DRN-5598937

The complaint

M Ltd complains that Zempler Bank Limited ("Zempler") won't reimburse money it lost as a result of a scam.

What happened

As it was one of M Ltd's directors – Mr C – that interacted with the fraudsters, for ease I've generally referred to him throughout this decision.

On 6 November 2024, Mr C received a call from someone claiming to represent Zempler. He says that he was cautious about the approach as the call came from a number he didn't recognise. He asked the caller to call back from a number associated with Zempler, which they did. The number they called back on matched a number he found online for Zempler.

Mr C says that the caller knew the name of his business, his address and the last four digits of his card. He was told that there had been attempts to use his card in a different part of the country (one that he says he'd recently visited) and that his account was now at risk. In order to protect it, the caller claimed he'd need to move money to a new account.

Mr C recalls that the caller had a good working knowledge of the Zempler application and explained what would happen at each stage.

Under the fraudster's instructions Mr C made a single payment from the account of M Ltd of £23,500 to the account of a third party.

According to Zempler, Mr C moved past a number of relevant warnings and misled it about the purpose of the payment. It also said that he disregarded a negative 'Confirmation of Payee' ("CoP") match result – which informed Mr C that the payee name he'd entered (that of M Ltd) didn't match the name on the beneficiary account.

When the caller suggested that Mr C make additional payments up to the daily £25,000 limit on his account and he received codes that related to card payments to recipients he had no connection with, he says that he started to become concerned. He contacted his wife who suggested that he might be falling victim to a scam.

Mr C ended the call and reported the scam to Zempler. He asked it to consider reimbursing him. Zempler declined. It said that it had considered the claim under the relevant reimbursement rules but had decided that M Ltd didn't have a reimbursable claim as it had warned Mr C about the scam he fell victim to. It also said that it had contacted the beneficiary bank to ask for the return of M Ltd's money but had not received a response.

Zempler has also said that there were a number of high value card payments attempted following the successful £23,500 payment but it has not provided evidence of these payments and none of them debited Mr C's account.

Mr C made a complaint about Zempler and ultimately referred that complaint to our service.

One of our Investigators looked at the complaint and noted that the FPS Reimbursement Rules ("the Reimbursement Rules") applied to the payment Mr C made. Under the Reimbursement Rules a firm must reimburse victims of APP scams unless it can demonstrate that an exception to reimbursement applies. Zempler argued that it could rely on the Consumer Standard of Caution Exception ("the Exception") because Mr C had failed to have regard to its interventions with gross negligence.

The Investigator considered Mr C's overall conduct and concluded that it didn't amount to gross negligence or engage the Exception. They therefore recommended that Zempler reimburse the payment he made, minus the excess allowable under the Reimbursement Rules.

Mr C accepted our investigator's recommendation, but Zempler did not. In summary it argued:

- It's evident that Mr C had suspicions about the call as he was concerned that the number he initially received a call from was not associated with Zempler. Mr C should have realised that the second call was from a 'spoofed' number and he should have called them using the number on the back of his card, as advised in the warnings it gave.
- Whilst it acknowledges that some of the warnings Mr C saw are shown to every customer, it didn't matter what the warning said, because Mr C ignored all of them, including the CoP mismatch, which should have alerted him to the fact the account he was paying was not held in the name of M Ltd.
- Its warnings used the same language as the fraudsters – referring to a 'safe account', so they ought to have resonated with Mr C.
- In the months before the scam, it sent him correspondence which explained number spoofing and how it works.
- Mr C is an IT business consultant and ought to be aware of fraud.

As no agreement could be reached, the case was 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.

In 2022, against a backdrop of increasing APP fraud and the devastating consequences it can have (victims in the UK lost half a billion pounds in 2023), the Treasury announced its intention to introduce legislation for the Payment Systems Regulator to require payment service providers to reimburse victims of authorised push payment ("APP") scams.

Section 72 of the Financial Services and Markets Act 2023 required the PSR to introduce a reimbursement requirement for payments made over the Faster Payments Scheme as a result of fraud or dishonesty. And during 2024 the PSR duly required the Faster Payments scheme operator (PayUK) to change the Faster Payment Rules to require the firms that operate over Faster Payments in certain circumstances to reimburse their customers sums paid as a result of APP scams.

The Reimbursement Rules came into force on 7 October 2024 and apply to all UK-based Payment Service Providers (PSPs). They put a requirement on firms to reimburse APP scam payments made via the Faster Payments Scheme (a similar set of rules covers CHAPS payments), in all but very limited circumstances.

My role is to determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case. In doing so I must take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time.

In this case I've first considered whether the Reimbursement Rules and associated guidance issued by the PSR are relevant to the payments in dispute. Where they are relevant, I must have regard to the rules and guidance, as well as considering what is fair and reasonable in all the circumstances of the complaint.

The Reimbursement Rules[1] set out the requirements for a payment to be covered. I've summarised those below:

- The payment must have taken place after 7 October 2024 and have been reported within 13 months after the date of the final covered payment of the scam claim; and
- It must have been made as part of an APP scam (whether to a recipient or for a purpose otherwise than the payer intended); and
- It must have been authorised by the account holder; and
- It must have been made to another UK account that was not under the control of the consumer[2].

There's no dispute that the above criteria apply to the Faster Payment made by Mr C.

In order for a payment to be 'reimbursable' under the Reimbursement Rules it must meet the following criteria, which again have been summarised:

- The Exception does not apply or the consumer was a vulnerable consumer at the time the payment was made.
- The consumer is not party to the fraud, and is not claiming dishonestly or fraudulently.
- The payments were made in relation to a fraud, rather than in circumstances only giving rise to a private civil dispute.
- The purpose of the payment was not unlawful.

And a PSP will be responsible for reimbursing a maximum of £85,000 from any single APP scam claim.

Again, it's my understanding there's no dispute about any of the criteria above applying, other than whether the Exception applies. And as the complainant is a limited company, rather than a natural person, it cannot be considered a 'vulnerable consumer'.

The Consumer Standard of Caution Exception

---

[1] https://www.wearepay.uk/wp-content/uploads/2024/09/FPS-Reimbursement-Rules-Schedule-4-v3.0.pdf at paragraphs 3.8-3.10

[2] Under the Reimbursement Rules the definition of a "Consumer" is defined as follows: *"Refers to Service users of PSPs. These are individuals, microenterprises (enterprises that employs fewer than ten persons and have either an annual turnover or annual balance sheet total that does not exceed €2 million), or charities (a body whose annual income is less than £1 million per year and is a charity as defined by the Charities Act 2011, Charities and Trustees Investment (Scotland) Act 2005 or the Charities Act (Northern Ireland) 2008)."*

In order to rely on the Exception, a sending PSP must show that, as a result of *gross negligence*, a consumer has not complied with one or more of the following standards:

- The consumer should have regard to any intervention made by their PSP and/or by a competent national authority (which includes, but is not limited to, any police force or service in the U.K.)

- The consumer should, upon learning or suspecting that they have fallen victim to an APP scam, report the scam claim promptly to their PSP.

- The consumer should respond to any reasonable and proportionate requests for information made by their PSP for a limited number of purposes (principally to validate the scam claim and whether it is reimbursable).

- The consumer should, after making a scam claim, consent to the PSP reporting to the police on the consumer's behalf or request they directly report the details of a scam to a competent national authority.

Zempler has sought to rely on the first standard set out above - ("the Intervention Standard") and I can't see that any other standard would apply here.

The Intervention Standard

The Payment Systems Regulator's Consumer Standard of Caution Exception Guidance ("the Guidance")[3] provides guidance to supplement the Reimbursement Rules. It gives a more detailed and specific description of the Intervention Standard:

"Consumers should have regard to specific, directed interventions made either by their sending PSP, or by a competent national authority. That intervention must offer a clear assessment of the probability that an intended payment is an APP scam payment."

That description is expanded on in paragraphs 1.8 – 1.10 of the Guidance:

"PSPs can expect their consumers to have regard to specific, directed interventions raised either by their sending PSP, or by a competent national authority. Those interventions must clearly convey the PSP's, or competent national authority's, assessment of the probability that an intended payment is an APP scam payment. Only in circumstances where the PSP can demonstrate that a consumer who has not been classed as vulnerable has, as a result of gross negligence, not had regard to such interventions can a reimbursement claim be refused.

It will be up to payment firms to consider the approach they might take in creating tailored, specific interventions and to develop their own operational approaches and identify best practice.

Any intervention for the purpose of this exception should be bespoke. They must be consumer, scam, and transaction specific. They should not consist of 'boilerplate' written warnings. Providers should not refuse reimbursement claims on the basis that a consumer received vague, non-specific written warnings, or warnings that routinely accompany most or all transactions of a similar type. Where a PSP does choose to intervene with a written

[3] https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf

warning, this must be actively brought to the attention of the consumer. PSPs should not rely upon the availability of passive warnings, such as on public websites."[4]

The guidance further explains that a consumer who chooses to proceed with a transaction after an intervention by their PSP should not automatically be deemed to have been grossly negligent. Instead, any assessment of the degree of negligence should include consideration of all relevant factors, including:

- "the specificity and nature of the intervention made by their sending PSP
- the degree of certainty any intervention, whether written or otherwise, conveys that a prospective transaction is an APP scam
- the complexity of the scam to which the consumer has become victim, including whether the victim has been subject to any degree of social engineering, or was otherwise in thrall of a scammer
- any claims history from the consumer suggesting a propensity to fall repeatedly for similar types of scams"[5]

Based on the PSR's guidance, it seems to me that the PSR envisages that the assessment of whether the Intervention Standard is met, is normally a two-stage test: whether the intervention met the criteria set out in the Guidance and whether the consumer was grossly negligent in moving past it.

In this case, as set out in more detail below, Mr C provided a payment purpose to Zempler that wasn't accurate. I also think on balance he's likely to have indicated to Zempler that he wasn't on the phone to anyone asking him to make a payment, which wasn't the case. He did also receive some directly relevant warnings but I understand these were not bespoke and accompany most or all transactions of a similar type.

Following the Guidance closely in this case *might* result in a finding that Zempler had not provided sufficiently bespoke and specific interventions to Mr C and therefore that its arguments have to fall at the first stage. However, Mr C's actions, to an extent, hindered Zempler from giving the kind of intervention envisaged by, and detailed in, the Guidance. The PSR have clarified the application of the Guidance to circumstances such as this. The clarification said:

"In assessing whether the interventions were bespoke and specific, consideration should be given to the nature of the information given by the consumer to their PSP including its accuracy, as part of their overall assessment of whether the CSOC exception applies. The fact that the consumer failed to give accurate responses at the time of the payment should not, of itself, automatically mean that the consumer has not acted with caution or that they have been grossly negligent. This will be one of various considerations which will need to be weighed up in determining whether a PSP should reimburse their customer."

Taking the PSR's clarification into account, instead of applying a two-stage test as to whether the Intervention Standard is met, I should consider the overall question of whether Mr C failed with gross negligence to have regard to Zempler's interventions. In doing so I should take into account a number of factors, including the fact that Mr C didn't give accurate responses during some of those interventions.

---

[4] https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf at paragraphs 1.8 to 1.10

[5] https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf at paragraph 1.13

How did Zempler intervene during the scam?

I've outlined the interventions and warnings that Zempler provided to Mr C in relation to the payment he made.

I consider an intervention to be any steps Zempler took to interact with its customer that otherwise interrupted the expected payment journey.

Intervention 1

Zempler advise that every time a customer clicks 'PAY' they receive a warning which says:

"We will never call and ask you to transfer your money to a safe account"

It can't demonstrate that Mr C definitely saw this message.

Intervention 2

When 'Set up a new payment' was selected, Zempler says (but cannot demonstrate) that another warning was displayed which said the following:

"Check for fraud before you add a new payee

Could someone be scamming you? Criminal [SIC] may pretend to be a person or company you trust and ask you to send money to a new account.

Is someone on the phone asking you to make this payment?"

Two options are given: yes or no. Zempler is unable to confirm which option Mr C selected.

I understand that if 'no' is selected, the following additional text is shown:

"Once you make a payment, it's not always possible to get the money back. You can read more about identifying fraud **here** [link]"

Finally Mr C would have been asked to confirm *'I understand the warning and want to set up this payee'* before clicking 'next'.

If 'yes' had been selected then Mr C would have received a message which says "Zempler will never call and ask you to transfer money to any account, this is a scam, please end the call."

Intervention 3

Mr C was then asked for the purpose of the payment. He selected "paying for a bill", instead of "transfer to my own account". Because of this Mr C received a warning that was mostly unrelated to 'safe account' scams. That warning largely focussed on the risk of unexpected bills and account details being replaced by a fraudster. It did, however, also say "Criminals can often try to impersonate organisations and individuals in order to trick you into sending over the funds".

Intervention 4

Zempler also informed Mr C that the account details he entered didn't match those of the account that he was paying. It said:

"Check the payee name

The name you gave us is not the same as the name held on the account. Double check the details with the recipient before proceeding."

And then on a separate screen:

"Review recipient details

Initiating this payment may lead to funds being sent to the wrong account and we may not be able to recover your money."

Zempler has also said that Mr C would have provided codes to the fraudster in order to allow the debit card payments to be attempted. However, these payments took place after the Faster Payment and it cannot, in any case, show what the message that accompanied the codes said.

Gross negligence under the Reimbursement Rules

It is entirely for Zempler to demonstrate that Mr C was grossly negligent[6]. The Guidance says "We interpret 'gross negligence' to be a higher standard than the standard of negligence under common law. The consumer needs to have shown a 'significant degree of carelessness."[7] No further guidance is given as to the interpretation of gross negligence.

In Red Sea Tankers Ltd v Papachristidis [1997] 2 Lloyd's Rep. 547, Mance J said of gross negligence that it "is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence. But, as a matter of ordinary language and general impression, the concept of gross negligence seems to me to be capable of embracing not only conduct undertaken with actual appreciation of the risks involved, but also serious disregard of or an indifference to an obvious risk."

The Guidance doesn't provide a significant expansion on the PSR's brief definition of gross negligence, but does provide some direction on the practical application of the test in relation to the Exception, particularly at paragraph 1.13, which I've repeated (in part) below.

"…any assessment of the degree of negligence should include consideration of all relevant factors, including:

"…the complexity of the scam to which the consumer has become victim, including whether the victim has been subject to any degree of social engineering, or was otherwise in thrall of a scammer"

A consideration of "the complexity of the scam" suggests that I should be considering, objectively, whether the scam had complex features (which, given the context, I've taken to mean an assessment of whether these were so sophisticated that a reasonable person in the consumer's position would have found it plausible or compelling, rather than the scam simply being complicated). Whereas a consideration of whether the consumer was subject to any degree of social engineering, or was otherwise in thrall of a scammer seems to me to introduce a more subjective element – whether the consumer was psychologically manipulated into acting in the way the fraudster desired.

The Guidance does not provide any further explanation on this point. But it seems unlikely that a purely subjective assessment of gross negligence was intended – that would render the test little more than whether the fraudster was able to manipulate the victim into misunderstanding who was the beneficiary of the payment, or its true purpose. And that is almost always going to be the case, or the payment would never have been made and the fraud would not have succeeded; so there could almost never be a finding of gross negligence. It would also mean that there would be little purpose in considering the complexity of the scam, because what would matter would be whether it succeeded in misleading the victim rather than how that was achieved.

---

[6] https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf paragraph 1.6

[7] https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf paragraph 1.7

On the other hand, it's also hard to conclude that a purely objective test is intended – that would render a consideration of whether and to what extent the customer was, as a matter of fact, under the thrall of the scammer irrelevant; whereas that is a matter to which the Guidance refers as amongst the relevant considerations.

Standing back, therefore, I think the Guidance is asking me to consider the complexity of the scam, while also recognising in that context the role that social engineering can have in a victim's decision making, particularly in persuading the victim to move past interventions that might, without such manipulation, have been expected to deter them from making the payment.

Did Mr C fail to have regard to Zempler's interventions with gross negligence?

It's important to point out that this is a scam in which Mr C had nothing to gain but, on the face of it, a significant amount to lose. This kind of scam works by preying on the fear of a victim. It presents a choice: dismiss the call and run the risk of losing money to fraud or engage and attempt to avoid that loss. In other words: the scam relies heavily on social engineering for its success.

The effect of that social engineering was to put Mr C immediately on the back foot. He was told he'd need to act now to avoid loss and doesn't appear to have been given time to take a step back and consider what he was being asked to do. Those circumstances should be kept in mind when considering why Mr C moved past the interventions.

I've first thought about why Mr C didn't dismiss the call and whether a reasonable person in his circumstances would, or should, have simply not accepted that the call was genuine. That's relevant because, if it wasn't reasonable for Mr C to have believed the call to be genuine at all, then the risk of following the fraudster's instructions to move past Zempler's interventions ought to have been clearer to him.

Mr C says that the caller knew information about him – the name of his business, his address and the last four digits of his Zempler debit card. I have no reason to doubt what Mr C has told us about this and Zempler appears to accept that some information might have been known to the fraudster in advance of the call. While none of this information would prove that the caller was from Zempler (and, of course, the name of his business and his address are likely to be in the public domain), the knowledge that the caller had would have reasonably given Mr C the impression that the call was, at least, specifically targeted at him.

Mr C says that there was added credibility to the claim that the fraudster made – that payments were being attempted by a fraudster using his Zempler account in a specific part of the country that he'd recently visited. I can only imagine that this claim was a coincidence, but it nevertheless appears to have added weight to the caller's claim that his account was at risk and that they had information that it would be unlikely for a third party to be aware of.

Mr C says he was concerned that he'd been called on a withheld number. Zempler suggests this points to Mr C having a concern that the call was not genuine and he failed to then take adequate steps to verify that, and ought to have known that the subsequent call he received was from a 'spoofed number'.

I don't think that's fair. Mr C took what appeared to be sensible steps to verify the caller – by asking them to call back on a number associated with Zempler. I don't think a reasonable person in his circumstances (and his professional experience) would necessarily know either about the existence of 'number spoofing' or, that in order to combat the fraud, they'd need to contact Zempler directly. I also don't think it's reasonable, as Zempler argues, to say that Mr

C ought to have been aware of number spoofing because it had sent him emails about this months, or even years, before the scam took place. Of more relevance here is the fact that the interventions that Zempler did provide did not alert him to the risk of number spoofing – a key factor in Mr C deciding that the call was genuine. While Mr C's own responses to Zempler's questions may have prevented such a warning being provided, it nevertheless meant that there was nothing within the intervention that alerted him to this possibility.

So, Mr C had been called by someone who made a credible claim about the misuse of his account, knew personal information about him and his company and appeared to be able to call him from a number associated with Zempler. I don't think it's unreasonable, as Mr C says was the case, that he'd accepted he was speaking to the genuine Zempler at this point. I think many other people would have believed the same in his position. That means I think the scam had a fairly high degree of complexity – by design and also, probably, by accident.

So, prior to Mr C being presented with the interventions by Zempler I think he had a fairly strong and reasonably held belief that the call was genuine. Therefore, when presented with the interventions, I can understand why he attached less significance to them, given that he believed that the entity providing the warnings and the person he was speaking to were essentially the same.

I've gone onto consider, taking into account the above, whether the interventions that Mr C moved past should have made the risk that he was not dealing with Zempler so clear and obvious that he should be considered to have acted with gross negligence in moving past those interventions.

First there is a factual issue to be resolved of what Mr C saw and how he answered the question that was presented to him in relation to Intervention 2. Zempler can't evidence that Mr C actually saw Intervention 1 or 2, but I understand these warnings always appear when a payment is being created – they weren't specific to Mr C's payment. For that reason, I think it's more likely than not that Mr C did see these warnings. It's also reasonable to assume that he chose the option "no" when asked the question "Is someone on the phone asking you to make this payment?". I say this because he acknowledges that he was being guided by the fraudster (as he was when he selected an inaccurate payment reason) and it would not be in the interest of the fraudster for him to have told Zempler he was on the phone and being asked to move money.

Having established what Mr C likely did and didn't see, I've thought about the nature of Zempler's interventions and why Mr C moved past them. Mr C's recollections of these interventions are very limited. He doesn't recall any of the specifics and says that he was guided through the interventions by the fraudsters, reassured that everything would be OK and that he needed to move the money quickly.

I acknowledge that Intervention 1 was specific to this type of scam and was quite clear, if rather brief: "We will never call and ask you to transfer your money to a safe account". The question in relation to Intervention 2: "Is someone on the phone asking you to make this payment?", is perhaps slightly less directly relevant, given that it doesn't make it clear that 'someone' could include Zempler itself. Nevertheless, the two interventions were directly relevant to Mr C's circumstances. That said, neither warning requires significant interaction – simply clicking 'close' on Intervention 1 and answering one question in relation to Intervention 2 allows the user to move past the warnings. I can see how that would make it easier for a fraudster to persuade the user to move past the warnings – particularly in circumstances where time appears to be of the essence and the user is being guided by an apparently knowledgeable member of staff.

In relation to Intervention 3, I've not been provided with evidence of the screen that showed the payment options, so I'm not sure how this was positioned. However, the evidence suggests that one question was asked about the purpose of the payment and again, that would make it relatively straightforward to move past the warning in the circumstances I've described.

The limited nature of these interventions is likely due to the fact they were not prompted by any concerns about the particular payment, instead they appear to be simply part of the payment process. I think that's relevant here – I think the risk of proceeding ought to have been more apparent where it was clear that the PSP has specific concerns about the payment that is being made and had taken steps to interrupt the payment journey to warn its customer. That wasn't what was happening here and again, I suspect it made it easier for the fraudsters to persuade Mr C that the interventions were simply standard procedure that could be moved past. That said, I do acknowledge that had Mr C answered the question in relation to Intervention 2 positively, he would have received a warning that conveyed a very high degree of certainty that the transaction he was attempting was part of an APP scam. Intervention 4 (the CoP warning) highlighted that the account name Mr C entered did not match the recipient account. On the face of it, that would be an unexpected result. Mr C can't recall this warning or why he moved past it. I do not intend to put words in Mr C's mouth or draw inferences from the experiences of other scam victims. But fraudsters are clearly aware of the CoP system and have devised numerous explanations to give to victims to explain why a negative CoP match would be returned. So while it's possible that Mr C simply didn't question the result in light of the faith he clearly had in the fraudsters, it's also possible that a plausible explanation was given that Mr C simply cannot recall.

Overall, I acknowledge that Mr C moved past a number of interventions and likely misled Zempler in relation to two of those, but it's important to recognise that Mr C was on the phone to the fraudsters throughout and did not have the benefit of taking a step back and considering those interventions, and the wider circumstances, without being subject to a competing narrative: that any failure to comply would result in him losing his money. That competing narrative also had an advantage over Zempler's interventions – it was verbal and was able to react dynamically to both Zempler's interventions and any concerns or misgivings Mr C might have had. Mr C says that the fraudsters knew the application and the warnings very well and were able to pre-empt each screen and intervention before it appeared – reassuring him as they did so. And, as I've set out, the interventions appeared to be part of the payment process, rather than being the result of any specific concerns Zempler had about the payments, which likely aided the fraudster's narrative. In those circumstances and taking into account the limited nature of the interventions, his actions in both giving misleading responses and moving past the interventions become, in my view, more reasonable.

Considering the circumstances overall, I acknowledge there were reasons for Mr C, at least in hindsight, to be concerned about what he was being asked to do. It perhaps should have appeared odd to him that Zempler would be asking him to move his own money and that its staff should ask him to move past its warnings.

But it's important to note that Mr C did not abandon all scepticism – he became concerned when the fraudsters began trying to process more payments and he sought the advice of his wife, who suspected he had been the victim of a scam. Those card payments, he says, were clearly not going to an account in his or M Ltd's name. In other words: Mr C was alive to the fact that those payments weren't consistent with the narrative he'd been given. I think this is further evidence that Mr C was not behaving carelessly but put misplaced trust in whom he genuinely believed to be Zempler staff (up to the point where that belief was reasonably shaken).

As I've set out, there was a significant amount of social engineering here. I think that social engineering, rather than, for example, expediency or disinterest explains why Mr C moved past relevant warnings. It's clear Mr C thought that he was dealing with Zempler and acting to avoid serious financial harm.

As I've set out, this was also a scam with complex features – including number spoofing (a feature that none of the interventions mentioned) and, on the face of it, the fraudsters holding some knowledge of Mr C and his account. And, although there were aspects of the scam which were less plausible, gross negligence requires a significant degree of carelessness. It's not enough for Zempler to show that a reasonable person in Mr C's shoes might have acted differently. It needs to demonstrate that his actions fell so far below that of a reasonable person that he was grossly negligent. I don't think it has done that.

Overall, I'm not persuaded that Mr C acted with gross negligence in moving past Zempler's interventions and I think M Ltd should be reimbursed in full (subject to the excess) under the Reimbursement Rules.

The excess

The Reimbursement Rules allow a firm to deduct an excess to each APP scam claim[8], unless a customer was vulnerable to a particular APP scam[9]. The maximum excess that can be applied is currently £100[10].

Zempler can deduct up to £100 from the amount reimbursed, should it decide to do so. It has not indicated in response to our Investigator's view whether it intends to apply an excess but its website, at time of writing, says that it will apply an excess of up to £100[11].

Finally, I'm satisfied with the steps that Zempler took to recover M Ltd's money – it reached out very quickly to the bank which holds the payee's account but did not receive a response.

My final decision

I uphold this complaint and instruct Zempler Bank Limited to pay M Ltd:

- the amount lost to the scam - £23,500, minus the excess of a maximum of £100
- 8% simple interest per year on that amount from the date Zempler declined his claim under the Reimbursement Rules to the date of settlement, less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask M Ltd to accept or reject my decision before 13 March 2026.

Rich Drury
Ombudsman

---

[8] https://www.wearepay.uk/wp-content/uploads/2024/09/FPS-Reimbursement-Rules-Schedule-4-v3.0.pdf paragraph 4.15(i)
[9] https://www.wearepay.uk/wp-content/uploads/2024/09/FPS-Reimbursement-Rules-Schedule-4-v3.0.pdf paragraph 4.15(iii)
[10] https://www.psr.org.uk/media/maslkvyo/sr1-excess-value-supplementary-dec-2023.pdf
[11] https://www.zemplerbank.com/help/security-and-fraud/fraud-and-scams/app-fraud/