

## The complaint

Miss D is unhappy that Starling Bank Limited won't refund the money she's lost to a scam.

## What's happened?

Miss D found a company selling wholesale clothing items ('the seller') on a popular social media platform. She contacted the seller and agreed to purchase 200 items of clothing for £1,000, to be delivered within 10 days of payment. From her conversations with the seller, she was expecting to receive vintage sweatshirts in an almost new condition.

On 17 July 2020, Miss D transferred £1,000 to the seller from her Starling bank account. But six weeks later, she says she still hadn't received her order and when she chased the seller, they kept making excuses – she was even provided with a tracking number for a parcel going to someone else. Eventually, she realised she had been scammed and reported the fraud to Starling. Since then, Miss D says that:

- the seller became nasty and threatening towards her – they wanted her to withdraw her fraud claim.
- she has received a package from the seller containing around 60 pieces of poor-quality/counterfeit clothing.
- she has found evidence of the seller scamming other people.

Starling contacted the beneficiary bank on the same day that Miss D reported the fraud to it, but no funds were returned, and Starling declined to reimburse Miss D under the Lending Standards Board's Contingent Reimbursement Model ('CRM Code'). It said that it had sufficient fraud prevention measures in place, but Miss D didn't take reasonable steps to check the payment she was making was genuine. It also said that this matter could be considered a buyer-seller dispute.

Miss D was unhappy with Starling's decision not to reimburse her. So, she asked this Service to consider her complaint.

## What did our investigator say?

Our investigator didn't uphold Miss D's complaint. He said that this matter is a civil dispute, and civil disputes are not covered by the CRM Code.

Miss D didn't agree with our investigator. In responding, she maintained that the seller is a liar and a fraudster, and she provided evidence to show that the seller has engaged in criminal activities with other victims.

The complaint was passed to me to decide.

## My provisional decision

I issued my provisional decision on 15 March 2022. I'll set out what I said below.

Starling has signed up to the CRM Code, and it was in force when Miss D paid the seller. Under the CRM Code, the starting principle is that a firm should reimburse a customer who has been the victim of an Authorised Push Payment ('APP') scam. But the CRM Code is quite explicit that it doesn't apply to all APPs. It says:

*"DS2(2) This code does not apply to:*

*(b) private civil disputes, such as where a Customer has paid a legitimate supplier for goods, services, or digital content but has not received them, they are defective in some way, or the Customer is otherwise dissatisfied with the supplier."*

I've considered the evidence Miss D has provided – including the messages she sent to and received from the seller, pictures of the items of counterfeit/poor-quality clothing she received from the seller, and the messages the seller has sent to other individuals. Having done so, I'm not persuaded that the seller is a legitimate supplier for goods. I acknowledge that the seller continued to correspond with Miss D after receiving her payment, and that they sent her some items of clothing (albeit not in the condition or quantity that Miss D was expecting). This is undoubtedly unusual in cases of fraud. But overall, considering what the seller has said and done, I'm satisfied that they set out to defraud Miss D.

The CRM Code requires firms to reimburse customers who have been the victims of APP scams, like the one Miss D has fallen victim to, in all but a limited number of circumstances. Starling has argued that two of the exceptions apply in this case. It's said that Miss D ignored an effective warning it gave during the payment journey and she made the payment without a reasonable basis for believing that the payee was the person she was expecting to pay, the payment was for genuine goods or services and/or the person or business she was transacting with was legitimate.

The CRM Code says:

- SF1(2)(e) As a minimum, Effective Warnings should meet the following criteria*
- (i) Understandable – in plain language, intelligible and meaningful to the Customer*
  - (ii) Clear – in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's [Financial Conduct Authority] Principles for Businesses*
  - (iii) Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;*
  - (iv) Timely – given at points in the Payment Journey most likely to have an impact on the Customer's decision-making;*
  - (v) Specific – tailored to the customer type and APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*

Starling has said that it gave Miss D a sufficient warning and took reasonable steps to help her protect herself from financial harm. When Miss D added the seller as a new payee, it would have displayed a message which said:

*“Could this be part of a scam? If in doubt, just stop here and visit our website to learn more about fraud”.*

And its website clearly refers to the type of scam Miss D fell victim to, saying:

*“We’re all partial to a spot of online shopping – but you should always be careful when you’re using an online marketplace and not a recognised retailer. Fraudsters will sometimes advertise high value items such as designer watches, vehicles and games consoles/the latest tech on social media or online marketplaces – remember, if it sounds too good to be true, it probably is!! You may also be pressured into making a payment quickly and advised that you are unable to make a payment by card or Paypal which offer more protection to the payer. You should always be cautious about sending money to an individual you haven’t met, for an item you haven’t seen – especially if the website doesn’t offer payer protection or you are asked to bypass normal payment methods on that website.”*

Miss D has said she doesn’t recall Starling giving her a fraud warning. Based on her recollections, I think there’s a good chance she didn’t take the required, extra step of manually visiting Starling’s website to receive a fraud warning. But even if she did, I’m not satisfied that the requirements of the effective warning exception were met. Specifically, I don’t think the warning given was specific or impactful enough to be considered an effective warning under the terms of the CRM Code.

The warning doesn’t really bring to life what the type of scam Miss D fell victim to looks like or highlight the common features of the scam. It mainly refers to purchasing high value items from an online marketplace at a price that’s too good to be true. This, of course, is not what happened in Miss D’s case. She found the seller on a social media platform, agreed a seemingly reasonable price for goods she wanted to purchase that weren’t of high value and arranged a bank transfer to the seller. The warning also doesn’t set-out the potential consequences of continuing with an irrevocable payment if it turns out a scam is underway as it is required to do under the CRM Code. Overall, I’m not persuaded that the warning is likely to have positively affected a customer’s decision-making in a manner whereby the likelihood of the scam succeeding was reduced.

If Starling had brought to life what this type of scam looks like with specific and impactful information, and explained the potential consequences of going ahead with the payment, then I think this would’ve been important information in the context of this scam that would’ve affected Miss D’s decision making.

I’ve also thought about whether Miss D had a reasonable basis for belief. I’ve considered what steps she took to reassure herself about the legitimacy of the transaction, and whether it was reasonable for her to proceed with paying the seller.

From the text messages Miss D has sent us, I can see that she requested photos and videos of the clothing she could expect to receive from the seller, and her requests were fulfilled to her satisfaction. But I can also see that Miss D was aware there were more secure methods of paying the seller than bank transfer, and she had reservations about paying the seller in this way. But she ultimately decided to proceed with the payment regardless. And I can see that when Miss D reported the fraud to Starling, it asked her *“How did you verify that the person you were expecting to pay was genuine?”* Miss D replied that she *“Attempted to click their website link in their bio on [social media platform] which lead to a dead end and did not work, otherwise no attempt was made.”*

Given the reservations Miss D had about paying the seller via bank transfer and that she found their website link led to a dead end, I would've expected Miss D, or anyone else, to be put on guard. But, by her own admission, Miss D didn't carry out any extra checks or make any substantial attempts to protect herself as I would've expected her to do – such as, for example, taking steps to research the seller or verify they were genuine.

Overall, I'm not persuaded that Miss D had a reasonable basis for belief in this case.

As Starling failed to provide Miss D with an effective warning and that failure is likely to have had a 'material effect' on preventing the scam, but Miss D also lacked a reasonable basis for belief in paying the seller, Miss D should be reimbursed 50% of her loss under the provisions of the CRM Code.

Finally, I've considered whether Starling took reasonable steps to recover Miss D's funds, and I think it did. It's evidenced that it contacted the receiving bank on the same day that Miss D reported the fraud to it, but no funds have been returned. I'm not persuaded that Starling could've taken any further action that would've led to the recovery of Miss D's funds.

For the reasons I've explained, I've provisionally decided to uphold this complaint in part and instruct Starling to:

- reimburse 50% of Miss D's loss; plus
- pay 8% simple interest on that sum from the date that Miss D should have been reimbursed under the CRM Code to the date of settlement.

#### Responses to my provisional decision

In summary, Miss D said:

- Starling has still not put in place any extra warnings to prevent others from making the same mistake.
- She thinks Starling could've taken further steps to recover her funds – it was aware they had been sent to a 'criminal'.
- She accepts that she should have made additional checks to verify the seller was genuine. But she was young and just starting out with her business venture at the time. She had not come across anything like this before or had a negative experience which would put her on guard. When she saw the seller's photos and videos of the clothing she could expect to receive from them, she was happy that she'd found a wholesaler that she thought larger shops received their stock from.
- When it comes to wholesalers, other people are very secretive in revealing their trusted suppliers, or information on their suppliers.
- The seller's website link leading to a dead end was not significant to her as other wholesalers mainly operate via social media platforms and have websites just to showcase photos and provide further information.
- She was happy to compromise if that meant building a long-term relationship with a new supplier.
- The scam has put a strain on her finances, and she would like to be fully reimbursed for her loss.

Starling maintained that it had provided Miss D with an effective warning and that she made the payment without a reasonable basis for belief, but it agreed to settle the complaint in line with my provisional 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 appreciate that the scam has had a negative impact on Miss D's finances, and that she would like Starling to fully reimburse her. But in responding to my provisional decision, I don't think she's given me any new information which persuades me that Starling should reimburse more than 50% of her loss.

As I have previously explained, I'm not persuaded that Starling provided Miss D with an effective warning on this occasion, and I have seen that Starling did all I would reasonably expect it to do to recover Miss D's funds from the beneficiary account. I won't explore these elements further as no new evidence has been provided in this respect.

Miss D has made some further comments about her reasonable basis for belief. I appreciate that she was young and inexperienced when she made the payment. And I can see from the evidence that her requests for photos and videos of the clothing she could expect to receive from the seller were fulfilled to her satisfaction. I don't doubt that this gave her some reassurance. But from what I've seen, she had reservations about paying the seller via bank transfer but went ahead with the payment regardless. And I still think she ought reasonably to have been put on guard when the seller's website link led to a dead end. She's said that other wholesalers trade via social media platforms and their websites merely showcase photos and provide further information, but this is different to a website link not working.

Ultimately, Miss D accepts that she should have made additional checks to verify the seller was genuine, and I agree with her. She says she was happy to compromise in order to build a long-term relationship with a new supplier, and I can understand why she was willing to take the risk involved in sending the payment. But overall, I can't reasonably conclude that she had a reasonable basis for belief on this occasion. So, I'm still persuaded that she should be reimbursed 50% of her loss under the provisions of the CRM Code.

## **My final decision**

For the reasons I've explained, my final decision is that I uphold this complaint in part and instruct Starling Bank Limited to:

- reimburse 50% of Miss D's loss; plus
- pay 8% simple interest on that sum from the date that Miss D should have been reimbursed under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 27 April 2022.

Kyley Hanson  
**Ombudsman**