DRN-5967417

The complaint

Mrs B complains that Paynetics UK Limited ("Paynetics") won't refund payments made as part of a scam.

The payments were made from Mrs B's account with Trading 212. Paynetics provides the debit card offered with this account, and it was a tokenised version of the card that was used to make the disputed payments. So, Paynetics is the respondent business here. But for simplicity, I'll refer to Trading 212 in my decision.

What happened

The full details of this complaint are well known to the parties, but briefly:

- In July 2024, Mrs B received a call purportedly from the fraud department of her bank, "H", and the caller mentioned suspicious activity. Under the guise of protecting Mrs B from fraud, the caller persuaded her to move funds into a safe account. Mrs B says she the caller told her Trading 212 was a subsidiary of H and they helped her create an account with it. She followed the caller's instructions and moved £9,500 to the newly created account. Subsequently, the funds were moved out of the Trading 212 account through tokenised card transactions. Mrs B says she only realised something had gone wrong when H contacted her about a recent loan application that she had no knowledge of.

- Trading 212 declined to refund Mrs B. It said the transactions were authorised and couldn't be disputed.

- Our Investigator explained that under the relevant legislation, a payment would be considered authorised if the customer consents to it or gives someone else permission. They concluded that the payments were unauthorised as Trading 212 hadn't provided the required technical evidence to demonstrate that they were correctly authenticated in accordance with the form and procedure agreed between the parties. Also, the Investigator wasn't persuaded that Mrs B had failed with intent or gross negligence to keep her account safe. As such, Trading 212 was liable to refund the loss suffered.

- Trading 212 disagreed with the Investigator's findings, and the complaint was passed to me to decide. I issued a provisional decision and gave reasons for why I agreed with the Investigator's overall outcome that the payments were not authorised and needed refunding along with interest.

- I gave both parties an opportunity to provide further comments or evidence for my consideration. Mrs B accepted my provisional decision. Trading212 said that the Financial Ombudsman Service's general stance is that customers must take responsibility for their actions. It questioned that given my comments in the provisional decision about Mrs B acting with a degree of negligence, shouldn't that translate into a finding that there was contributory negligence on her part.

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 line with the Payment Services Regulations 2017 ("PSRs"), the relevant legislation here, the starting position is that Trading 212 is liable for unauthorised payments, and Mrs B is liable for authorised payments. She says she didn't authorise the payments and this was done by the scammer.

It's not in dispute that Mrs B was the victim of an impersonation scam. Trading 212 has since provided technical data which shows that Mrs B's account was accessed from a new device. It accepts that it was this device that created the tokenised card used to make the disputed payments. It's also explained that to access the account from a new device, a one-time passcode (OTP) is sent to the existing device which needs to be entered on the new device. The technical data provided shows that an OTP was sent to Mrs B's registered device.

Trading 212 says it's not arguing that the transactions were authorised in the context of completing the form and procedure. Instead, Mrs B created the account and provided access to the scammer which enabled them to make the payments she's now disputing.

It's not entirely clear whether Trading 212 is arguing that it considers the payments are authorised because Mrs B gave access to a third-party, or whether it accepts that they are unauthorised but considers her actions amount to gross negligence and therefore it isn't liable. So, I've considered both arguments.

Our Investigator asked Mrs B about the OTP, and she said she had no recollection of receiving or sharing a code with the caller. Mrs B also said that she was under so much pressure from the caller and wanted to ensure her money was in the safe account, that she did as she was asked.

I appreciate Mrs B has been unable to recall receiving or sharing the OTP. But having considered the available information, including the technical evidence, I'm satisfied that Trading 212 sent the code to her device which was used to create the account. I'm also persuaded on balance that Mrs B shared the code with the scammer, and this then allowed them to access her account on their device.

But I can't agree that Mrs B sharing this code means she authorised the payments that subsequently took place, after the new device accessed her account. The form and procedure for making the payments required someone to log into the account, create the tokenised card, use it at the merchant's checkout, as well as authenticate the payment through some form of verification such as biometric verification. The information we hold indicates that these steps were not completed on the device we know Mrs B was using at that time.

I can see that at one point Trading 212 asked the Investigator why the provision of access to the account wouldn't reasonably translate to consenting to funds being moved. For a payment to be considered as authorised, consent needs to be given in line with the PSRs. As I've set out above, I'm not persuaded that Mrs B consented to the payments being made. I don't consider Trading 212 can fairly rely on Mrs B's sharing of the log-in code as her confirmation (or even representation) that she consented to the disputed payments. Having reviewed the message contained in the OTP notification, while it explains the code is for logging in it doesn't explain that a tokenised card is being set up or the consequences of sharing it with a third party.

Considering the above, in line with the PSRs, I consider the payments were unauthorised and so the starting point is that Trading 212 is liable for them. I have then considered whether Mrs B has failed with gross negligence or intent to keep her account details safe, as it's clear she has compromised the security of her account. But I'm not persuaded she did this with intent and this hasn't been suggested.

In relation to gross negligence, Trading 212 argues that it would have been reasonable for Mrs B to have verified the caller's claim that Trading 212 was part of H. I accept that there's more Mrs B could have done to verify the caller's legitimacy, though I note that she did attempt to verify that the call came from a genuine number used by H. But when establishing whether Mrs B failed with gross negligence, the test isn't whether she acted unreasonably. It's whether she acted with very significant carelessness; seriously disregarded an obvious risk; or acted so far below what a reasonable person would have done. I can't agree that Mrs B's failure to cross-check that Trading 212 was somehow linked to H alone means that she was grossly negligent.

Considering the situation Mrs B has described being in and the pressure she was under, I think she was persuaded she was talking to her bank, and it was acting to help her secure her funds. So, in the moment, she wouldn't have felt she needed to contact Trading 212 and cross-check the information – and the pressured situation wouldn't lend itself to doing so.

The scammer knew information about Mrs B's account with H, and that persuaded her they were genuine. And the actions they instructed her to take did result in her funds appearing to be secured with Trading 212. So, this built trust too. I accept that with hindsight there were some red flags Mrs B ought to have detected, such as being asked to share a code. And she did act with a degree of negligence. But this isn't the same as her being grossly negligent. So, Trading 212 is liable for the unauthorised payments and is required to refund them in full.

I've considered Trading 212's comments in response to my reference to Mrs B's negligence. It's argued that the principle of contributory negligence should apply, and liability should be shared between the parties. But when it comes to unauthorised payments, the test that the PSRs set out for circumstances in which a payment service user could be held liable is of gross negligence and not contributory negligence. I've set out why I don't consider Mrs B's actions amount to gross negligence.

Contributory negligence is not a relevant consideration for unauthorised payments. So, it doesn't apply to Ms B's complaint. It is something that I would take into account when deciding scam complaints involving authorised payments, where a payment service user is liable in the first instance, but a payment service provider has also been found to have failed in preventing or limiting the loss.

Putting things right

As I've concluded that Mrs B isn't liable for the disputed payments, to put things right for her, Paynetics UK Limited needs to refund them in full. It also needs to add simple interest at 8% per year (less any tax lawfully deductible) to the refunded amounts, to be calculated from the date of the payment to the date of settlement.

My final decision

For the reasons given, my final decision is that I uphold this complaint and Paynetics UK Limited needs to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 19 December 2025.

Gagandeep Singh
Ombudsman