DRN-5239026

The complaint

Miss A is unhappy Starling Bank Limited ('Starling') hasn't refunded her the money she lost after falling victim to an Authorised Push Payment ('APP') holiday purchase 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, Miss A fell victim to a holiday purchase scam.

In June 2024, Miss A was looking to go on holiday with some family members. Miss A says a friend of hers recommended someone who could get discounted rates on holiday packages. Miss A believes her friend had used them before, not to purchase a holiday package but had possibly bought some clothes. Miss A contacted the supposed seller through a well-known social media and instant messaging app which I'll call 'S'.

Miss A says the seller's profile on S showed they could get discounted holiday packages and also had links to customer reviews. Miss A contacted the seller and liaised with them in regard to the holiday package she wanted. Miss A sent across what holiday she had already been looking at, which she had found through a genuine UK-based travel retailer, and the seller showed Miss A that they could get the same package, through the same travel retailer, but at a discounted price. Miss A was of the understanding that the seller either worked for the genuine travel retailer or worked alongside it, as the seller was able to apply what she thought was a promotional code to get a discount.

Miss A then received an email which she said appeared to be from the genuine travel retailer which had a link to pay. But as this was from the genuine travel retailer, Miss A contacted the seller to advise that if she proceeded in this way, then she wouldn't get the discount. Miss A explained the seller apologised and advised there was likely an error. The seller then explained he would make the booking with the discount, and Miss A, believing everything to be genuine, sent £950 (which was 50% of the total package price) on 8 July 2024 to the account details she had been provided with. When Miss A was making the payment, she said that the name of the account didn't match (often referred to as 'Confirmation of Payee') and so she asked her friend to confirm the payee's name. Miss A was then provided with the name that subsequently matched and Miss A proceeded with the payment.

Miss A didn't receive a confirmation or invoice confirming the holiday had been booked, and the seller then stopped responding to any contact and subsequently blocked her also.

Realising she had been the victim of a scam, Miss A contacted Starling on 11 July 2024 to report the matter and to see if it could recover or reimburse her funds.

Starling subsequently contacted the Receiving Firm (the beneficiary bank where the funds had been sent to), but unfortunately only £1.76 remained that could be recovered and returned to Miss A.

Starling also considered whether Miss A was due a refund of the funds she lost. Starling considered the case under the Lending Standards Board 'Contingent Reimbursement Model' (referred to as the 'CRM Code') which it was a signatory of at the time of the payment.

The CRM Code was implemented to reduce the occurrence of APP scams. The CRM Code required firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances.

Under the CRM Code, where there is a failing by either the Sending Firm or Receiving Firm, they may be required to reimburse the customer. And, importantly, the customer may also be required to share some responsibility for the loss if it is determined that one of the exceptions to full reimbursement, as set out within the CRM Code, applies.

Starling didn't agree that it was liable to reimburse Miss A for the funds she had sent. It considered the seller wasn't a verified travel agent who was 'ATOL' or 'ABTA' protected, and a professional company or travel agent wouldn't conduct their business through 'S'. It also considered that an unverified individual or company offering discounted deals ought to have been a cause for concern. And that the seller also didn't appear to have any other genuine online presence such as a company website or a company that was listed on Companies House or registered with the ATOL and ABTA registers.

Unhappy with Starling's response, Miss A brought her complaint to this service. One of our Investigator's looked into things and didn't uphold the complaint. In short, they considered one of the exceptions to re-imbursement under the CRM Code applied, in that Miss A made the payment without having a reasonable basis for believing that the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate. They considered there were some concerning features that ought to have given Miss A cause for concern that all might not be 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.

Miss A didn't agree with the Investigator's opinion. So, as agreement couldn't be reached, 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 aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. And that is whether it was fair for Starling to decline reimbursing Miss A under the provisions of the CRM Code or whether there was any other failing by Starling that meant Miss A's loss could have been prevented. If there's something I've not mentioned, it isn't because I've ignored it. I haven't. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

I'm sorry to disappoint Miss A, but I'm not upholding her complaint. I know she's been the victim of a cruel scam, and I don't doubt that these events have had a significant impact on her. But I don't believe Starling has acted unfairly or unreasonably in not reimbursing Miss A under the provisions of the CRM Code. I'll explain why.

There's no dispute that Miss A authorised the payments that are 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 (which are the relevant regulations here), 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. Under the CRM Code, a Sending Firm may choose not to reimburse a customer if it can establish that*:

- 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 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 Miss A 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.

I have taken into account all of the circumstances of this case, including the characteristics and complexity of the scam. Having done so, I think the concerns Starling has raised about the legitimacy of the transaction Miss A made are enough to support its position that she didn't have 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. I'll explain why.

In order to determine whether this exception to reimbursement applies, I must ask if Miss A made the payment she did whilst having a reasonable basis for belief that all was genuine. I'm afraid I don't find that's the case having considered all the testimony, call recordings and evidence presented to me by both parties.

I do accept, having listened to the calls Miss A had with Starling when reporting the scam, and with our service when referring the complaint and then also with our Investigator, that there were some characteristics of the scam that might have seemed plausible to Miss A. But I also consider there were areas that should have given her a greater cause for concern that things might not be legitimate or as they seem.

I think it is important to note that Miss A was told by her friend of someone who can get discounts, and her friend had used them before. Although it appears the friend didn't really know them, had used them seemingly some time ago and hadn't also used them for a holiday package purchase. And I'm mindful that this 'seller' was operating through a social media account with 'S', and with a profile that didn't have a company name and wasn't a travel agent. The profile seemingly had just a 'letter' as their profile name. And I think Starling raised a notable point in that the seller didn't seemingly have any other online presence other than on social media with 'S'.

Given this seller was potentially promoting themselves as being able to get discounts on genuine holiday packages but wasn't a registered travel agent/company/business – or didn't have a company website, I think it ought to have led to Miss A considering how any potential discounts could actually be achieved and whether this was a legitimate seller carrying out genuine activity. Our Investigator carried out an online search which approximately estimated the package would have cost around £1,000 - £1,200 per person. So, between £3,000 and £3,600 for three people. And Miss A was being quoted £1,900 in total for three people. So around 30% less (conservatively). And Miss A, having looked at the genuine travel retailers website's package, reasonably ought to have been aware of the price at face value.

So, I think Miss A ought to have been wary from the outset. I accept that Miss A in liaising with the scammer was showed a genuine travel company's website – one that she had used to find the holiday package in the first place and possibly thought that the 'seller' either was an employee for that travel company or that they worked alongside them as they applied what Miss A thought was a promotional code. But nothing was seemingly asked by Miss A to confirm whether this individual worked for the genuine travel company, or, if he worked alongside them, what was his travel company's name.

Miss A prior to making the payment, was sent a link in which to pay for the holiday package, and Miss A says this had come from the genuine travel company. And it is most likely that the scammer possibly did this, so starting to reserve the holiday package with the genuine company – meaning it could be sent through to Miss A. And I accept that Miss A might have found that quite plausible. But I also have to consider that Miss A upon receipt of that email, contacted the seller and advised that if she clicked on the link to pay, it would be her paying the genuine travel company and it wouldn't have the discount applied. And this led to Miss A agreeing to send the money directly to the seller's own personal account. I think that ought to have raised some concern. Miss A was sending money to an individual's account and not a business account, wasn't paying the genuine travel retailer itself and this payment was also to a person she hadn't met, who wasn't operating under a company name or website, and wasn't a registered travel agent / broker.

I might understand how in isolation any one of these things I've mentioned above may not have prevented Miss A from proceeding. But when taken collectively I think there were sufficient red flags here that reasonably ought to have led Miss A to have acted far more cautiously than she did, and ask questions of the seller, or carry out some additional checks to ensure the seller was in fact acting in a legitimate capacity.

Overall, I think there were some warning signs here, and Miss A needed to approach the purchase with considerable caution to ensure that she was dealing with a legitimate seller.

So, I think Starling can fairly rely on one of the exceptions to reimbursement – that Miss A made the payment without 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.

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 Miss A 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 believing that its customer was falling victim to an APP scam at the time the payment was made. So, when considering the CRM Code, it wasn't required to provide its customer with an 'effective warning' – as defined by the CRM Code. I say this because I don't consider the payment appeared so out of character or unusual and the payment wasn't particularly large or remarkable. So, I can't fairly or reasonably conclude that Starling hasn't met its obligations under the CRM Code.

Also, I'm not persuaded it would've had any grounds for intervening to question the payment any further with Miss A, such as through human intervention, before allowing it to be processed. So, I can't fairly say it would have been able to prevent Miss A's loss.

Recovery of funds

I have also considered whether Starling did all it could to try and recover the money Miss A 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 Miss A had reported the matter – it was unfortunately three days after she had made the payment. Sadly, it is common for fraudsters to withdraw or move the money on as quickly as possible. And that was the case here with the Receiving Firm confirming in its response to Starling that nearly all the funds had already been utilised and only £1.76 was recoverable.

Summary

With all of this in mind, I am sorry that Miss A lost her money this way and fell victim to a cruel scam and is out of pocket as a result. And I don't underestimate her strength of feeling and why she thinks this money should be returned in full. 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 they transacted was legitimate.

So, I don't consider Starling has acted unfairly or unreasonably in not reimbursing Miss A under the provisions of the CRM Code.

And it isn't liable for the loss either, as I don't find it could have reasonably prevented her loss or recovered any further funds as they had already been moved on or utilised already.

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 Miss A to accept or reject my decision before 5 September 2025.

Matthew Horner
Ombudsman