DRN-4947800

The complaint

Mr T complains that Trading 212 UK Limited ("T212") wrongly enabled money to be withdrawn from his trading account.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 March 2023 Mr T became aware that the shareholdings in his T212 account had been sold and a withdrawal of the proceeds made. He contacted T212 but it was unable to stop the transactions, the withdrawal having been processed and sent to a bank account that didn't belong to Mr T.

T212 explained that it had received a request, apparently sent from Mr T's account, to withdraw the money held on the account. It replied and in line with its usual process, requested verification documents – a photo of Mr T's passport, a 'selfie' showing him holding the passport and a photo of a statement for the new bank account. These were provided and the withdrawal request completed.

Mr T complained about the matter to T212 as he didn't feel it had taken sufficient steps to protect his account. He said that the documents supplied to it had been falsified. But having investigated the situation T212 concluded it had done nothing wrong. It was satisfied it had followed its normal procedure, acting in good faith and there'd been nothing to cause concern or alert it to any issue with the activity. It felt that Mr T's email account had likely been hacked and it highlighted that in accordance with the terms of the account Mr T was responsible for monitoring it and ensuring the security of the log-in details.

The complaint was referred to this service and our investigator felt it should be upheld. In brief, he noted the terms of the agreement between Mr T and T212, which said that deposits and withdrawals could only be made from accounts belonging to the T212 account holder. The investigator felt that T212 had therefore breached the terms of the agreement by allowing what had transpired to be a payment to third party, not Mr T. The investigator also felt that T212 should've utilised a 'Confirmation of Payee' check to confirm that the new account details – sort code and account number – matched with Mr T's name. Had it done such a check, he felt the discrepancy would've come to light and the withdrawals not processed. The investigator also noted that T212 had not previously requested a copy of Mr T's passport, for instance at account opening, so it had had no way of making a comparison to determine if the passport and selfie supplied to it were genuine.

The investigator felt that T212 had therefore failed to take account of its general regulatory responsibilities to maintain effective systems for countering the risk of financial crime and to act in its customers' best interests. The investigator did acknowledge that the situation had, in part at least, seem to have been caused by Mr T's email account/T212 account being hacked. But he felt overall there had been opportunities for T212 to have prevented the situation. He considered T212 should therefore make good Mr T's losses and pay him £400 for the distress and inconvenience caused.

T212 didn't accept the investigator's view. In brief, it said that there'd been no requirement for a copy of Mr T's passport to be provided when the account was opened. And it reiterated that it had followed its usual process for a change of bank details and said it felt the investigator had misinterpreted the term in the client agreement regarding payments to third parties. This didn't imply 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 made.

Further, T212 processed payments in bulk, so didn't carry out confirmation of payee verification checks. It made no commitment to do so and was under no regulatory obligation to do so. T212 stressed it had followed its usual verification procedures correctly and highlighted again that the situation had arisen by way of a 'hack' of Mr T's account/s.

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

I issued a provisional decision explaining that I'd reached 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:

"I think it's important to stress that this is a complaint specifically concerning the actions, or inactions, of T212. In short, did it do anything wrong in respect of its custody of Mr T'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.

It's not entirely clear whether the withdrawal request came from Mr T's registered email account or from his T212 account. But either way, it was made as a result of an apparent hack of his email/T212 account details. While I accept he was likely the victim of fraud – which I note he has reported to the appropriate authorities – he was nevertheless responsible, in line with the terms of the agreement between him and T212, for maintaining the security of his log-in details.

Upon receipt of the withdrawal request it appears that T212 followed its normal procedure to verify it. It's apparent now that the documents supplied to it as part of that process had been falsified. But having looked at them I don't think there was anything obvious about them that ought to have alerted T212 to a potential issue.

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 that 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 providers in similar 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 T 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 in question 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 T's situation and appreciate how frustrating and distressing this situation must have been for him. But it must be remembered that it primarily, if not wholly, stemmed from the action of a party who had access to Mr T'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 that it should be required to make good Mr T's losses."

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

Mr T made further submissions, focussing in particular on T212's account opening processes. He felt information should've been obtained from him when the account was opened that could've been compared with the doctored information later provided by the fraudster, preventing the withdrawal. He also many several other points, in brief:

- The IP address associated with the withdrawal wouldn't have been consistent with his location.
- The access was only by email, and it hadn't been shown that the T212 account was logged into.
- How was the sale and withdrawal activity completed? Was it done via his T212 account or separately?
- There was a discrepancy in the date of birth information held T212 for him.
- Was there anything to show that the security breach had not been on the part of T212?
- He'd never shared any information about his log-on details with anyone.
- His email account and his T212 had different passwords.

In light of Mr T's comments, further information was sought from T212 regarding the account opening process, how the sales and withdrawals were actioned and the date of birth information.

Upon receipt, a summary of the information was provided to Mr T. T212 confirmed that its system in 2020 automatically verified his account without the need for verification documents. His details were submitted within the application, which were run against a proprietary electronic verification system, verifying automatically that there was a match.

T212 also confirmed that sale and withdrawal instructions were only accepted via its platform. The withdrawal in this case was requested from the platform and as the original payment details were out of date T212 had contacted the email address registered to the account to request the verification documents, which were then provided. T212 provided a copy of the withdrawal request, showing that it was instigated on-line, from Mr T's T212 account.

It was explained to Mr T that while I could understand his concern that the account opening process didn't appear to be wholly in line with the current requirements described on T212's website, I was satisfied it had acted reasonably in 2020 and was entitled to open the account using the process it had in place at the time. I accepted that if a copy of Mr T's passport had been provided in 2020 a comparison would've been possible, but I didn't consider it was wrong of T212 to not have obtained a copy at that time.

In respect of the other points Mr T had raised in response to my provisional decision, it was

explained to Mr T that –

- There was no evidence to indicate that T212 was responsible for any data breach that enabled the fraudster to obtain Mr T's email and/or T212 security details.
- Although a UK IP address was logged against the withdrawal request, it would not be usual process to perform any sort of IP address and location check.
- While I noted the concerns Mr T had raised regarding the photo used on the doctored passport, I didn't feel it was sufficiently unusual to have prompted further action by T212.
- In respect of Mr T's date of birth, T212 confirmed it had a record of the correct date, which matched that shown on the doctored passport.

Mr T remained of the view that I hadn't addressed his concerns fully. He maintained that T212 had failed to follow its account opening process correctly and questioned again whether it could've been responsible for a data leak that enabled his details to be compromised. He also raised concerns that an ID number registered to his account wasn't his, suggesting a failure of process on T212's 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.

Having done so, I remain of the view that the complaint should not be upheld. As I said in my provisional decision, I understand how distressing and frustrating this matter will have been for Mr T. But, having looked carefully at the details of the situation, the evidence available and, as noted, having sought further information following my provisional decision, I'm still unable to conclude that T212 acted incorrectly.

I note Mr T's points about the account opening process. Clearly, had it involved the provision of his passport a comparison could potentially have been made that would've alerted T212 to an issue. But it wasn't part of T212's process to obtain a copy of ID documents in 2020. It carried out an electronic check. And even if there had been some sort of error made when the account was opened, it wouldn't necessarily mean the complaint should be upheld, not unless that error could be shown to have directly led to the fraud being facilitated.

Mr T has questioned the ID number that T212 has registered to his account. It appears to be a National Insurance number, and Mr T says it isn't his. T212 has said it was provided by Mr T, not at the account opening stage, but later in December 2021. There's clearly a conflict here, but ultimately, I don't think it's relevant to my findings in respect of whether T212 acted correctly in March 2023 when the sales and withdrawal occurred. As I said in my provisional decision, T212 followed its usual procedure at that time. And that didn't include making any reference to the ID number. So, whether it was correct or not would not appear to have made any difference.

I do understand why Mr T has picked up on various apparent discrepancies in T212's process and information. I can see why he would feel that these undermine the robustness of T212's systems. But, as I say, unless they were directly related to the sale and withdrawal process, I don't feel they impact on the matter.

I understand Mr T will be very disappointed, as I recognise his strength of feeling, but I'm unable to conclude that T212 acted incorrectly.

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 T to accept or reject my decision before 5 September 2024.

James Harris
Ombudsman