

## **Important Fraud Alert – Potential Scam Involving Third Parties Impersonating Clipper Fund**

Clipper Fund has become aware of potential scams in which third parties may falsely claim to represent or be affiliated with Clipper Fund in an attempt to commit fraud. These individuals may attempt to contact investors by telephone, email, text message, social media, messaging applications, or other means in an effort to obtain personal or financial information or initiate unauthorized financial transactions. These activities are not affiliated with or authorized by Clipper Fund in any way.

Clipper Fund is not responsible for any losses you may experience resulting from communications or interactions with such individuals.

### **What is Spoofing?**

Spoofing refers to the forgery of sender information (e.g., email addresses, phone numbers, websites) to make communications appear as though they come from a trusted source such as Clipper Fund.

### **Protect Yourself**

If you are contacted by or receive communication from someone claiming to represent Clipper Fund that you do not recognize, and/or you are uncertain of its legitimacy:

- Do not provide passwords, security codes, account credentials, or other sensitive information. Legitimate organizations will never ask for this via email or text.
- Do not authorize requests to transfer or withdraw money, change payment instructions, or provide banking instructions.
- Avoid opening links/attachments in emails or text messages that you are not expecting.
- Hang up the telephone or close the email or text and contact us using a trusted telephone number or contact information you already have on file or listed on our official website, clipperfund.com.

### **Report Suspicious Activity**

If you receive a suspicious communication from someone claiming to represent Clipper Fund, please report it to [CRInvestor.Services@dsaco.com](mailto:CRInvestor.Services@dsaco.com).

When possible, we ask that you provide information that may help us evaluate the incident, including:

- Your full name and contact information (physical address, telephone number, email address).
- The date and approximate time of the communication or when you were contacted.
- The telephone number, email address, username, or account used to contact you.
- A description of what occurred or what was requested (provide as much information as you can detail about the event).
- Copies or screenshots of any written communications, emails, text messages.
- Your yes-or-no responses to the following questions, if applicable:
  - Did you open links or images within the email or text message?
  - Did you enter or submit any of your login credentials?
- When you email us, please do not include passwords, PINs, verification codes, or other sensitive credentials.

While Clipper Fund is under no obligation to take any action based on this information, reporting suspicious activity may assist Clipper Fund in identifying fraudulent activity and taking appropriate steps to help protect our investors and organization.

If you believe you are a victim of fraud or a scam, you should also consider reporting the incident to a law enforcement agency, or government authority on your own behalf. Please note that any outreach by Clipper Fund to law enforcement regarding any fraudulent activities will be conducted solely on behalf of Clipper Fund.

**Your security is important to us. Please remain vigilant and independently verify any unusual request involving your account or personal information.**