

**MEMO# 31356**

August 28, 2018

# **FINRA Sanctions Broker-Dealer for Fraudulent Transfers Resulting from Hacking of Customer's Email**

[31356]

August 28, 2018 TO: Broker/Dealer Advisory Committee  
Chief Information Security Officer Advisory Committee  
Compliance Advisory Committee  
Operations Committee  
Transfer Agent Advisory Committee RE: FINRA Sanctions Broker-Dealer for Fraudulent Transfers Resulting from Hacking of Customer's Email

FINRA recently announced that it has censured and fined one of its members \$50,000 for processing fraudulent wires that resulted from the hack of a customer's email.[\[1\]](#) According to the settlement of this matter, the broker-dealer violated FINRA Rule 3110, relating to supervisory procedures, and Rule 2010, relating to high standards of commercial honor, by having inadequate procedures to protect its customer from such fraudulent activity. The facts leading to FINRA's sanctions are briefly described below.

According to FINRA's AWC, while the Respondent in the case did not have any written supervisory procedures that addressed wire transfer of customers' funds to third-party accounts, it followed a routine and accepted firm practice to process such transfers. Customers who utilized the firm's bill payment service would sign a blank letter of authorization (LOA) form so they would not have to sign a new LOA for each future transfer. The firm's practice, in connection with these transfers, was for a firm employee to contact the customer who requested the wire transfer about its specifics. This contact was typically made via email. The employee would then complete a copy of the LOA that the customer had previously signed in blank and present it to a compliance assistant, who would process the form and the payment. The LOAs were not sent to the customer as or for confirmation.

In February 2015, a customer notified the firm to expect her requests for fund transfers in the near future from her trust accounts, without providing the specifics. On February 27th, the customer requested a wire transfer of approximately \$570,000 to a title company. This request was processed using a pre-signed LOA in accordance with the firm's practice. Within the next few days, the customer's email account was hacked and, between March 4-11, the Respondent received requests for five wire transfers that ranged from \$16,000 to \$77,000 and that totaled over \$207,000. When the Respondent received these wire

requests, it did not contact the customer to verify them – instead, it used the pre-signed LOAs it had on file to process them.<sup>[2]</sup> Following these wires, the firm received a request, allegedly from the customer, to wire \$205,710 to a company in Malaysia. The firm was suspicious of this request and contacted the customer to verify its legitimacy. It was only then that the fraud was discovered. The firm, working with its clearing firm, was able to recover all but approximately \$62,000 of the fraudulent transfers. It reimbursed the customer for their full amount and self-reported the violations to FINRA.

FINRA found that the supervisory system the firm had in place was not reasonable because (1) it allowed the firm's employees to copy pre-signed, blank LOA forms as the sole means for recording the customer's authorization for third-party wire transfers and (2) there was no notification to or follow up with a customer for each transfer. The AWC notes that the firm has revised its supervisory procedures to require a newly signed LOA with each wire transfer and to confirm each such transfer with the client.

Tamara K. Salmon  
Associate General Counsel

#### **endnotes**

<sup>[1]</sup> See *In Re Buttonwood Partners, Inc. Acceptance, Waiver and Consent* (AWC), FINRA (No. 2015045144001, dated Aug. 20, 2018), which is available at: [http://www.finra.org/sites/default/files/fda\\_documents/2015045144001%20Buttonwood%20Partners%20Inc%20CRD%2027108%20AWC%20sl.pdf](http://www.finra.org/sites/default/files/fda_documents/2015045144001%20Buttonwood%20Partners%20Inc%20CRD%2027108%20AWC%20sl.pdf).

<sup>[2]</sup> Also, although the last of these wire transfers did not go through because the account receiving the transfer had been closed, the Respondent never followed up with the customer about it.