

## The complaint

Mrs O, on behalf of Company T, complains that Barclays Bank UK PLC didn't do enough to protect her from the financial harm caused by a job scam, or to help her recover the money once she'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

The complaint is brought by Mrs O on behalf of Company T, which holds a business account with Barclays.

Mrs O received a WhatsApp message from someone I'll refer to as "the scammer" who claimed to work for a recruitment agency. They told her about a part-time job working for a well-known company I'll refer to as "C". The role would require her to rate movies and 'like' social media pages for marketing purposes, and Mrs O could earn £15 to £20 per day.

The scammer also told her about a role for "F", which worked with digital influencers to promote brands. The role would require her to 'like' and follow social media pages and posts to help increase the exposure of the brands. She would also be required to complete tasks which she would have to pay for in advance using cryptocurrency. The scammer explained she would earn a commission on each task and that she could earn £80 per day.

Ms C had been looking for work and was satisfied the opportunities were genuine because she googled the recruitment company and C was very well-known. She was also added to a chat group with others claiming to be doing the same role. She wasn't given any employment documents, but the scammer did provide a written job description.

The scammer told Mrs O how to make a withdrawal on the platform and told her to buy cryptocurrency and load it onto an online wallet. Between 25 July 2023 and 31 July 2023, she transferred funds from her personal Barclays account to T's business account before making twelve faster payments to cryptocurrency and EMI accounts in her own name. She also made payments to the scam from an EMI account I'll refer to as "W".

Mrs O realised she'd been scammed when the tasks increased in value, and she was unable to make any more withdrawals. She complained to Barclays about funds sent from both her personal and business accounts, and it refunded payments she'd made from her personal account.

Regarding the payments from Mrs O's business account, Barclays said the transactions weren't covered under the Contingent Reimbursement Model ("CRM") Code because the payments were to accounts in Mrs O's own name. It also said there was no loss to T because Mrs O had used funds from her personal account to fund the payments.

Mrs O complained to Barclays with the assistance of a representative who said she had never purchased cryptocurrency before and the largest payment from the account in the 12

months prior was £442.26, so the frequent and large payments should have been concerning.

They said Mrs O was asked for the purpose of the payment on the fourth payment when she explained she was purchasing cryptocurrency and had it asked why, she'd have explained that she'd been approached on WhatsApp and was making payments for a job, she didn't have an employment contract and the earnings were unrealistic. With this information, it would have been obvious that she was being scammed and the loss would have been prevented. They said Mrs O had explained that there was no agreement between the scammer and T, but she used the business account to pay taxes on the potential income.

Our investigator didn't think the complaint should be upheld. He explained that Mrs O had transferred funds from her personal account to T's business account, and payments were made towards the scam from there. He commented that there was no agreement in place between T and the scammer, rather Mrs O was contacted personally and offered a job. He explained that as the funds were used in a personal capacity, there was no loss to T, so she couldn't ask Barclays to refund the payments back to T.

He also said there would have been no chance of a successful recovery because the funds were moved to an account in Mrs O's name before being moved onwards to the scam. And for the card payments, she'd paid a legitimate cryptocurrency exchange and would have received a service which would have involved changing the payments into cryptocurrency, before sending it to the wallet address she supplied it with.

Mrs O's representative has asked for the complaint to be reviewed by an Ombudsman arguing that the payments were for potential revenue driving tasks and T was the beneficiary of the potential revenue. They've reiterated that the payments were out of character and that Barclays should have intervened.

# 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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons.

The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mrs O says she's fallen victim to, in all but a limited number of circumstances. But the Code doesn't apply to these payments because they were to accounts in Mrs O's name.

I'm satisfied Mrs O 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although she didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of the bank account, T is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mrs O didn't intend her money to go to scammers, she did authorise the disputed payments. Barclays is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

I consider the crux of this complaint is the question of whether these payments were made to benefit T as a business, or to benefit Mrs O personally.

Initially Mrs O said there was no agreement between the scammer and T, but she used the business account to pay taxes on the potential income. She has since said T was the beneficiary of the potential revenue.

I find this testimony contradictory because the initial comments indicate the agreement was between Mrs O and the scammer, which suggests the payments from T's account were for her personal benefit. This is inconsistent with Mrs O's later explanation that T would benefit from the potential revenue.

Where there is contradictory evidence, as I find there is here, I am required to reach my findings on the balance of probabilities – in other words on what I consider to be most likely given the information available to me.

I consider it relevant here that Mrs O had transferred funds from her personal account to the business account before paying them out to the scam. The nature of T's business wasn't related to the nature of the tasks Mrs O expected to by earning commission on, and her explanation of having used the account only for tax purposes was the initial explanation.

While I cannot know for certain what the intended beneficiary for the commission was, I find it is more likely than not it was intended for the personal benefit of Mrs O, not the business of T and that she was essentially using T's account to transfer her own personal funds. Because of this, I'm satisfied that T hasn't suffered a loss – Mrs O has, so I can't fairly ask Barclays to reimburse funds to T.

### Recovery

I don't think there was a realistic prospect of a successful recovery because Mrs O paid an account in her own and moved the funds onwards from there.

#### My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 21 April 2025.

Carolyn Bonnell
Ombudsman