quickly. While Mrs M, after realising she was the victim of a scam, reported the matter promptly – it was unfortunately four days after she had made the payment. Sadly, it is common for fraudsters to withdraw or move the money on as quickly as possible. So, while Starling didn't receive a response from the beneficiary bank advising funds remained – it was sadly always likely the case that the funds had been moved on.

I note Mrs M has referenced that she was the victim of a scam – and should be reimbursed. And Mrs M points to the new APP scam reimbursement rules ('ASR') that have come into force. However, the ASR was brought in with an effective date of 7 October 2024, and isn't retrospective. As Mrs M's payments were in 2023 – it means the newly introduced ASR isn't applicable.

I'm sorry Mrs M lost her money in this way, and I don't underestimate her strength of feeling and why she thinks this money should be returned. But for the reasons explained, I don't find that she had a reasonable basis for believing the payment was for genuine goods or services; and/or the person or business with whom she transacted was legitimate. So, I consider it was fair and reasonable for Starling to decline to reimburse her for her losses under the CRM Code.

### **My final decision**

For the above reasons, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 9 May 2025.

Matthew Horner  
**Ombudsman**