DRN-6034453

The complaint

M, a limited company, complains that Zempler Bank Limited won't refund the money it lost as the result of a scam.

M has been represented in this complaint by its director, Mr M.

What happened

In March 2025 Mr M received a phone call, claiming to be from Zempler. The caller explained that they were monitoring M's account, as they believed fraudulent activity was taking place. Unfortunately, the caller ultimately turned out to be a scammer, and I'll refer to them as "the scammer" in this decision, even though I appreciate that Mr M didn't realise that's who he was dealing with at the time.

Mr M says that the scammer had M's bank details, and his full name and address. They told Mr M that a payment for a significant amount was being attempted on M's account, and that he'd need to act quickly to stop the transaction. They instructed him to log onto M's account on Zempler's app, confirm that he could see the payment that was being attempted and authorise it. The scammer claimed that this was necessary to enable them to stop the payment.

Mr M has explained that he logged on to Zempler's app and it displayed an "in-app authorisation" for a payment of £17,110 to a luxury retailer. The caller reiterated that he needed to authorise the payment to stop the fraudulent activity. Mr M says the combination of the pressure of the call, the amount of the payment, the scammer's insistence and the speed with which he was told he needed to act was intense. He authorised the transaction, believing he was authorising Zempler to stop the payment.

Mr M has told us that his wife expressed concern that the call might not be genuine, and he then realised he might have been speaking to a scammer. So he ended the call. After a further call from the scammer, Mr M phoned Zempler to get M's card blocked. He says he was told its fraud team didn't work at weekends, and would contact him the next working day.

Zempler refused to refund the money on the grounds that Mr M had authorised the payment. And it said it couldn't pursue a chargeback claim.

Unhappy with Zempler's response, Mr M brought a complaint on behalf of M to this service.

One of our investigators considered the complaint and thought it should be upheld. In summary, she thought that the payment was so out of character for M's account that Zempler ought to have spoken to Mr M when the payment was attempted. And she thought that if it had done so, the scam would likely have been uncovered, and M's loss prevented. In the particular circumstances, she didn't think Mr M had acted unreasonably in authorising the payment. So she said Zempler should refund M's loss in full, with interest on the refund.

Zempler disagreed with the investigator's view, so the complaint's 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.

While I've taken into account everything that both parties have said, I've summarised the complaint in my own words, and have focused my decision on what I consider to be the key issues. This isn't intended as a discourtesy. It simply reflects our role as an informal dispute resolution service.

In broad terms, the starting position at law is that banks are expected to process payments and withdrawals that customers authorise them to make, in line with the terms and conditions of the customer's account.

It isn't in dispute that Mr M authorised the payment. He's told us that he did so under the mistaken impression that it would enable the transaction to be stopped. Nonetheless, the payment is regarded as authorised for the purposes of the Payment Services Regulations 2017, and M is presumed liable for its loss in the first instance. But that's not the end of the matter.

In deciding what's fair and reasonable, I'm required to take into account relevant law and regulations, regulators' rules, guidance, standards and codes of practice and, where appropriate, what I consider to have been good industry practice at the time. Taking those things into account, I think that at the time the payments were made, Zempler should have been doing the following to help protect its customers from the possibility of financial harm:

- monitoring accounts and payments to counter various risks, including fraud and scams;

- keeping 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) – especially given the increase in sophisticated fraud and scams in recent years, with which financial institutions are generally more familiar than the average customer;

- acting to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring that all aspects of its products, including the contractual terms, enabled it to do so;

- in some circumstances, regardless of the payment method used, taking additional steps, or making additional checks, before processing a payment, or, where appropriate, declining to make a payment altogether; and

- being mindful of - among other things – common scam scenarios, how fraudulent practices were evolving (including, for example, the common use of multi-stage fraud by scammers) and the different risks these can present to customers when deciding whether to intervene.

There's a balance to be struck. Banks have obligations to be alert to fraud and scams, and to act in their customers' best interests, but they can't reasonably be involved in every transaction. And I think it would have been reasonable for Zempler to consider a range of factors when deciding whether to take any additional steps before making the payment.

I've looked at M's bank statements covering a period of 12 months before the payment that M's complaining about. The account was generally used for day-to-day business spending. There'd been two transactions of £9,000 each to a business in one day in December 2024, but those were to another business which operated in broadly the same field as M, and M had made payments to that business before. The £17,110 payment was significantly higher than any individual payment from the account over the previous 12 months. M's business is centred on a particular industry which has no connection with luxury goods. All in all, I think it's fair to say that the payment for £17,110 to a luxury retailer was highly unusual for the account, and ought to have caused Zempler concern that M was at risk of financial harm from fraud.

Zempler has told us that it did flag the payment as high-risk. It's explained that that's why it was routed through 3D Secure for two-step authentication. Zempler says it considers the 3D Secure prompt to amount to a clear and explicit warning. It points out that it instructs the customer to approve a purchase, provides specific details about the transaction, and clearly states that it would never contact a customer to request approval for a payment. It adds that industry-endorsed guidance emphasises the customer's responsibility to read and act on fraud warnings. It's Zempler's view that where such warnings are clearly presented, but disregarded by the customer, it wouldn't be reasonable to hold the bank solely responsible for the resulting loss.

But I don't think the warning included in the 3D Secure process clearly fitted the circumstances here. Although the scammer had asked Mr M to authorise the payment, they told him that this was in order to *stop* the payment, rather than to approve it. And given the highly unusual nature of the payment for M, I consider that Zempler should, in any event, have been concerned enough to decline the payment and speak to Mr M to ask him about it.

I think it more likely than not that if Zempler had spoken to Mr M, it would quickly have become clear to both parties that the call he'd received wasn't genuinely from Zempler, and that it was a scammer who'd asked Mr M to authorise the payment.

I've thought about whether M should bear any responsibility for the loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all the circumstances of this complaint.

I accept that, with the benefit of hindsight, what Mr M was being asked to do might not seem fully plausible. But I've borne in mind that he was reassured by the fact that the scammer knew some of his personal details. And they put considerable pressure on Mr M, instilling a feeling of panic, where he believed he needed to act immediately to prevent a substantial loss. His ability to stop and rationalise was therefore limited. I think it would have taken an intervening act – such as a phone call from Zempler – to uncover that this was a common scam tactic.

Taking everything into account, I don't think it would be fair to hold M jointly responsible for the loss.

Mr M has described the way the scam affected his wellbeing and his confidence in making financial decisions. I was sorry to learn of this. I have sympathy for Mr M, and don't doubt the personal impact the situation has had on him. But the complainant here is M, a limited company, which can't itself feel stress. So while I can understand how distressing the situation is bound to have been for Mr M personally, I'm unable to take this into account when considering redress.

Putting things right

To put things right, I require Zempler Bank Limited to:

- Refund £17,110 to M; and
- Add simple interest at 8% per year to the refund from 23 March 2025 until the date of the refund.

My final decision

My decision is that I uphold this complaint. I require Zempler Bank Limited to put things right by doing as I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask M to accept or reject my decision before 25 March 2026.
Juliet Collins
Ombudsman