DRN-6124260

The complaint

C, a limited company, complains that Zempler Bank Limited ('Zempler') won't refund all the money it lost to an 'impersonation' scam.

The complaint has been brought by C's director ('Mr H') and referred to us through a firm of solicitors. For simplicity, I'll generally refer to C and Mr H throughout this decision.

What happened

The background is known to both parties, so I won't repeat every detail. In summary, on 1 January 2024, Mr H was cooking for his family while also caring for his father and feeling the absence of his mother, who has dementia. In the middle of this, he received a call from someone claiming to be from Zempler's fraud team. He later discovered the caller was a scammer.

The scammer told Mr H there had been fraudulent activity on C's account and referred to a card payment Mr H could see had been attempted and didn't recognise. Mr H says the caller was very convincing, appearing to know sensitive information such as the last four digits of the account number, which made the call seem genuine. In the call, the scammer instructed Mr H to log out of his mobile device, claiming it contained viruses that needed to be cleared. Mr H then logged into online banking through his desktop and downloaded remote-access software, as instructed. He understood that the caller was helping him secure C's account and recalls being told that his screen would go black in the process.

The call lasted about an hour. At one stage, the scammer asked Mr H to read out a code, saying it was needed to recover a fraudulent transaction and prevent further payments. Mr H says that when the call ended, he logged back into C's account and saw that payments had been made without his knowledge. He thinks the code he provided allowed the scammer to make the payments. The disputed payments are listed below. Mr H has also said fraudulent payments, made from his accounts with two other banks, were fully refunded.

Date	Time	Method	Payee	Amount
01-Jan-2024	16:56	Card payment	3Kicks.com	£6,220.26*
01-Jan-2024	17:26	Transfer	Britcare	£24,000

* *Linked to the card payment, a £185.98 fee was also taken on 3 January 2024*.

Mr H called Zempler on 1 January 2024 to report the scam but was asked to call back the next day to speak to its fraud team. In February 2024, Zempler told Mr H it wouldn't refund any of the payments on the basis that the transactions were completed after he'd provided the scammer with remote access; he hadn't taken any steps to confirm the identity of the caller; the area code of the incoming call should have served as a warning about the caller. It noted two further payments were later flagged by its systems and declined.

The complaint was referred to our Service. Our Investigator upheld it. They concluded the scammer had likely obtained C's card details and initiated the card payment. However, they

didn't think this payment should be refunded because Mr H had approved it in-app. It was reasonable for Zempler to rely on that representation and treat that payment as authorised. For the transfer, the Investigator said the scammer had likely completed the transaction using remote access after Mr H provided a code sent to his app to approve the login. As Mr H neither knew about nor consented to the transfer, and hadn't failed with intent or acted with gross negligence, they concluded that this payment should be refunded, with interest.

Mr H accepted that outcome. Zempler didn't and instead offered to pay 50% of the £24,000 transfer saying that Mr H should have done more and had the opportunity to contact Zempler directly to verify that the call was genuine before engaging with the caller. This was rejected by Mr H. As the matter couldn't be resolved informally it's been passed to me to decide.

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 conclusions as the Investigator.

Under the relevant law, the Payment Services Regulations 2017 (PSRs), the starting point is that C is liable for authorised payments and, subject to some exceptions, Zempler is liable for unauthorised payments.

Where a payment is 'authorised', that will often be because the customer has made the payment themselves. However, there are other circumstances where a payment can be considered authorised, such as where the customer has given permission for someone else to make a payment on their behalf or they've told their payment services provider they want a payment to go ahead. Here it's not in dispute C was the victim of a scam, and it doesn't seem to be in dispute Mr H took certain steps which led to payments from C's account.

The first was a card payment. As the Investigator noted, Zempler's terms explain at section 8.9 that enhanced security measures may be required – for example, entering a passcode sent by email or text, or authenticating a payment in the mobile app. Zempler's technical evidence shows that this card payment was approved in-app through the stronger customer authentication method (known as 3DS). I'm satisfied this approval was made on Mr H's registered device, which was the only device accessing the app at the time. Given that the terms make clear that completing in-app authentication is one of the ways to make a card payment, I think it's arguable this payment should be treated as authorised for this reason.

I'm also satisfied that, when approving the card payment, Mr H would have been taken through a series of in-app screens. These began with the message, *"Please confirm you'd like to make this purchase".* The app then displayed payment details, including merchant and amount, and presented clear options either to decline or approve the payment. I'm satisfied Zempler clearly asked Mr H whether he wanted to approve that payment. And given the clarity of the screens, I think it's reasonable for Zempler to rely on the steps Mr H took as a representation of him confirming he gave consent, so as to treat that payment as authorised.

I've considered if there are other reasons why the card payment (and linked fee) should be refunded. But I don't think that payment ought to have appeared as particularly suspicious when compared to C's usual account activity, such that it was a failure on Zempler's part not to have intervened. And I'm satisfied it's unlikely a chargeback would have succeeded, as the merchant likely provided the goods as intended (albeit for the benefit of the scammer).

As I've found that Zempler can fairly treat the card payment as authorised, that Zempler wasn't at fault for processing it without carrying out additional checks, and that it's unlikely a

chargeback would have succeeded, I don't think Zempler needs to refund this or the fee.

For the transfer, Zempler's terms say that Mr H can authorise payments (on behalf of C) through online banking or the mobile app. Zempler has also explained that if the transfer was made using online banking on a desktop, a verification code—sent to the mobile app—would have been needed to approve that log in. This is supported by Zempler's audit logs, which show a mobile login at 17:19, followed by a desktop login at 17:20.

Mr H has explained that the scammer instructed him to log in on his desktop after convincing him that his mobile had a "virus" that had to be cleared as fraudsters were taking money out through that device. He says he entered his login details himself, didn't share his password or security answers, and that his screen went black once the scammer had remote access.

On balance, I'm persuaded the scammer made the transfer using remote access *after* Mr H had already logged into online banking. Mr H has said he shared codes during the call. But once he had logged in, he wouldn't have needed to share the verification code Zempler says would have been sent to his app. And as I've seen nothing to suggest Zempler issued any further codes required to complete the transfer, I think the codes Mr H remembers sharing likely related to other parts of the scam – for example, granting remote access or linked to scam payments made from his other bank accounts, all of which took place in the same call.

Mr H has consistently explained he allowed remote access because he genuinely believed the caller was from Zempler's fraud team, helping him secure C's account. He followed their instructions because he thought they were stopping fraudulent payments scheduled to leave the account. I'm persuaded by Mr H's testimony that he didn't knowingly grant remote access in a way that would allow further payments. And Zempler appears to accept this too. When asked to explain why it had offered to refund 50% of the transfer – if, for example, it accepted it was unauthorised but believed Mr H could have done more – it replied: *"yes, we believe the customer could have done more"* and referred to the steps it thinks Mr H could have taken to verify the caller. Taking everything into account, I'm satisfied the transfer was likely made by the scammer without Mr H's consent and was unauthorised.

Zempler can refuse to decline a refund of an unauthorised payment where, for example, Mr H (acting for C) failed with intent or gross negligence to take all reasonable steps to keep safe C's personalised security credentials. I'm not persuaded that's the case here.

Zempler has argued that several factors should have raised concerns for Mr H – for example, that the incoming call's area code didn't match Zempler's contact details, that he could have contacted Zempler directly to verify the caller's identity, and that his request to speak to a manager showed he had doubts. Zempler appears to rely on these points to suggest negligence and to justify splitting liability for the transfer. It's unclear whether Zempler is applying a contributory negligence approach (relevant to authorised scams).

However, as I've found that the transfer was unauthorised, the test under the PSRs is whether Mr H's actions amounted to *gross* negligence. That's a significantly higher bar than negligence. I'm considering whether Mr H acted with a lack of care that goes significantly beyond what we would expect from a reasonable person. There's no concept of shared liability.

The scam began when Mr H received a call from someone claiming to be from Zempler. The scammer already had C's card details. There's no suggestion Mr H shared this information himself – fraudsters can obtain such details in many different ways. Using those card details, the scammer initiated the card payment and used it to convince Mr H that C's account was at risk. This was a deliberate social-engineering tactic designed to create panic and urgency.

Mr H has explained that when the call came in, he was panicked, stressed, distracted, and already vulnerable to the scammer's approach. In his mind, he took some precautions, such as checking Zempler's opening hours. He was reassured when a so-called "manager" called back and sounded professional. The caller knew the last digits of C's account number, which Mr H believed only Zempler would know – and Mr H has also said he trusted the caller because they appeared to be warning him about fraudulent activity.

In this context, I think it's understandable that Mr H believed he was speaking to Zempler. I'm not persuaded he ignored clear or obvious concerns that the caller was a scammer before granting remote access, thinking that the caller was helping to protect C's account. And even if he might have taken more steps – such as checking Zempler's contact details or calling it directly – I don't think his actions, especially in the heat of the moment, fell so far below the standard expected of a reasonable person that they amount to gross negligence.

In my view, Mr H's behaviour was consistent with someone trying to protect the account, not someone disregarding obvious risks. I think many people faced with similar pressure would have acted in a similar way. So while there were extra steps he might have taken, I'm not persuaded his actions show he failed with intent or a level of carelessness that amounts to gross negligence. Under the PSRs, C isn't liable for the unauthorised transfer, and Zempler should refund it in full with interest.

Putting things right

To put things right, I direct Zempler Bank Limited to refund C the amount of the unauthorised £24,000 transfer, together with simple interest at 8% per year from the date of payment to the date of settlement.

Interest is intended to compensate C for the period it was unable to use this money. If HM Revenue & Customs requires Zempler Bank Limited to deduct tax from the interest, it should provide C with a certificate showing tax deducted if it asks for one.

My final decision

For the reasons given, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask C to accept or reject my decision before 24 March 2026.

Thomas Cardia
Ombudsman