

The complaint

Mrs M complains that Modulr FS Limited (trading as HyperJar) has declined to reimburse payments made in relation to a scam.

What happened

In November 2024 Mrs M received a call from a scammer impersonating one of her banking providers. She was persuaded her money was at risk in her accounts due to a “*trojan virus*” that could be linked to a previous phishing email she’d received. Mrs M was convinced to move her money to keep it safe, and as part of this she transferred funds to her account with Modulr. A new Apple Pay token was set up and used to make payments totalling over £8,000. Mrs M was told to expect “ghost transactions” and that this was how they tracked scammers but they would be refunded, so she wasn’t initially concerned when she saw them. Mrs M became concerned the next day when the refunds were taking longer than expected and reported the matter to Modulr.

Modulr declined to reimburse Mrs M on the basis that she had been negligent in sharing one-time passcodes (OTPs) and not checking what she was told with Modulr. It paid her £100 compensation for how it initially assessed the claim.

When Mrs M referred her complaint to our service the investigator upheld it – they thought the payments were unauthorised and that Mrs M hadn’t failed in her obligations with gross negligence. They recommended Modulr reimburse the payments and pay interest to reflect the time Mrs M had been without her funds.

Mrs M accepted these findings, but Modulr didn’t – it said that it thought Mrs M’s actions amounted to her authorising the payments and that she had been grossly negligent in sharing the OTPs used to set up Apple Pay.

The investigator explained why they remained of the opinion that Modulr should reimburse the payments. As an agreement couldn’t be reached, the matter has been passed to me for consideration by an ombudsman.

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’m upholding this complaint for similar reasons to the investigator.

Under the relevant law - the Payment Services Regulations 2017 (PSRs) – the starting point is that Mrs M is liable for payments she authorised and Modulr is generally expected to reimburse unauthorised payments. So, I’ll address this point first.

Has Modulr acted fairly in treating the payments as authorised?

It’s common ground that Mrs M has been the victim of a scam here and that she didn’t make the disputed payments herself. Rather the scammer used a newly set up Apple Pay to make

the payments themselves. So, Mrs M didn't complete the procedure to consent to any of the individual disputed payments.

This would normally mean that the payments were unauthorised, but I've considered Modulr's points about whether Mrs M did anything that would make it fair for it to treat the payments as authorised – such as giving apparent authority. In doing so I've considered how the scammer was able to set up Apple Pay and what Mrs M may have agreed to.

Mrs M recalls moving money to her Modulr account due to the security risks she was told about on her other accounts and re-setting her Apple Pay on her Modulr account. While Mrs M doesn't recall specifically doing so, she appears to accept that she may have shared OTPs with the scammer. I also think it's more likely than not that Mrs M did this as there's no other explanation for how a third party could have obtained the code sent to Mrs M's phone.

Mrs M has been consistent in her explanation that she thought they were helping her re-set her existing Apple Pay and at no point did she think she was setting Apple Pay up on a new device or that someone else would be able to use it. I accept that Mrs M didn't appreciate sharing the OTP would mean that a third party could make payments on her behalf and that she didn't agree to this. So, I don't think it would be fair and reasonable to treat payments made using this token as authorised in the circumstances. I note that it was well known to payment service providers at the time that scammers would seek to manipulate customers into sharing OTPs.

Modulr has raised that Mrs M knew payments would be made. But I consider being warned by the scammer that she may see "ghost transactions" on the account that would be returned to be different to agreeing to any payments. Mrs M was told this in the context that a virus had affected the security of her accounts rather than in connection to the OTP she shared. So, I don't think this means any of the disputed payments were authorised.

Is there any other reason why it would be fair for Modulr not to provide Mrs M with a refund?

Modulr says Mrs M can be held liable on the basis that she was negligent in sharing OTPs – and that the Apple Pay OTP said it was for Apple Pay and not to share it.

The PSRs set out situations in which Modulr can hold Mrs M liable for unauthorised transactions. Of relevance here is the obligation on Mrs M to "take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service". And that Modulr can hold Mrs M liable for the payments if they were made as a result of her failing in this obligation with gross negligence. This is reflected in the applicable terms and conditions of Mrs M's account.

When considering if Mrs M has failed in her obligations with gross negligence, the test isn't simply whether she was careless. For someone to fail with gross negligence they would need to have seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person.

Mrs M thought the caller was genuine because she had received a phishing email a couple of weeks earlier impersonating a delivery company, and the caller asked her about that. She was then persuaded this had created a security risk and they told her about a "trojan virus" putting her accounts at risk. Unfortunately, scammers can be very sophisticated and use this kind of methodology to socially engineer their victims – so it is in this context that I must consider Mrs M's actions. Mrs M was also on the phone for over two hours during which time it's likely she was convinced the caller was genuine.

I've thought carefully about Modulr's point that it ought to have appeared odd to Mrs M that

one banking provider was helping her with another account. And that the message containing the OTP to set up Apple Pay said that it was for Apple Pay and not to share it. I note though that the message didn't say that it was being set up on a new device or name the device it was being set up on. Mrs M has explained she thought she was re-setting her existing Apple Pay. While there are elements of this scam that are less plausible, and so Mrs M may have been careless in her actions, I don't think they amount to gross negligence.

I appreciate that when Mrs M saw payments leaving her account she could have contacted Modulr, but she wasn't suspicious of this because the scammer had told her she might see this, it was how they tracked fraud, and the payments would be refunded.

For these reasons, I think Modulr should reimburse the unauthorised transactions and pay Mrs M interest for the time she has been without her funds.

I note Modulr has paid Mrs M £100 compensation for how it initially handled her claim and, in the circumstances, don't think a further payment is required. A certain amount of distress and inconvenience is inevitable when a scam occurs but Modulr is not responsible for this.

My final decision

My final decision is that Modulr FS Limited should reimburse the disputed payments and pay Mrs M simple interest at a rate of 8% on this award from the date of the payments to the date of settlement.

If Modulr FS Limited considers that it's required by HM Revenue & Customs to deduct income tax from this interest, it should tell Mrs M how much it's taken off. It should also give Mrs M a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 16 February 2026.

Stephanie Mitchell
Ombudsman