DRN-6020116

The complaint

Miss T complains that Trading 212 UK Limited trading as Trading 212 is holding her liable for transactions which she says she didn't authorise.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Miss T says that her phone was stolen on her way to work on 24 February 2025 and at 22.33, her Trading 212 account was accessed from an unauthorised device. A virtual Trading 212 card was then used to process five transactions totalling £8,44071.

But Trading 212 refused to refund the transactions. It said that whoever had access to the Trading 212 app used a one-time verification code to register a new Android device. They then created a Trading 212 card and conducted the transactions via the newly registered device.

Miss T wasn't satisfied and so she complained to this service. She said her Trading 212 account was protected by Face ID and she had erased the stolen phone remotely, so she didn't think the app could be accessed by a third-party. She argued that Trading 212 ought to have been concerned that a new device was added just minutes after her phone was erased, and because the login came from an overseas IP address.

But our investigator concluded that Miss T had either shared personal information or allowed someone else to make the transactions. She noted that the IP address for the stolen phone and the device Miss T used to log into the account after she says her phone was stolen both showed in the same area. She explained that to register a new device would have required Miss T's email address, her Trading 212 password, and one-time verification code, which was sent to the stolen phone at 10:33. The new device was then used to open a new virtual card and to process the disputed transactions.

Our investigator said she couldn't see how a third party had gained access to the Trading 212 account, which would have required Miss T's email address and password, as well as the one-time verification code and she commented that she could have notified Trading 212 sooner that her account might be compromised. She questioned why Miss T sent money to her Trading 212 account so shortly after it was compromised and she thought it was suspicious that the account was accessed by the spare phone shortly before the new device was added and the disputed transactions occurred. And she felt the timing of the disputed transactions was inconsistent with them having been made by an unauthorised third party.

Miss T has asked for her complaint to be reviewed by an Ombudsman. She's explained that she sent funds from Bank R to Trading 212 because she was trying to keep it safe.

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 conclusion as our investigator. And for largely the same reasons. I know Miss T feels strongly about this complaint, and this will come as a disappointment to her, so I'll explain why.

Authorisation

Authorisation has two limbs – authentication and consent. So, Trading 212 needs to show the transactions were authenticated as well as showing Miss T consented to them.

Authentication

Trading 212 has shown the transactions were made in person by someone using a virtual card which was created on a device which was correctly registered to the account. So, I'm satisfied they were authenticated.

Consent

Miss T has stated that her phone could only be opened using either her password or Face ID, and I accept that if she'd used it immediately before it was stolen, it might have been unlocked. However, an unauthorised third party would have needed to know Miss T's email address and password to access the Trading 212 account in the app, and there's no plausible explanation for how an unauthorised third party would have had access to this information.

Trading 212 has explained that whoever registered the device which was used to process the disputed transactions to the account was required to enter Miss T's email address and password and a one-time verification code, which was sent to the stolen phone at 10.33. This isn't consistent with Miss T's account that she remotely erased the phone at 10.28. In addition, the IP addresses show the stolen device and Miss T's phone were in the same area, which would be consistent with Miss T still being in possession of the stolen device, while the device used to process the payments might reasonably have been registered to the account by a third party to whom Miss T had given her email address, password and the one-time verification code.

I'm not concerned that Miss T didn't notify Trading 212 as soon as her phone was stolen, but I agree with our investigator that the delay between the phone having been stolen, and the disputed transactions isn't consistent with them having been made fraudulently. In addition, Miss T had sent funds to her Trading 212 account shortly after she says it was compromised and she used her spare phone to log into her account shortly before the new device was added. This activity points towards Miss T's involvement in the disputed transactions.

Overall, having carefully considered the evidence and the circumstances leading up to the disputed transactions, I think it's most likely that Miss T shared her personal information with a third party which enabled them to make the disputed transactions. I consider that in doing so, she consented to transactions, so I'm satisfied Trading 212 has shown they were authorised by Miss T.

My final decision

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 19 March 2026.

Carolyn Bonnell
Ombudsman