SHOREBIRD CAPITAL MANAGEMENT, LLC

PRIVACY POLICY STATEMENT

Neither the Firm nor any of its Supervised Persons may share nonpublic personal information of consumers with nonaffiliated third parties, except as required in order to provide the services offered. Client information will be safeguarded by restricting access to the information to only those employees who need access in order to service the client's account. The Designated Principal is responsible for ensuring that security controls are adequate to prevent unauthorized persons from accessing information.

Hard copy documents should be secured by locking the file cabinet or office in which they are stored. Information kept on the Firm's computers should be passwordprotected and secured behind firewalls. A paper shredder is to be used for destruction of all client-related documents that are not required to be retained by the Firm. All Supervised Persons will participate in new hire training, and additional training at least once annually thereafter.

Privacy Notices

The Firm must provide new clients with an initial privacy notice and annual privacy notices thereafter. The Designated Principal is responsible for compliance with Regulation S-P, including the following: • Providing an initial notice to each client; • Sending an annual notice to clients (excluding certain institutional investors) for as long as the relationship continues; • Safeguarding customer records and information; and • Including all of the required disclosures and information in all notices to clients.

Reporting Privacy Violations

If at any time a Supervised Person suspects the misuse or mishandling of confidential information or identity theft, he must immediately notify the Designated Principal. As required or deemed appropriate, the Designated Principal will promptly report any suspected identity theft to the SEC and Federal Trade Commission and retain copies for the files. The CCO is ultimately responsible for ensuring compliance with Regulation S-P.

Breach Notification Laws

Many states have laws that require notification to persons affected by data breaches. In the event of a breach involving client or investor information, the Designated Principal will ensure that the Firm complies with applicable state laws.

Testing

The Firm will perform reasonable testing of its information safeguards at least annually. Additionally, the Firm will perform testing of any new technologies to assess whether they pose any risks to clients' information and privacy. The Designated Principal is responsible for overseeing such testing functions and ensuring that they are adequate.