DRN-4628799

## The complaint

Mr M has complained that after he lost his phone eToro (UK) Limited didn't prevent a third party accessing his account, liquidating his positions, and transferring the proceeds. He would like his lost funds returned to him.

## What happened

When attending a concert on 10 July 2023 Mr M lost his phone. Mr M returned to the venue, but his phone hadn't been handed in.

Further to unauthorised transactions with other providers Mr M tried to contact eToro but couldn't access his account.

eToro didn't recognise his email address. Mr M then changed his password and email and found a third party – presumably a 'hacker' or malicious third party – had closed his Ethereum and Bitcoin positions and transferred the proceeds to Mr M's eToro Crypto Wallet. The funds were then sent to external wallets and £1,240 was also sent a third-party bank account via Mr M's eToro Money Account.

Mr M raised his concerns with eToro who responded to the complaint but didn't think it should be upheld. It said;

- It had identified logins from a third party by comparing the IP address from two devices that Mr M had used at earlier times.
- Since Mr M had contacted eToro it had ensured his account password was updated and the two-factor authorisation ('2FA') had been enabled. It had also logged out the device that had been logged in via a 'kill session'.
- Mr M's account had been accessed using the correct username and password details. And the third party was able to get the 2FA because they were in possession of the device.
- A withdrawal of US$1600/£1,240 was made and transferred to an external bank account. eToro was trying to retrieve the funds which were subsequently returned.
- It could not find any evidence that eToro had experienced any technical failure or that a security breach had occurred with eToro. So, the third party must have accessed Mr M's login details through other means.

Unhappy with the outcome, Mr M brought his complaint to the Financial Ombudsman Service. After an initial assessment, our investigator who considered the complaint didn't think it should be upheld. He said;

- It would not be fair or reasonable to conclude Mr M's crypto activity was unusual.
- It would not have been unreasonable for Mr M to have transferred the cryptocurrency to his Crypto Wallet before transferring them out.
- The email address change had occurred after the funds had been transferred.

- He didn't think it would be fair to say eToro would have been able to identify potential phone hacking due to unique circumstances.
- The IP address used would not have flagged up any activity as suspicious.

As the complaint remains unresolved, it has been passed to me for a decision in my role as 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.

This complaint concerns the actions, or inactions, of eToro and whether it did anything wrong in respect of its custody of Mr M's holdings and money and its administration of the account that led to him incurring a loss. It doesn't seem to be in dispute by the parties that the situation has arisen because of the actions of a third party acting maliciously to obtain monies.

Mr M said the behaviour on his account was unusual. Multiple small transactions had taken place, everything had been sold which he had never done before, it was a first time use for his eToro card and he hadn't received any communication about a change of password if this was what happened. He hadn't traded in over six months and only ever put money in using his credit card two years earlier.

The proceeds obtained by the third party came from Bitcoin and Ethereum positions Mr M had already opened before the incident which the third party closed and then reinvested into two Bitcoin positions. The cryptocurrency coins were sent onto an eToro Crypto Wallet linked to Mr M's account and from there to external wallets.

As Mr M has said the behaviour on the account was abnormal, I have reviewed the timeline of events to consider whether, at any point, eToro should fairly and reasonably have intervened. Ultimately, I need to consider whether what came about, was because of any failings by eToro.

As a regulated firm, eToro's required to arrange adequate safeguarding for any assets it holds on its customers' behalf. And to implement systems and controls to prevent its services from being manipulated by fraudsters. These obligations are significant. But I should be clear that in the circumstances of this complaint, there's no requirement for eToro to automatically reimburse Mr M if he has been the victim of fraud. I would only require eToro to do so if I was satisfied that both:

1. The transactions Mr M has identified as being unauthorised were suspicious enough that in order to meet with its obligations, eToro ought reasonably to have vetted them further prior to approving them. And,

2. Had eToro vetted the transactions in question then, acting fairly and considering Mr M's best interests as it's required to, it would have concluded that it should not approve those transactions.

I've begun therefore by reviewing the evidence to decide whether, in my opinion, eToro ought to have identified the instructions on Mr M's account as being suspicious. But taking the above into account, I must be fair and reasonable and consider whether eToro was sufficiently aware to the potential of fraudulent action and whether it acted reasonably in its protection of Mr M's account.

We know that Mr M lost his phone sometime on 10 July 2023. I understand Mr M used two devices to access his account prior to the incident – two Android handsets (one with identity number ending 0B2 and the other 18B). The device used during the incident was the one ending 0B2 and was initially used to log in to Mr M's account at 14:04:14 on 10 July.

So, I don't think there was anything in the device use in and itself that would have given eToro cause for concern.

To access Mr M's eToro account the third party would have needed access to his username and password which I understand were successfully used. And because the third party was in possession of Mr M's phone, they would have received the 2FA codes which is an additional layer of security used by eToro to protect an account over and above a username and password. As the username and password were correctly input and the 2FA was successfully applied as part of the login process, I can't conclude there would have been any cause from eToro's perspective that would have made it question whether the person accessing the account was Mr M or a malicious third party. So, at this point in the process I think eToro would have concluded it was most likely Mr M accessing the account.

And I also understand the IP address used was inside the UK, which if it hadn't been would have been another potential 'red flag', namely if it was outside of the UK. But It's not unusual for clients to access accounts away from their usual IP address or via a VPN. And I don't think eToro could have reasonably concluded that a change in IP address, in isolation, was an indication that someone other than Mr M was in control of his account. Particularly as this was corroborated by the fact that the account login had been successfully completed as well as the application of the 2FA.

Mr M contacted eToro on 12 July 2023 saying that his phone had been stolen. And once that contact had been made, eToro ensured the account's password was updated and 'killed sessions' meaning any device logged in was logged out. But from the data eToro has provided it's clear that the many transactions took place on the account and Mr M's positions in Ethereum and Bitcoin were closed and transferred between 10 July and 12 July.

Mr M has said he didn't use his account, but I can see prior to the incident there were opening and closing of positions on his trading platform account. But I accept the first time his Crypto Wallet was used was on 10 July 2023, as does eToro. But my understanding is that it's not unusual for cryptocurrency positions to be left untouched for some time before any trading takes place. It doesn't seem unreasonable to me that eToro wouldn't have taken any action at this time – it is an execution only platform. From its perspective Mr M was starting to trade on his positions which had been dormant for some time.

And eToro told us it is a multi-asset trading platform which means that its clients have access to invest into crypto assets, contracts for difference and stocks once they are on-boarded as a client. The businesses that provided the Money Card and the Crypto Wallets are regulated separately from eToro (UK) so in this decision I'm not making any findings about their roles or any actions they carried out. Once Mr M had opened his eToro UK account and had been fully verified, acting as the account holder, he could open a Crypto Wallet without any additional action from eToro.

This doesn't seem unreasonable to me. From eToro UK's perspective, by Mr M opening a Crypto Wallet may just have been him taking advantage of a further facility it offered within his account. Potentially this could have caused eToro to check this was authentic but considering eToro's multi asset service, I think there wouldn't have been any reason for it to conclude that the transfer out by Mr M to a Crypto Wallet for the first time would have given it cause for concern. This is especially the case as, from eToro's perspective, the person most

likely to be in control of the account, who'd correctly entered the username, password, and provided a 2FA code, was Mr M himself.

On 10 July a withdrawal was initiated – £1,240 – and the funds were sent to Mr M's eToro Money Card. The funds were then sent to an external bank account. But I'm satisfied the bulk of the activity which could be construed as ordinary account activity, most likely to be caried out by the genuine account holder, happened in the lead up to the money being transferred to the Crypto Wallet and Money Cards. And looking at the timeline up to that point, I can't identify anything that should have raised the alarm while the funds were with eToro (UK).

There was a change in one of the account credentials during the incident when the email address linked to Mr M's account was changed at 20:24:53 on 10 July 2023 to what we now know was a third party's email address. However, by this time Mr M's known device had been accessed using the correct login username and password and the 2FA. And the withdrawals totalling US$48,086.70 to the Crypto Wallet had already taken place (at 13:57:25 on 10 July) and so, there wasn't anything that would have pointed eToro to raise any concerns about that change.

I am of course sorry to hear Mr M has found himself in this situation and appreciate how frustrating and distressing this must have been for him. But it must be remembered that the situation stemmed primarily from the loss of his phone and action of a party with malicious intent who had access to Mr M's phone and, it would appear, his eToro account log-in details – username, password and 2FA. While he's clearly been victim of some sort of 'hack', it was nevertheless ultimately his responsibility to ensure the security of his phone and log-in credentials.

While this matter has been very unfortunate, I've not seen that eToro acted incorrectly or unfairly. So, I'm not persuaded it should be required to make good Mr M's losses. No doubt Mr M will be disappointed with my decision – it's clear he feels strongly about his complaint – but I hope I have been able to explain how and why I have reached that decision.

**My final decision**

For the reasons given, I don't uphold Mr M's complaint about eToro (UK) Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 20 March 2025.

Catherine Langley
**Ombudsman**