## Important Fraud Prevention Information from Pershing

Federal Trade Commission data show that consumers reported losing more than $10 billion to fraud in 2023, marking the first time that fraud losses have reached this benchmark. This marks a 14% increase over reported losses in 2022, according to **ftc.gov.** Trends in 2024 do not suggest the trend is abating. In most cases, these fraudulent events become financial exposure, ultimately making your firm the victim of these fraudulent activities.

To mitigate this risk, your firm has a responsibility to **verbally** verify all asset movement instructions with investors on the day of the asset movement**.** Additionally, your firm has obligations under Financial Industry Regulatory Authority® (FINRA®) NTM 12-05 about detecting and preventing fraud. Fraud attempts occur, and are sometimes successful, if these practices are not consistently followed.

### Best Practices for Investor Confirmation of Asset Movement Instructions

Listed below are best practices for **confirming** asset movement instructions are valid

- Verbally confirm the specific instructions, such as bank routing details and account names, for all disbursement requests and not only third-party transfers.
- Fraudulent requests can appear as both first and third party.
- Make the confirmation call on the same day. Always call the investor on the number on his/her account profile. Verify the identity of the person being called with security/challenge questions, even if on a known phone number.
- Confirm the account profile had no recent updates prior to calling the investor.
- Verbally confirm all written instructions, whether it be in email, fax or in writing. This includes instructions between an advisor/assistant and an operations team.
- Confirm the payment reason and relationship to a third-party disbursement, as well as how the investor obtained the payment instructions. If the instructions were received via email, caution your investors, and recommend they call the intended recipient on a known phone number to confirm the instructions.
- If payments or transfers are rejected/returned by the receiving bank, verbally confirm with the investor again regarding any attempt to re-send the disbursement. This might be your second chance to stop a fraudulent transaction.
- Never conduct your confirmations via email.
- Never use signature comparisons as a stand-alone confirmation method.

## Fraud Prevention: Red Flags

Unauthorized disbursements often start with a compromised email address sending fraudulent instructions to transfer assets. The instructions may request assets to/from same name or third-party accounts. Listed below are some of the red flags associated with these scenarios:

- Requests expressing an undue sense of urgency.
- Requests for an exception regarding callback or verbal confirmation policies.
- Requests for accommodation because a family member or relative needs something accomplished quickly.
- Letters of authorization (LOAs) for payments or services inconsistent with the expected activity of the account holder. LOAs with signatures that seem 'copy and pasted' from prior requests.
- Executive spoofing scenarios where an associate of a firm acts on a fraudulent email instruction they believed to be coming from an executive of the firm. Requests to change settlement instructions or authentication methods.
- Large, unusual cash or securities movements.
- Disbursement requests to institutions not previously known to be associated with the account holder.
- Misspelled contact or email domain names.

## Select Relevant FINRA Regulatory Notices

**(12-05)**
Verification of Emailed Instructions to Transmit or Withdraw Assets from Customer Accounts

**(20-32)**
Reminds Firms to Be Aware of Fraudulent Options Trading in Connection with Potential Account Takeovers and New Account Fraud

**(21-14)**
Alerts Firms to Recent Increase in ACH "Instant Funds" Abuse

**(21-18)**
Shares Practices Firms Use to Protect Customers from Online Account Takeover Attempts

**(22-18)**

Reminds Firms of Their Obligation to Supervise for Digital Signature Forgery and Falsification

**(22-31)**
Shares Practices for Obtaining Customers' Trusted Contacts

**(23-06)**
Shares Effective Practices to Address Risks of Fraudulent Transfers of Accounts Through ACATS

Please contact us if you have any questions.