SECTION 14 – PRIVACY POLICY

INTRODUCTION

This section of the Manual explains how BAMCO collects, utilizes and maintains non-public personal information about its Clients, as required under federal legislation. This privacy policy only applies to non-public information of Clients who are individuals.

The Gramm-Leach-Bliley Act (the "**GLB Act**"), passed in November 1999 provides certain privacy requirements, such as the protecting of personal information of consumers. In response to privacy requirements of the GLB Act, the SEC issued Regulation S-P in June of 2000, effective in November of 2000, and required mandatory compliance by July 2001.

Regulation S-P imposes complex and affirmative obligations on SEC registered investment advisers, broker-dealers and investment companies, among others. Regulation S-P prohibits the sharing of non-public personal information with any non-affiliated third parties unless the firm has provided notices of its privacy policies and an opt-out notice for consumers or customers to opt-out of the disclosure of such information.

The Fixing America's Surface Transportation Act (the "FAST Act") enacted in December 2015 updated an investment adviser's Privacy Policy notice requirements and clarifies investment advisers' obligations with regards to the Privacy Rules. Under the FAST Act, investment advisers are not required to send annual Privacy Notices to "consumers" if the adviser (i) only shares nonpublic personal information with nonaffiliated third-parties in a manner that does not require an opt-out right be provided to customers; and (ii) has not changed its policies and procedures with regards to disclosing nonpublic personal information since it last provided a Privacy Notice to customers.

STATEMENT OF POLICY

BAMCO is required to develop, implement and maintain a comprehensive information security program to provide administrative, technical and physical safeguards and respond to unauthorized access or use of customer information. In adopting this program for the protection of customer information (the "**Program**"), BAMCO seeks to (i) promote the security and confidentiality of Client information, (ii) protect against any anticipated threats or hazards to the security or integrity of Client information; and (iii) protect against unauthorized access to or use of Client information that could result in substantial harm or inconvenience to any Client, employee, Fund investor or security holder who is a natural person.

In general, the privacy rules require that firms provide a "clear and conspicuous" notice that reflects its privacy policies and procedures to a Client at the time of establishing a Client relationship and as best practice, will be provided annually thereafter as long as the relationship exists. A Client is one who has established a continuing relationship with BAMCO.

Identity Theft Protections

Prevention of identity theft is an integral aspect of the BAMCO's privacy program. Advisory employees should evaluate the extent to which the Firm's information safeguards and protection systems are adequate in preventing unauthorized access to client-sensitive nonpublic personal information. Identity thieves using client nonpublic personal information may be able to gain access to Clients' custodial account(s) for purposes of (1) liquidating the accounts and rerouting the proceeds to third-party account(s), (2) laundering money, and (3) engaging in fraudulent pump and dump schemes. Often the evidence will reflect that the account holder was engaged in the unlawful activity, and not the true perpetrator. The end result for the Firm is that if this information was accessed as a result of an advisory client having a relationship with the Firm then it will negatively impact that adviser-client relationship.

Any questions pertaining to the BAMCO's identity theft prevention initiatives should be addressed with the CCO.

MONITORING REG. S-ID COVERED ACCOUNTS

Identification of Red Flags

A "covered account" is defined in line with Regulation S-ID, which states that the definition includes "(i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[12]

The Firm will maintain a Red Flag Watch List detailing all clients determine to be a "covered account" and will be subjected to more stringent security precautions. The CCO will oversee the ongoing adequacy of related policies as well as the implementation of this program.

The following trigger placement on the Red Flag Watch List:

- Alerts, notifications, or other warnings from consumer reporting agencies or fraud detection service providers, as applicable;

- Presentation of suspicious documents, appearing to have been altered or forged, or that contains Nonpublic Personal Information inconsistent with other information in application;

- Presentation of suspicious Nonpublic Personal Information. This includes, *inter alia*, Nonpublic Personal Information inconsistent with Firm records, Nonpublic Personal

[12] Identity Theft Red Flags Rules, Release Nos. 34-69359, IA-3582, IC-30456, Securities and Exchange Comm'n, 23 (2013) *available at* http://www.sec.gov/rules/final/2013/34-69359.pdf

Information associated with known fraudulent activity, or inability to supply complete Nonpublic Personal Information;

- Unusual use of, or other suspicious activity, related to a covered account, including notification of unauthorized withdrawals or a request for withdrawal from the account that does not conform to the established pattern of activity and the request comes via email/mail or some other channel where the identity of the client remains unauthenticated;

- Address Change Requests of a covered account;

- Notification by Client that the security of Nonpublic Personal Information may have been compromised, or that the security of their email/mail has been compromised. This includes notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

The Red Flag Watch List will also include a list of all Nonpublic Personal Information that has been associated with known fraudulent activity.

If a Client is placed on the Red Flag Watch List, then the Firm will monitor certain activites related to the covered account for evidence of identity theft, and transfers of third party payments by the covered account will require verbal confirmation from the client either via phone or personal interaction or as prescribed by the client's custodian (e.g., Charles Schwab). Clients will remain on the Red Flag Watch List as determined by the Adviser.

Interactions with Covered Accounts

Whenever the Firm receives a request to open an additional covered account, the following information must be obtained or updated from the Client as necessary in order to confirm identification:

- Personal information, including name, address, date of birth, social security number, and signature

- Account information for the funding source

This information must be compared to existing records, as well as the Red Flag Watch List maintained by the Firm. If the Client appears on the Red Flag Watch List, the Client must be contacted either in person or via phone for a verbal confirmation by a staff member familiar with the client's voice. If any of the information supplied is inconsistent with existing Firm records, the client must be contacted either in person or via phone for a verbal confirmation. If the Nonpublic Personal Information supplied matches Nonpublic Personal Information associated with known fraudulent activity, as recorded on the Red Flag Watch List, then the Client must likewise be notified and a verbal confirmation received. Absent the requisite verbal confirmation, no covered accounts may be created.

Whenever the Firm receives a request to transfer funds from, or modify the information associated with, a covered account (including change of address), the Firm will confirm the following:

- If a change of address is requested, the address will be compared to Firm records to ensure that the address is one previously supplied by the Client as a valid address. If the address is not one currently on file with the Firm as the preferred address, the Client must be contacted either in person or via phone for a verbal confirmation of address validity. .

- If a fund transfer is requested, the destination account will be checked against existing Firm records to determine whether prior transfers have occurred to or from the destination account. If the destination account is not one previously associated with the covered account, the Client must be contacted either in person or via phone for a verbal confirmation. A Client must provide authorization and wiring instructions to the qualified custodian prior to BAMCO wiring any client funds.

- If any interaction occurs with a covered account where the client has been placed on the Red Flag Watch List, the client must be contacted either in person or via phone for a verbal confirmation by a staff member familiar with the Client's voice.

Ongoing Review of Regulation S-ID Policies and Procedures

The CCO will review, at minimum annually, the policies and procedures relating to Regulation S-ID. In conducting the review, the CCO may assess the following non-exhaustive factors: (a) the Firm's experiences over the prior calendar year with identity theft; (b) the changes, if any, in methods of identity theft; (c) whether any changes in methods of detecting, preventing or mitigating identity theft are called for; (d) changes in the business arrangements of the Firm, including the types of accounts that the Firm interacts with.

The annual review may also include: details of the nature of all identity theft incidents over the past year, an evaluation of the effectiveness of existing policies and procedures, an analysis of service provider arrangements, and recommendations for material changes to existing policies and procedures.

Collection of Information

BAMCO generally collects personal information about its Clients through the following sources:

- Subscription documents, custodian account applications, Advisory Agreements, IPS's, and other information provided by the client in writing, in person, by telephone, electronically or by any other means.

- This information can include:

    - Name;
    - Address;
    - Nationality;
    - Birthdate;
    - the name address and nationality of the investors as well as the Tax Identification Number; and

- Transactions with BAMCO either through a pooled investment vehicle or a separately managed account.

Disclosure of Non-Public Personal Information

BAMCO does not sell or rent Client information. BAMCO does not disclose non-public personal information about its Clients or Fund investors to non-affiliated third parties or to affiliated entities, except as permitted by law. For example, BAMCO may share non-public personal information in the following situations:

- To service providers in connection with the administration and servicing of the Client Accounts, which may include attorneys, accountants, auditors and other professionals. BAMCO may also share information in connection with the servicing or processing of Client transactions.

- To affiliated companies in order to provide the Client with ongoing personal advice and assistance with respect to products and services purchased through BAMCO and to introduce the Clients to other products or services that may be of value to the Client.

- To respond to a subpoena or court order, judicial process or regulatory authorities;

- To protect against fraud, unauthorized transactions (such as money laundering), claims of other liabilities; and

- Upon the consent of a Client to release such information, including authorization to disclose such information to persons acting in a fiduciary or representative capacity on behalf of the Client.

Massachussetts Information Security Regulations

The Massachusetts Standards for the Protection of Personal Information (201 CMR 17.00) (the "**Standards**") applies to all firms that maintain personal information about a Massachusetts resident regardless of the location of BAMCO. As such, financial services firms such as investment advisers with access to "personal information" (as defined below) about a Massachusetts resident generally must meet the Standards.

Under the law, "personal information" to be protected includes a Massachusetts resident's name (either first and last name or first initial and last name) combined with a complete social security number, driver's license, or other state-issued number, a financial account number or a complete credit card or bank account number.

BAMCO has established the following procedures in relation to protecting Client data:

- Assess information security risks periodically;
- Terminate access to information by former Employees;
- Oversee service providers;
- Place reasonable restrictions on physical records;
- Implement secure user authentication and access controls for electronic systems;

- Encrypt, where feasible, all electronically transmitted records;
- Maintain up-to-date virus definitions, firewall protections, and operating system security patches;
- Provide initial and ongoing training to Employees; and
- Document the responses to information security breaches and records of corrective actions taken as a result of the breach.

It is essential that BAMCO dispose of such non-public personal information in a secure fashion when it is no longer required for record keeping requirements. In general, BAMCO will have methods to shred physical documents as well as the erasure and over-writing of electronic media.

OPERATING PROCEDURES AND COMPLIANCE REVIEW

It is BAMCO's policy to require that all employees, financial professionals and companies that provide services on behalf of BAMCO, keep Client information confidential.

BAMCO maintains safeguards that comply with federal standards to protect Client information. BAMCO restricts access to personal and account information of Clients to those employees who need to know that information in the course of their job responsibilities. Third parties with whom BAMCO shares Client information must agree to follow appropriate standards of security and confidentiality. BAMCO's privacy policy applies to both current and former clients. BAMCO delivers a Privacy Policy to all clients annually as best practice.