

The complaint

Mr W complains that Trading 212 UK Limited ("T212") wrongly enabled money to be withdrawn from his trading account.

What happened

The background to the matter will be well-known to both parties, so I'll just briefly summarise what occurred.

In early March 2023 Mr W became aware that some shares held in his T212 account had been sold when he discovered a contract note for the sales in his email spam folder. As he'd not instigated these sales, he attempted to access his T212 account to find out what had happened but was unable to, so he contacted T212 directly.

It transpired that T212 had received a request a few days earlier, sent from Mr W's registered email address, for new bank account details to be added to the account for withdrawals to be sent to. In response to this request, T212 had sought verification documentation to support it, which had been provided, so the new details had been added. The sales of the shares in the account had then been made and a withdrawal of the proceeds requested. T212 had then made the payment.

Mr W explained that he had not instigated any of this activity and as such it appeared that his email account and/or T212 account had been hacked and the bank account to which payment has been made wasn't his.

T212 investigated the situation but concluded that it had done nothing wrong. It was satisfied it had followed its normal procedure, acting in good faith and there had been nothing to cause concern or alert it to any issue with the activity. It shared the view that Mr W's email account had likely been hacked and highlighted the requirement in the terms of the account agreed with Mr W that he was responsible for monitoring the account and ensuring the security of the log-in details.

The complaint was referred to this service and our investigator felt it should be upheld. He acknowledged that in accordance with the terms of the account it was the account holder's responsibility to keep all security details safe. But he went to say, in brief:

- The terms also said that deposits and withdrawals could not be made from and to a third-party account, as it appeared had happened here. So, T212 had been acting contrary to its terms in making the payment as it had done, and the investigator felt Mr W would've been given assurance regarding the security of his account by this term.
- No 'confirmation of payee' process (where a check that the account details and account name match is carried out) had been in place, which would've have identified the discrepancy and prevented the withdrawal going ahead.
- The sales and withdrawal were actioned within 48 hours of the new account details being added.
- The bank details supplied featured a non-British International Bank Account Number

(IBAN).

As such, the investigator felt T212 had acted incorrectly in facilitating the withdrawal and recommended that T212 put Mr W's account back in the position it had been prior to these events, and pay him £250 for the distress and inconvenience caused.

Mr W accepted the investigator's view, but T212 did not. It said, in brief:

- The investigator had misinterpreted the term in the client agreement regarding payments to third parties. This wasn't intended to confirm that payments couldn't physically be made to third-party accounts. Rather, it was intended to clarify how payments between the account holder and T212 should be managed and made.
- The point concerning the IBAN didn't consider the bank in question's pre- and post-Brexit position. It had moved its accounts to its European entity, hence changing the prefix of its IBANs. So, there was nothing unusual about it.
- The sales of holdings and a withdrawal request following closely upon a change of bank account details was not activity in itself sufficient to raise suspicion of potentially fraudulent activity.
- T212 processes its payments in bulk and therefore doesn't carry out payee verification checks. It makes no commitment to do so, nor is it under any regulatory obligation to do so.

The investigator wasn't persuaded to change his opinion. So, as no agreement could be reached, the matter was referred to me to review.

I issued a provisional decision explaining that my review had led me to reach a different conclusion to that reached by the investigator. I didn't think the complaint should be upheld and I explained why. I said, in part:

“...it’s important to stress that this is a complaint concerning specifically the actions, or inactions, of T212. In short, did it do anything wrong in respect of its custody of Mr W’s holdings and money and its administration of the account that led to him incurring a loss? It seems generally agreed by both parties that the matter involved the actions of third party acting maliciously to obtain monies. But here I’m considering solely what T212 did or didn’t do.

As I understand it, T212 received an email from Mr W’s registered email address asking how a new bank account could be added the account. T212 replied explaining its usual process, which involved the provision by the account holder of a photo of their passport, a ‘selfie’ of them holding the passport and a photo of a statement for the relevant bank account.

These three documents were provided to T212 from Mr W’s registered email address and the new account details were added. It’s apparent now that the documents weren’t genuine (although it appears that the passport used was Mr W’s). But I’ve looked at the documents closely and not seen that there was any obvious reason for T212 to question their authenticity.

The sales of Mr W’s share holdings were then actioned, indicating that the person or persons with access to his email account also had access to his T212 log-in details. The payment of the proceeds was then made.

I’ve not seen that T212 deviated in any way from its usual processes for dealing with these types of transactions. While, with hindsight, it’s possible to highlight points where a different course of action on T212’s part might have prevented the withdrawal, that doesn’t necessarily mean it acted incorrectly in managing the process as it did.

The most obvious of these potential different courses of action is, as the investigator suggested, the use of a confirmation of payee process. But that's not something T212 does as standard, in common with other similar providers in such circumstances. So, I'm not persuaded that T212 was acting incorrectly or unfairly in not carrying out such a confirmation.

In respect of its terms of the agreement between Mr W and T212, I don't think that any breach occurred as a result of the withdrawal being paid to what transpired to be a third-party account. I accept T212's view that the term is intended to set out what is expected of the account holder in respect of associating bank accounts with the T212 account under 'normal' conditions. It doesn't mean that payments to third parties are physically prevented in some way, particularly where, as in this case, there has been an apparent malicious intervention by another party and provision of false information.

I am of course sympathetic to Mr W's situation and appreciate how frustrating and distressing this situation must have been for him. But it must be remembered that the situation stemmed primarily from the action of a party who had access to Mr W's email account and, it would appear, his T212 account log-in details. While he's clearly been victim of some sort of 'hack', it was nevertheless ultimately his responsibility to ensure the security of his email and log-in details.

While this matter has been very unfortunate, I've not seen that T212 acted incorrectly or unfairly. So, I'm not persuaded it should be required to make good Mr W's losses."

T212 confirmed it had nothing further to add in response to my provisional decision.

Mr W responded to say that he was unhappy with my decision. He was concerned that his bank details had been changed following an email request and that a request for his passport details and a photograph of him with his passport were accepted. Having been supplied with copies of the documents T212 received, he felt someone should've noted that the photo on the passport and the selfie were not of the same person.

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.

As I noted in my provisional decision, I understand this will have been a distressing and frustrating matter for Mr W. But having looked again at all the evidence and considered Mr W's further comments, I remain unable to conclude that T212 acted incorrectly or unreasonably in the way that it handled the matter.

The email address used in the interactions between T212 and the person purporting to be Mr W was the email address registered to the account. In respect of the photo of the passport and selfie provided, I note Mr W's comments but as I said before I've looked at the documents closely and not seen that there was any obvious reason for T212 to question their authenticity.

While I recognise that it will be very disappointing for Mr W, I am still of the view that the complaint should not be upheld.

My final decision

For the reasons given, my final decision is that I don't uphold the complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 5 September 2024.

James Harris
Ombudsman