

## The complaint

G complains that Barclays Bank UK PLC (Barclays) won't refund money it lost in a scam.

## What happened

*What G says:*

In October 2022, G placed an order to buy goods from a company in China (which I will call 'A'). Three days later, G changed the specification of the order. On 17 November 2022, the company in China ('A') sent a pro forma invoice and G confirmed the order and paid the amount due – which was £2,533 plus charges - £2,548 was debited to G's Barclays Premium account on 21 November 2022.

The business manager at A then said the order was delayed due to Covid. G asked for an official letter to say this. The business manager then said the price had increased, and another payment of USD3,000 (£2,533) was needed before the factory would start production.

G terminated the contract and asked for a refund. Contact continued via WhatsApp and WeChat. Then, on 19 December 2022, the business manager said they didn't have the money and it was 'with her boss'. She gave different numbers for WhatsApp and WeChat, but after a short period these numbers were blocked. G contacted Barclays on 10 January 2023 to report the matter.

*Payment:*

Date	Transaction	Amount
21 November 2022	International payment (USD2,950.44) – from Barclays Premium account	£2,533
	Charges	£15
<b>Total Loss</b>		<b>£2,548</b>

(continued)

G says it did sufficient due diligence on A. It 'googled' it and saw its factory, its warehouse of products, saw a photo of the business manager and the numbers on its website were those they used to contact A. A also had a quality accreditation on its website.

G says the lost money has left a big hole in its cashflow and it may now need to cease trading. G says Barclays should reimburse it for the fraud/scam under the 'APP Code

pledge' – whereby Barclays should refund victims of Authorised Push Payment scams.

*What Barclays said:*

Barclays discussed G's complaint with its director and declined to refund the money.

*Our investigation so far:*

G brought its complaint to us. Our investigator said it appeared to be a civil dispute and not a scam. As far as she could see, A was a legitimate trading company and its terms and conditions outlined its complaint procedures in the event of a dispute. So – she said G should contact A to do that.

G disagreed. It said it was the victim of a scam. It said cloned/ fake websites had been set up, together with other umbrella and proxy companies, with fake company profiles. The method of the scam was to attract a buyer (such as G) by reference to the reputable website, and then issue a pro-forma invoice with fake company credentials. The fake website has now been taken down.

A asked that an ombudsman looks at its complaint, and so it has come to me to make 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.

As a first step, I need to decide whether this was a scam (where a scammer takes money from a customer with no intention of providing any services or returning the money to them) or a civil dispute (where a payment is made to a legitimate trading company or business, but the promised services or products don't materialise, or are sub-standard).

Looking at the evidence that A has provided, I'm persuaded that this was a scam. I say that as:

- G has shown us that several websites were being used.
- The fake website has been taken down.
- A was given new WhatsApp and WeChat numbers, and these were then blocked and communications ceased.
- A doubled the price of the goods within a few days.
- A (or the scammer company) showed no signs of dealing with G, listening to its complaint, or renegotiating the contract - or trying to find an agreeable outcome for both parties.

This has all the signs of a scam – rather than G dealing with a reputable company.

So – I will look at this complaint as an Authorised Push Payment scam case. The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case. That is because it applies to faster payments made to a UK beneficiary– and in this case, the payments were to an overseas account. So – a refund using the CRM Code principles cannot be considered.

But, taking into account the law, regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Barclays to take additional steps or make additional checks before processing a payment in

order to help protect its customer from the possibility of financial harm from fraud.

I'm sorry to hear that G has lost money in a scam. It's not in question that G authorised and consented to the payment in this case. So although G didn't intend for the money to go to a scammer, it is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Barclays should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- 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 (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.
- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I need to decide whether Barclays acted fairly and reasonably in its dealings with G when it made the payment, or whether it should have done more than it did. I have considered the position carefully.

The first consideration here is: if the payment was of a sufficient size and was out of character with how G normally used its accounts – then we would expect Barclays to have intervened and spoken to G about it. In this case, I don't consider Barclays acted unfairly or unreasonably in allowing the payments to be made.

**(continued)**

Whilst I understand the loss has had a big impact on G, I don't consider the payments were so out of character that Barclays ought reasonably to have had concerns that G may be the victim of fraud. I am mindful of the fact the payments were made from a business account where larger payments aren't unusual. I reviewed both the statements for G's current account and premium account. There were large payments made of a similar amount to the disputed payment – such as:

*Barclays Premium account:*

- 6 October 2022: £2,000
- 20 September 2022: £1,000
- 12 September 2022: £1,200
- 5 September 2022: £3,000
- 12 July 2022: £3,000
- 6 June 2022: £1,096
- 9 February 2022: £1,699

*Current account:*

- 6 October 2022: £2,000
- 12 September 2022: £1,000
- 5 September 2022: £3,000
- 12 July 2022: £3,000
- 6 June 2022: £1,068

I accept that some of the payments were between the premium account and current account but nevertheless, they were payments of a similar amount to the disputed payment. And – this, taken together with the fact that this was a trading business account, means I’m persuaded that we wouldn’t have expected Barclays to have intervened and questioned the payment.

There’s also a balance to be struck: Barclays has obligations to be alert to fraud and scams and to act in their customers’ best interests, but they can’t be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think Barclays acted reasonably in processing the payments.

*Recovery:*

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Barclays took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money.

I can see that Barclays contacted the recipient bank in February 2023 to ask if the funds could be returned. In cases where an overseas bank is concerned, this process can take a lot longer than where a UK bank is involved, and the bank must ask the beneficiary’s permission to return the funds.

In March 2023, I can see the recipient bank responded to say the money was in the beneficiary’s account – but it was for G to contact the beneficiary to ask for a refund. I know that won’t be helpful to G – as it means it is back to ‘square one’, but as far as Barclays’ obligations are concerned, they did what was expected under the regulations and best practice.

G has argued strongly that this was a sophisticated scam, and therefore Barclays should refund the money – but as I’ve set out here, the payment wasn’t of a size, or was unusual enough, to have reasonably expected Barclays to have intervened and stopped it. So – I don’t hold Barclays liable for the amount of the payment.

**My final decision**

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask G to accept or

reject my decision before 4 December 2023.

Martin Lord  
**Ombudsman**