CLARKSTON CAPITAL PARTNERS, LLC

Privacy Policies and Procedures

I. Introduction

Clarkston Capital Partners, LLC ("CCP") is committed to protecting the confidentiality of all Nonpublic Personal Information regarding its clients. "Nonpublic Personal Information" means personally identifiable financial information about "consumers" (as that term is defined in Regulation S-P) and any list, description or other grouping of "consumers" (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information.

CCP is an investment adviser registered under the Investment Advisers Act of 1940, as amended ("Advisers Act") and, as such, has a general fiduciary obligation to keep all client records and information confidential. CCP also has considered state law requirements when formulating its privacy practices. While the terms "consumer" and "customer" have specific definitions under Regulation S-P, all Nonpublic Personal Information relating to CCP's clients (including current and former) is subject to these Privacy Policies and Procedures.

In the event of new privacy-related laws or regulations or identified new threats or hazards affecting the information practices of CCP, these Privacy Policies and Procedures will be revised as necessary and any changes will be disseminated and explained to all CCP employees.

II. Policies

CCP will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. CCP will not disclose Nonpublic Personal Information except (i) in accordance with these Privacy Policies and Procedures, (ii) as permitted or required by law, or (iii) as authorized in writing by the client. CCP will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, CCP will strive to: (i) ensure the security and confidentiality of the information; (ii) protect against anticipated threats and hazards to the security and integrity of the information; and (iii) protect against unauthorized access to, or improper use of, the information.

Although these policies and the following procedures apply specifically to Nonpublic Personal Information, employees must be careful to protect all of CCP's confidential and proprietary information.

III. Procedures for the Protection of Nonpublic Personal Information

A. General

To protect Nonpublic Personal Information, CCP maintains appropriate security measures for its computer and information systems and, by reference, incorporates CCP's Identity Theft and Cybersecurity policies and procedures into these Privacy Policies and Procedures.

CCP's Privacy Policies and Procedures are designed to provide administrative, technical and physical safeguards to assist employees in maintaining the confidentiality of Nonpublic Personal Information collected from CCP's clients.

Employees should notify CCP's Chief Compliance Officer ("CCO") promptly of any threats to the security of, or improper disclosure of, Nonpublic Personal Information. Employees with questions concerning the collection and sharing of, or access to, Nonpublic Personal Information of CCP's clients must look to the CCO for guidance. A violation of these Privacy Policies and Procedures is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

B. Protecting Confidential Information

Each employee is required to sign a confidentiality agreement upon being hired by CCP. Each employee has a duty to maintain the confidentiality of information acquired in connection with their employment, with particular care being taken with regard to Nonpublic Personal Information.

Nonpublic Personal Information will be restricted to employees who have a need to know such information to either provide services to a client or conduct operations, or otherwise have a legitimate business purpose to have access to the information.

No employee is authorized to sell, on behalf of CCP or otherwise, Nonpublic Personal Information of CCP's clients.

C. Information Stored in Hard Copy Formats

CCP has implemented the following procedures to protect Nonpublic Personal Information stored in hard copy formats:

1. Employees are required to keep hard copy documents containing Nonpublic Personal Information in a secure facility, compartment(s) or receptacle(s) that is locked nightly ("clean desk policy").

2. Documents containing Nonpublic Personal Information being printed, copied or faxed must not be left unattended.

3. Employees are required to exercise due caution when mailing or faxing

documents containing Nonpublic Personal Information to ensure that the documents are sent to the intended recipients.

4. Employees are required to shred or dispose in a secure recycling bin any written documents containing Nonpublic Personal Information that CCP is not required to maintain.

5. The Chief Operating Officer ("COO") will ensure that storage areas are protected against destruction or potential damage from environmental hazards.

6. Employees may only remove documents containing Nonpublic Personal Information from CCP's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable.

D. Electronic Information Systems

CCP has implemented a Cybersecurity Policy that includes procedures designed to protect Nonpublic Personal Information stored on electronic systems. Employees are required to comply with CCP's Cybersecurity Policy when accessing and utilizing electronic systems that contain Nonpublic Personal Information.

Employees must utilize the utmost care to prevent improper or unauthorized use of access to client accounts. Any actual or suspected breach of security involving client accounts must immediately be reported to the CCO.

E. Discussions Including Nonpublic Personal Information

Conversations involving Nonpublic Personal Information should be conducted by employees in private, and care should be taken to prevent any unauthorized persons from overhearing or intercepting such conversations.

F. Working in Public Places and from Home

Employees should avoid discussing Nonpublic Personal Information in public places where they may be overheard, such as at conferences, in restaurants and in elevators. Employees should be cautious when using laptops or reviewing documents that contain Nonpublic Personal Information in public places to prevent unauthorized people from viewing the information.

Each employee working from home will be subject to the same standard of care, and will take the same precautionary measures, as employees working from CCP's office to safeguard Nonpublic Personal Information.

G. Discarding Information

Employees may only discard or destroy Nonpublic Personal Information in accordance with the following procedures:

1. The CCO has the sole authority to permit the destruction of any required record. No required record will be destroyed before the required retention period has lapsed.

2. Employees are reminded that electronic and hard copy media containing Nonpublic Personal Information must be destroyed or permanently erased before being discarded. Any employee discarding any document or electronic media containing Nonpublic Personal Information must ensure that such documents and electronic media are shredded, permanently erased, or otherwise destroyed so that the information cannot be reconstructed. Employees should be aware that some devices, such as scanners, photocopiers and fax machines, may save electronic copies of documents that have been scanned, copied, or transmitted. Employees should consult with the device's instruction manual or manufacturer to ensure that any stored information is erased before the device is removed from CCP's offices.

3. CCP must ensure that any companies engaged to dispose of Nonpublic Personal Information perform their duties in accordance with the Policies and Procedures. The COO is responsible for ensuring that such companies appropriately dispose of CCP's information, and may do so by, among other things:

   a. reviewing an independent audit of the disposal company's operations;

   b. obtaining information about the disposal company from references or other reliable sources; and/or

   c. requiring that the disposal company be certified by a recognized trade association or similar third party.

IV. Disclosure of Nonpublic Personal Information

A. General Requirements

Employees are required to comply with CCP's Identity Theft Prevention Program, which includes but is not limited to a prohibition against sharing Nonpublic Personal Information over the telephone or in response to an e-mail unless the employee has identified the person to whom they are communicating and confirmed that sharing the Nonpublic Personal Information is allowed under one of the privacy exceptions under The Gramm-Leach-Bliley Act ("GLBA"), as described below. Employees should take reasonable precautions to confirm the identity of individuals requesting Nonpublic Personal Information. Employees must be careful to avoid disclosures to identity thieves, who may use certain Nonpublic Personal Information, such as a social security number, to convince an employee to divulge additional information. Any contact with suspected identity thieves must be reported promptly to the CCO.

To the extent practicable, employees will seek to remove nonessential Nonpublic Personal Information from information disclosed to third parties. Social security numbers must never be included in widely distributed lists or reports.

B. Disclosure of Information to Nonaffiliated Third Parties – "Do Not Share" Policy

CCP has a "do not share" policy. CCP does not disclose any Nonpublic Personal Information to nonaffiliated third parties, except under one of the GLBA privacy exceptions, as described below, or as authorized by a client.

1. Types of Permitted Disclosures – The Exceptions

In certain circumstances, Regulation S-P permits registered investment advisers to share Nonpublic Personal Information about its clients with nonaffiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a nonaffiliate (i) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (ii) in connection with processing or servicing a financial product or a service that a client authorizes; and (iii) in connection with maintaining or servicing a client account with CCP.

a. Service Providers

From time to time, CCP may have relationships with nonaffiliated third parties (such as attorneys, auditors, accountants, brokers, custodians, information technology support and other consultants), who in the ordinary course of providing their services to CCP may require access to information containing Nonpublic Personal Information of CCP's clients. These third-party service providers are necessary for CCP to provide its investment advisory services.

CCP will periodically determine whether its service providers have adopted policies and procedures regarding the protection Nonpublic Personal Information as required by applicable laws and regulations. When CCP is not comfortable that service providers are already bound by duties of confidentiality (e.g., as attorneys, auditors, and other financial institutions, are), it will require contractual assurances from those service providers that they will maintain the confidentiality of Nonpublic Personal Information they obtain from or through CCP.

Prior to providing any third-party service provider with access to personal information about individuals who are residents of Massachusetts, CCP will take reasonable steps to verify that such service provider has a written, comprehensive information security program reasonably designed to comply with the provisions of the Massachusetts data security regulation (201 CMR §§17.01-05) ("Massachusetts Regulation"). The CCO will ensure that any new contracts with such service providers include provisions requiring the service provider's implementation of security policies and procedures that reasonably comply with the Massachusetts Regulation.

b. Processing and Servicing Transactions

CCP may also share information when it is necessary to effect, administer, or enforce a transaction requested or authorized by a client. In this context, "necessary to effect, administer, or enforce a transaction" includes what is required or is a usual, appropriate, or acceptable method:

i. to carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the client's account in the ordinary course of providing the financial service or financial product;
ii. to administer or service benefits or claims relating to the transaction or the product or service of which it is a part;
iii. to provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent or broker.

c. Sharing as Permitted or Required by Law

CCP may disclose information to nonaffiliated third parties as required or allowed by law. For example, this may include disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, an audit or examination, or the sale of an account to another financial institution.

2. Client Authorization

Clients may provide CCP with instructions to share their information with third parties. This authorization may be provided in writing, by e-mail, or orally (in person or by telephone). The Portfolio Administrator will update CCP's internal client profile record with the names of the authorized third parties.

3. Provision of Opt Out

As discussed above, CCP currently operates under a "do not share" policy; and, therefore, does not need to provide the right for its clients to opt out of sharing with nonaffiliated third parties, as long as such entities are exempted as described above. If CCP's information sharing practices change in the future, the CCO will implement opt out[1] policies and procedures and CCP will make appropriate disclosures to its clients.

[1] Model forms related to affiliate marketing are provided in Reg. S-AM. Model forms related to the use of Nonpublic Personal Information are provided in Reg. S-P.

C. Disclosure of Information to and from Affiliates

CCP does not currently share information covered by Regulation S-AM about consumers ("eligibility information") with any affiliates. In the event that CCP begins to share eligibility information with an affiliate and such affiliate intends to use the information to make marketing solicitations, the following procedures will apply.

1. Information Obtained from Affiliates

Prior to using any information about an individual obtained from an affiliated entity for marketing purposes, an employee must notify the CCO. The CCO shall be responsible for ensuring that the affected individuals have received clear and conspicuous notice of the information sharing arrangement and an opportunity to opt out[1], and that the affected individuals have not opted out.

2. Information Provided to Affiliates

Prior to providing information about individuals to affiliates for marketing purposes, an employee must notify the CCO. The CCO shall be responsible for ensuring that the affected individuals have received clear and conspicuous notice of the information sharing arrangement and an opportunity to opt out[1], and that the affected individuals have not opted out.

V. Privacy Notice

CCP has developed a Privacy Notice, as required under Regulation S-P, to be delivered to Customers initially and to current Customers when amended. The Privacy Notice is attached as Exhibit A. The Privacy Notice discloses CCP's information collection and sharing practices and other required information. The Privacy Notice will be revised as necessary any time information practices change.

A. Privacy Notice Delivery

1. Initial Privacy Notice

As required by applicable regulations, CCP will deliver an initial Privacy Notice to all new Customers at the time the Customer relationship is established (i.e., upon execution of the agreement for services).

2. Annual Privacy Notice

On December 4, 2015, President Obama signed the Fixing America's Surface Transportation Act, or "FAST Act", into law. The FAST Act, in part, amended the GLBA to remove a financial institution's obligation to provide an annual privacy policy notice when certain conditions are met[2]. Pursuant to this amendment, CCP would be required to provide an

[2] The SEC has not yet updated Regulation S-P to account for the amendment. Nonetheless, the amendment was effective immediately.

annual notice only if it changes its privacy policies to disclose Nonpublic Personal Information to nonaffiliated third parties in a manner that triggers an opt-out right (e.g., marketing purposes).

3. Revised Privacy Notice

Regulation S-P requires that CCP amend these Privacy Policies and Procedures and promptly distribute a revised disclosure to Customers if there is a change in CCP's collection, sharing, or security practices.

4. Joint Relationships

If two or more individuals jointly obtain a financial product or service from CCP, CCP may satisfy the initial, annual, and revised notice requirements by providing one notice to those individuals jointly.

VI. State Requirements for Protecting their Residents

A. California

The California Financial Information Privacy Act, generally referred to as "S.B. 1," is found at California Financial Code §§4050, et seq. S.B. 1 protects the privacy of Nonpublic Personal Information to a greater extent than GLBA. S.B.1 generally provides that (i) financial institutions that wish to share Nonpublic Personal Information with nonaffiliated third parties must obtain affirmative consent ("opt-in") to do so, and (ii) financial institutions that wish to share Nonpublic Personal Information with affiliated parties must permit customers to opt out of such sharing. S.B. 1 establishes specific content and form requirements for such opt-ins, but it also contains numerous exceptions, exemptions, and carve-outs applicable to specific fact patterns under which Nonpublic Personal Information may be shared by financial institutions.

B. Massachusetts

The Massachusetts Regulation contains the most stringent and detailed data security requirements for organizations by a state to date. Massachusetts is the first and only state to require covered organizations to adopt a comprehensive written information security program ("WISP") incorporating specific security measures. Effective since March 1, 2010, the Massachusetts Regulation has extensive reach, purporting to cover every organization, wherever located, that owns or licenses personal information of Massachusetts residents. The Massachusetts Regulation specifically applies to the following information associated with a Massachusetts resident: (i) last name and either first name or first initial; plus (ii) a social security number, state-issued identification number (such as a driver's license number) or a financial account number (including but not limited to a credit or debit card number). The Massachusetts Regulation does not apply to information that is lawfully obtained from public records, or to information that is not kept in connection with business activities or employment.

VII. Responding to Improper Disclosures

If any employee becomes aware of an actual or suspected improper disclosure of Nonpublic Personal Information, that employee must promptly notify the CCO. Upon becoming aware of an actual or suspected improper disclosure of Nonpublic Personal Information, the CCO will investigate the situation and take the following actions, as the CCO deems appropriate:

1. To the extent possible, identify the Nonpublic Personal Information that was disclosed and the improper recipients.

2. Take any actions necessary to prevent further improper disclosures.

3. Take any actions necessary to reduce the potential harm from improper disclosures that have already occurred.

4. With reference to CCP's Identity Theft Prevention Program, evaluate the need to notify affected clients.

5. Consider discussing the issue with outside counsel, and with reference to CCP's Identity Theft Prevention Program, consider discussing the issue with regulatory authorities and/or law enforcement officials.

6. Collect, prepare, and retain documentation associated with the improper disclosure and CCP's response(s).

7. Evaluate the need for changes to CCP's Privacy Policies and Procedures in light of the improper disclosure.

VIII. Privacy Protection Training

The CCO will ensure that all new employees who will have access to Nonpublic Personal Information are trained regarding their responsibility to protect Nonpublic Personal Information. The CCO will also periodically remind all employees of their obligations to protect Nonpublic Personal Information, as the CCO deems necessary.

IX. Records

The following records shall be maintained in accordance with CCP's Books and Records Policy:

1. Copies of Privacy Notices to Customers.

2. Evidence of client instructions to share their Nonpublic Personal Information with third parties.

3. Employee confidentiality agreements, if applicable.

4. Service provider contracts with confidentiality provisions or separate confidentiality agreements, if any.

5. Evidence of training sessions with copies of materials and attendee sign-in sheet.

Adopted: February 7, 2017
Amended: June 1, 2019

Exhibit A

PRIVACY NOTICE

This notice describes how Clarkston Capital Partners, LLC ("CCP") collects, shares and protects nonpublic personal information that you provide to us and that we obtain in connection with providing our products and services to you. Please read this notice carefully to understand what we do.

CCP limits the collection, use and retention of nonpublic personal information to what we believe is necessary or useful to conduct our business and to provide and offer you quality products and services, as well as other opportunities that may be of interest to you. Information collected may include, but is not limited to, name, address, telephone number, tax identification number, date of birth, employment status, annual income, and net worth.

In providing products and services to you, we collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms (e.g. investment/insurance applications, new account forms, and other forms and agreements);
- Information about your transactions with us, our affiliates or others (e.g. broker/dealers, clearing firms, or other chosen investment sponsors).

CCP limits its sharing of specific information about your account(s) and other personally identifiable data. As a rule, we do not disclose nonpublic personal information we collect to others. However, because we rely on certain third parties for services that enable us to provide our advisory services to you, such as our attorneys, auditors, other consultants, brokers, and custodians who, in the ordinary course of providing their services to us, may require access to information, we may share nonpublic personal information with such third parties. Additionally, we will share such information where required by legal or judicial process, such as a court order, or otherwise to the extent permitted under the federal privacy laws.

We may also disclose your nonpublic personal information to others upon your instructions. You may provide instructions below by listing the persons with whom you give us permission to share your nonpublic personal information. You may amend this list, and/or rescind your permission at any time in writing. Your signature below indicates your understanding and acceptance that we may share your nonpublic personal information.

We restrict access to nonpublic personal information about you to those persons associated with CCP who need access to such information in order to provide our products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

If you decide to close your account(s) or are no longer CCP's customer, we will continue to share your information as described in this notice.

CCP reserves the right to change its privacy policies, and any of the policies or procedures described above, at any time without prior notice. However, we will promptly provide you with a current copy of our privacy notice upon material changes or upon request. So long as you remain an active customer of CCP, you will receive a current copy of our privacy notice at least annually. This Privacy Notice is for general guidance and does not constitute a contract or create legal rights, and does not modify or amend any agreements we have with you.

If you have questions about this Privacy Notice, or if you wish to amend or rescind your written instructions below at any time, please contact [CLIENT SERVICE CONTACT] by phone at -[CLIENT SERVICE CONTACT PHONE NUMBER] or by e-mail at [CLIENT SERVICE CONTACT EMAIL ADDRESS].

Please list below any service provider (Attorney, CPA, etc.) for which you give CCP permission to discuss your nonpublic personal information. Do not return this form to CCP if you do not wish to name a designated authorized person at this time.

Name	Relationship	Mailing Address	Phone No.	Email Address

Client Signature _____ Print Name _____ Date _____

Client Signature _____ Print Name _____ Date _____
(if Joint Tenant)

Revised 06.01.19