TRICADIA CAPITAL MANAGEMENT, LLC

PRIVACY PROTECTION, CYBER SECURITY AND IDENTITY THEFT PREVENTION

Most Recently Revised: May 2018

Background

Privacy Protection

Regulation S-P ("Reg S-P" or the "SEC Privacy Rule") requires registered investment advisers to adopt and implement policies and procedures that are reasonably designed to protect the confidentiality of nonpublic personal records. Reg S-P applies to "consumer" records, meaning records regarding individuals, families, or households. Reg S-P does not explicitly apply to the records of companies, investors in a private fund, or individuals acting in a business capacity, but corresponding Federal Trade Commission ("FTC") rules may impose similar disclosure and safeguarding obligations. Tricadia is committed to protecting the confidentiality of all non-public information regarding its Clients, Investors, prospects, and Supervised Persons ("Nonpublic Personal Information").

Reg S-P requires Tricadia to provide its customers with notices describing Tricadia's privacy policies and procedures. These privacy notices must be delivered to all new Clients upon inception of a relationship, and at least annually thereafter. Reg S-P does not require the distribution of privacy notices to companies, to investors in a private fund, or to individuals acting in a business capacity, but Tricadia provides initial and annual privacy notices to all Clients and Investors as a best practice.

Information Sharing with Affiliates

Regulation S-AM ("Reg S-AM") prohibits a registered investment adviser from using information about an individual consumer that has been obtained from an affiliated entity for marketing purposes unless the information sharing practices have been disclosed and the consumer has not opted out.

Cyber Security

The staff of the SEC is concerned by the risk of cyber-attacks against registered investment advisers because of the potential for direct harm against advisers' clients, as well as potential disruptions to market stability that could be intentional or incidental results of a cyber-attack.

Identity Theft Prevention

In addition to Reg S-P and Reg S-AM, the SEC has adopted Regulation S-ID, the "Red Flags Rules," that require certain companies to take steps to detect, prevent, and mitigate the effects of identity theft.

The Red Flags Rules require each SEC registered broker-dealer, investment company, and investment adviser that is a financial institution or creditor to periodically evaluate whether it offers or maintains any covered accounts.

Definition of "Financial Institution" and "Creditor"

The term "financial institution" is defined to include any "person that, directly or indirectly, holds a transaction account belonging to a consumer." A "transaction account" includes any account that allows the account holder to make withdrawals by negotiable or transferable instrument, payment orders, telephonic transfers or similar transactions for the purpose of making payments or transfers to third persons. A "consumer" is defined to include natural persons.

Examples of arrangements that could cause an investment adviser to be deemed a financial institution for purposes of the Red Flags Rules include:

- An adviser with the ability to direct transfers or payments from one or more natural persons' accounts to third parties, either unilaterally or upon the instructions of the natural person account owners ; and

- An adviser managing a private fund with one or more natural person investors that permit the adviser or a related person to direct the natural person's redemption proceeds to third parties.

The term "creditor" is defined to include, among other things, any person who extends or arranges credit. A person would not be deemed to be a creditor solely because it bills for services in arrears, or because it advances funds for expenses incidental to the provision of a service. The SEC has stated that an adviser to a private fund that regularly and in the ordinary course of business lends money to permit individual investors to invest in the fund could qualify as a creditor.

Periodic Assessments

The Red Flags Rules require each investment adviser that is a financial institution or creditor to periodically assess whether it offers or maintains any covered accounts. "Covered accounts" are defined to include:

- An account that is primarily for personal, family or household purposes that is designed to permit multiple payments or transactions; and

- Any other account for which there is a reasonably foreseeable risk from identity theft to natural person customers or to the safety and soundness of the adviser.

The assessment as to whether an adviser maintains any covered accounts must include evaluations of:

- The adviser's method for opening accounts;

- The ways in which clients and investors can access accounts; and

- The adviser's prior experiences with identity theft.

Creating a Written Identity Theft Prevention Program

Any financial institution or creditor that offers or maintains one or more covered accounts must:

- Develop and implement a written Identity Theft Prevention Program (a "Program") that is reasonably designed to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. In particular, the Program must be reasonably designed to:

    - Identify patterns, practices, or specific activities that could be indicative of identity theft ("Red Flags");

    - Detect the Red Flags that have been identified by the adviser as potentially applicable;

    - Respond appropriately to any Red Flags that are detected; and

    - Call for periodic updates to reflect any changes in the risks posed by identity theft to the firm or its customers;

- Obtain approval of the initial written Program from the firm's board of directors or an appropriate committee of the board. If the firm does not have a board of directors then approval may be obtained from a designated member of senior management;

- Involve the board, an appropriate committee of the board, or a designated member of senior management in the oversight, development, implementation and administration of the Program;

- Train Supervised Persons, as necessary, to effectively implement the Program; and

- Ensure that service providers performing activities in connection with one or more covered accounts have their own reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, and exercise appropriate oversight of those service providers.

The Red Flags Rules also require persons that issue a credit or debit card (card issuer) to establish and implement reasonable written policies and procedures to assess the validity of a change of address notification if within a short period of time after the notification, the card issuer receives a request for an additional or replacement card for that account.

As part of the final rule release, the SEC and CFTC issued Program guidelines to assist financial institutions and creditors in the creation and maintenance of a Program meeting the requirements of the Red Flags Rules. These guidelines are described below:

- Consider the following factors when identifying relevant Red Flags:

    - The types of covered accounts it offers or maintains;

    - The methods it provides to open covered accounts;

    - The methods it provides to access covered accounts; and

    - Any previous experiences with identity theft.

- Incorporate relevant Red Flags from the following categories, as applicable:

    - Alerts, notifications, or other warnings from consumer reporting agencies or service providers;

    - The presentation of suspicious documents;

    - The unusual use of, or suspicious activity related to, a covered account; and

    - Notice from customers, victims of identity theft, law enforcement authorities, or others regarding possible identity theft in connection with a covered account.

- Detect Red Flags by:

    - Obtaining identifying information and otherwise verifying the identity of a person opening a covered account; and

    - Authenticating existing customers, monitoring transactions, and verifying the validity of change of address requests.

- Provide for appropriate responses to any Red Flags that are detected. Appropriate responses may include, among other things;

- Carefully monitoring the affected account(s) for evidence of identity theft or other improper activity;
- Contacting the affected customer(s);
- Changing passwords, security codes, or other controls designed to prevent unauthorized access or activity;
- Reopening a covered account with a new account number;
- Not opening a new account, or closing an existing account;
- Notifying law enforcement; and/or
- Determining that an affirmative response is not necessary in light of the relevant facts and circumstances.

- Reevaluate the Program and the risks associated with identity theft at least annually. Such an evaluation should be reflected in a written report that incorporates, as applicable.
  - The firm's experiences with identity theft;
  - Changes in methods of identity theft;
  - Changes in available methods to detect, prevent, and mitigate identity theft;
  - Changes in the types of accounts that the firm offers or maintains; and
  - Changes in the firm's relationships with other entities, such as third-party service providers;
- Oversight by the firm's board of directors, a committee of the board, or a designated member of senior management that includes:
  - Assigning specific responsibility for the Program's implementation;
  - Reviewing reports prepared by Supervised Persons regarding compliance with the Program; and
  - Approving material changes to the Program as necessary to address changing identity theft risks
- Report to the firm's board of directors, a committee of the board, or a designated member of senior management at least annually on the compliance by the firm with the Red Flags Rules. The report should address material matters related to the Program and evaluate issues such as:
  - Effectiveness of the firm's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Service provider arrangements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the Program.

State Privacy Requirements

In addition to Reg S-P, Reg S-AM and Reg S-ID, certain states have adopted consumer privacy laws that may be applicable to investment advisers with clients or investors who are residents of those states. For example, Massachusetts law 201 CMR 17 requires any company with certain information about a resident of Massachusetts[1] to adopt and implement a comprehensive information security program that includes, among other things:

- Developing security policies governing how Supervised Persons should be allowed to keep, access and transport records containing personal information outside of business premises;
- The selection of third-party service providers that are capable of maintaining appropriate security measures to protect personal information, and the inclusion of contractual provisions requiring the implementation of such measures;
- Prior to permitting third-party service providers access to personal information, the person permitting such access shall take reasonable steps to verify that such service provider can comply with the Massachusetts regulations;
- To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across the internet or other public networks, and encryption of all data to be transmitted wirelessly;
- To the extent technically feasible, encryption of all personal information stored on laptops or other portable devices; and
- Education and training of Supervised Persons on the proper use of the computer security system and the importance of personal information security.

The General Data Protection Regulation ("GDPR")

The European General Data Protection Regulation ("GDPR") extends the scope of EU data protection law to all foreign companies such as Tricadia, which may process personal data of any EU individual. Please note that this regulation applies to personally identifiable data or other information ("PII") that is held in relation to an EU natural person (e.g., an individual versus a corporation or other company). Personal information includes but is not limited to an individual's name, email address, telephone number and any other information that can be used to identify that person. This EU regulation requires that a company have a lawful basis or legitimate business reason for the "processing" of a person's personal data (e.g., storing or otherwise possessing in a Firm's records or systems PII such. Without such a lawful basis, the data must not be stored or otherwise retained in a company's records and must be deleted (e.g., if inadvertently temporarily added). As a general statement, all personal information, as defined by GDPR that is in Tricadia's possession is and will only be stored for "legitimate business purposes". Attachment B contains Tricadia's Privacy and Marketing Policy that is applicable with respect to Tricadia's receipt, processing and storage of PII of EU natural persons.

Risks

In developing these policies and procedures, Tricadia considered the material risks associated with privacy protection and the prevention of identity theft. This analysis included risks such as:

---

[1] Massachusetts law 201 CMR 17 specifically applies to the following information associated with a Massachusetts resident:

- Last name and either first name or first initial; plus
- 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).

Massachusetts law 201 CMR 17 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.

- Nonpublic Personal Information is not recorded accurately or protected from inadvertent alteration or destruction;
- Nonpublic Personal Information is not protected from unauthorized access by Supervised Persons or third-party service providers;
- Nonpublic Personal Information can be accessed, copied, or destroyed by physical or electronic intrusions;
- False or misleading disclosures are made to Clients or Investors about the use or protection of Nonpublic Personal Information;
- Third-party service providers have adopted inadequate policies and procedures to protect Nonpublic Personal Information;
- Tricadia fails to comply with applicable state privacy laws;
- Tricadia fails to comply with GDPR;
- Tricadia uses information obtained from affiliates for marketing purposes without ensuring that affected individuals have been given adequate notice and an opportunity to opt out;
- Tricadia does not identify potential risks to Clients or Investors associated with identity theft; and
- Tricadia does not detect fraudulent attempts to transfer assets out of Client or Investor accounts enabled by identity theft.

Tricadia has established the following guidelines to mitigate these risks.

Policies and Procedures

Categories of Information

The SEC Privacy Rule defines four basic categories of information:

1. Publicly available information – any information that the firm believes is lawfully made available to the general public from three types of sources: information from official government records; information from widely distributed media, such as telephone books or newspapers; and information that is disclosed to the general public as required by law, such as securities disclosure documents.

2. Personally identifiable financial information (e.g., CFTC Regulation 160) – any information the firm collects about a consumer (prospective client) in conjunction with providing a financial product or service. This includes information provided by the consumer during the application process when entering into an investment advisory contract, or obtaining a financial plan (e.g., name, phone number, address).

3. Nonpublic personal information (this category of information is protected by the SEC Privacy Rule) – any *personally identifiable financial information (e.g., CFTC Regulation 160),* and any list or description or groupings of consumers created from such information.

4. Consumer Report Information (this category of information is protected by the SEC Privacy Rule). – any record about an individual, whether paper, electronic or other form that is a consumer report or is derived from a consumer report. Consumer report also means any compilation of such records.

Tricadia does <u>not</u> disclose or share any nonpublic personal client information with anyone, except as required by law.

Tricadia uses unaffiliated third-party service providers for purposes of supporting its advisory services provided to Tricadia Clients. Tricadia provides these third parties with only the information necessary to carry out their assigned responsibilities and only for that purpose. To the extent that unaffiliated third-party service providers have access to "customer" information as defined under the SEC Privacy Rule, these parties must agree to comply with stringent security and privacy policies and procedures.

Regulation S-P requires that contractual agreements between an investment adviser and nonaffiliated third party service provider include terms to ensure that the third party will maintain the confidentiality of any nonpublic personal client information it may receive concerning the adviser's consumers or customers. Tricadia will ensure that all service agreements that contain Non-public personal "customer" information as defined under the SEC Privacy Rule, contain adequate confidentiality contractual provisions ("Applicable Service Agreements"). In addition, for all Applicable Service Agreements Tricadia will request a copy of the service providers' privacy policies and procedures (or other similar policies), and will provide a copy of Tricadia privacy policies and procedures to these entities and obtain written certification that they have read, understand and agree to adhere to Tricadia's privacy policies and procedures.

<u>Customer Relationships</u>

The SEC takes the position that if an investment adviser is required to deliver a brochure under the "Brochure Rule," then a customer relationship exists, even in the absence of a written advisory agreement. The SEC Privacy Rule does not apply to ***institutional or corporate*** Clients. Under the regulation, a consumer or a customer must be an individual. Therefore, a Client that is not an individual (such as a pension plan, trust, corporation or limited partnership) is neither a consumer nor a customer of the adviser under the SEC Privacy Rule.

<u>Privacy Notices</u>

Tricadia is required to provide to customers ***initial and annual privacy notices*** even though it does not share consumer information with anyone. For a <u>customer</u>, Tricadia will provide an initial privacy notice <u>no later than</u> the time of establishing the customer relationship.[2] The notice will be described within Tricadia's disclosure brochure (i.e., Form ADV Part 2A) and in other disclosure documents (e.g., Private Fund offering documents). In addition, Tricadia will provide an annual privacy notice to customers during the continuation of the customer relationship. More specifically, Tricadia will deliver the <u>annual</u> privacy notice, along with customer portfolio holdings statements or other customer notifications, once in every period of 12 consecutive months during which a customer relationship exists. Under the SEC Privacy Rule, notices must be provided in writing or, if the customer agrees, in electronic form. Initially, Tricadia will provide privacy notices to all customers in written form.

<u>Privacy Protection Standards</u>

The SEC Privacy Rule requires the adoption of policies and procedures that are reasonably designed to ensure the ***security*** and ***confidentiality*** of customer information. In addition, these policies and procedures must be designed to prevent unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. To ensure that the systems that process and store information are operated and maintained in a secure and recoverable environment, safe from misuse, theft and foreseeable catastrophes, Tricadia has adopted the following policy and procedures:[3]

Administrative Safeguards (Managers / Supervised Persons)

[2] See Attachment A for a copy of Tricadia's standard privacy notice.

[3] Please also see Mariner's Cybersecurity Policy and Standards Manual, utilized by Mariner and BOSG in providing IT and other services to Tricadia, maintained under separate cover, and related policies and procedures that further describe the control measures Tricadia has employed in this area.

a) Information owned by Tricadia must be treated with the same care as any other firm asset. All Supervised Persons are responsible for the protection of information.
b) All Supervised Persons must understand and adhere to the firm's Privacy Protection, Cyber Security and Identity Theft Prevention Policy (the "Privacy Policy"). Tricadia's Legal/Compliance Department will periodically train Supervised Persons in this area as part of its general training program. At the time of hire, however, all new Supervised Persons, including temps, must review the Privacy Policy, acknowledge their understanding and certify that they will comply with its requirements. See Attachment C.
c) Supervised Persons must safeguard information in their possession to prevent access by unauthorized individuals (e.g., conceal confidential client information). Departing Supervised Persons must not take with them or disclose nonpublic customer information.
d) Management must protect nonpublic personal "customer" information used in their area, and ensure that all Supervised Persons under their supervision understand and follow the firm's Privacy Policy.
e) Management must limit access to client information to those Supervised Persons that need access to the information to provide services to the client or conduct firm operations.
f) To prevent unauthorized disclosure, Supervised Persons should not give personal information out over the telephone or in response to an e-mail unless they have identified the person to whom they are communicating as either the client, a fiduciary representative of the client, or a party that needs information to complete a transaction for the client, (*e.g.*, broker-dealers and custodians).
g) Supervised Persons must report any attempted violations of security controls to the GC or CCO.
h) As laws come out that may impact our business (e.g., Identity Theft Red Flag Rules), Tricadia has controls in place to monitor where proceeds may be sent as part of a distribution (e.g., distribution to a client account versus a distribution to an individual).

Physical Safeguards

a) Client information should not be left in offices or conference rooms unattended.
b) Make sure all client records are appropriately secured at the end of the day.
c) Visitors should not be permitted to walk unattended in areas where client information is accessible.
d) Destroy or shred documents containing client information prior to disposal.
e) The building has established a security station on the ground floor, where all building Supervised Persons are required to present passes and visitors are required to show identification and sign in for the tenant being visited.
f) Regularly test any physical safeguards to confirm they are operating properly.
g) Protect against destruction of customer information due to potential physical hazards, such as fire and water damage (i.e., smoke and water detectors).

Technical Safeguards (Application & Data Security)

a) All computer systems must limit access to authorized users.
b) Access to client information must be restricted to those Supervised Persons who need access to the information to service the client or conduct firm operations.
c) Computer systems must be protected with individual user identifiers, each with a required password. Passwords must be kept confidential and secure.
d) PCs with access to client information should not be left unattended for extended periods of time.
e) Access privileges previously granted to those who are terminated or whose responsibilities change must be promptly revoked.
f) All emails or facsimiles sent that contain *Nonpublic personal "customer" information* should be accompanied with the following disclaimer: "This communication is for information purposes only and should not be regarded as an offer, solicitation or recommendation to sell or purchase any security or other financial product. The information and any opinions contained herein are as of the date of this message and the firm does not undertake any obligation to update them. Past performance is not indicative of future results, and no representation or warranty, express or implied, is made regarding future performance. All information contained in this communication is not warranted as to completeness or accuracy and is subject to change without notice. This email should be considered confidential and may not be reproduced in whole or in part, and may not be circulated

or redelivered to any person without the prior written consent of the firm. If you are not the intended recipient of this message you must not disseminate, distribute, copy or take any action in reliance on this e-mail or any attachment. Please see the following http://www.marinercapital.com/disclaimer/mariner.html for important disclosures that are incorporated by reference"

g) All computers should be protected with approved anti-virus software or hardware. Virus activity must be monitored on an ongoing basis, and threats dealt with appropriately.
h) Computer hardware should be installed in areas with restricted and physically secured access. .
i) All business critical systems and applications must be backed up each night.

Protection of Consumer Report Information

In addition to the above, Tricadia must take reasonable steps and measure to properly dispose of consumer report information. An adviser that obtains a consumer report for business purposes will be considered to be in possession of consumer report information. Consumer report information is defined to mean any record about an individual, whether paper, electronic or other form that is a consumer report. Consumer report information also means a compilation of such records. Accordingly, any information from a consumer report derived on an individual from a background check or due diligence service provider (Experian, Equifax, LexisNexis, etc.) that identifies an individual, including a person's name, social security number, telephone number, physical address and email address, would be covered by this SEC Privacy Rule. Supervised Persons must be especially cognizant of consumer report information when they dispose of company records that could contain covered information (See Tricadia's Records Maintenance and Retention Policy). For example, as a large manager and holder of customer information, the investment relations department must be particularly sensitive to this issue. **Any Supervised Person responsible for destroying company records must specifically look to see if any information scheduled for destruction includes Consu*mer Report Information and if it does, those relevant documents must be properly destroyed (e.g., shredded).***

Revision of Privacy Protection Standards

In the event of a recognized compromise of any of Tricadia's security systems (under its control), Tricadia will update its policies and procedures appropriately to reflect changes made to Tricadia's infrastructure as a result of that compromise.

Sharing Data with Law Enforcement Agencies

As a result of the September 11 terrorist attacks on America, Congress and Washington's law enforcement and regulatory agencies requested from financial institutions all financial data that could lead investigators to individuals financing terrorism. In the event that any law enforcement, government or regulatory agency should request (hereinafter referred to as "Official Request") customer personal/financial information from Tricadia for investigative purposes, Tricadia will fully comply with such Official Requests and will provide the information under the following guidelines:

a) The GC or CCO should be immediately notified of any Official Requests for customer personal information;
b) Tricadia will fully cooperate with law enforcement agencies and their investigative government authorities in terms of sharing customer information. The GC or CCO must first verify that such authorities are employed with the government agency, and/or be provided with a signed judicial subpoena or compliance certificate from the law enforcement agency; and
c) Tricadia will only provide the specific information requested, and not provide any additional or unsolicited information.

Regulation S-ID

The Fund Administrator and Tricadia's Investor Relations Department oversee the subscription and redemption processes on behalf of Tricadia. The Fund Administrator will not undertake the following without the specific approval of Tricadia'.

- Direct any redemption proceeds to an account not listed in the original subscription document;

- Change wire instructions;
- Partition, retitle, or otherwise change any indicia of ownership of an investment or account (including changes purportedly for estate planning and domestic relations reasons); or
- Consent to liens or control agreements being placed on an investment or account.

On an annual basis, Tricadia will take steps to ensure that the activities of Mariner, BOSG and the Fund Administrator are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Tricadia will inquire about any issues pertaining to a Client's or Investor's identity theft and assess whether enhancements are required to Mariner's, BOSG's and/or the Fund's policies and procedures are necessary. The CCO is responsible for overseeing and documenting such review.

Attachment A

FACTS

WHAT DOES TRICADIA DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service we provide to you. This information can include: ■ Social Security number and assets; ■ Account balances and transaction history; and ■ Investment experience and wire transfer instructions.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Tricadia chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Tricadia share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	No
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	No	We don't share
For our affiliates to market to you	Yes	Yes
For non-affiliates to market to you	No	We don't share

To limit our sharing:	■ Call (646) 388-5900 **Please note:** If you are a *new* customer, we can begin sharing your information 30 days from the date we sent this notice. When you are *no longer* our customer, we may continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call (646) 388-5900

Page 2

Who we are	
Who is providing this notice?	Tricadia Capital Management, LLC, on behalf of Tricadia Credit Strategies, L.P., Tricadia Credit Strategies II, L.P. and Tricadia Credit Strategies, Ltd., Structured Credit Opportunities Fund II, L.P., TNH Financials Fund, L.P, Tricadia Select Financials Fund, L.P., Tricadia Select Financials Fund, Ltd., Tricadia Convexity Fund, L.P. and Tricadia Convexity Fund, Ltd.

What we do	
How does Tricadia protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Tricadia collect my personal information?	We collect your personal information, for example, when you: ■ Give us your contact information; ■ Open an account or buy securities from us; and ■ Tell us where to send the money or make a wire transfer. We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only: ■ sharing for affiliates' everyday business purposes – information about your creditworthiness; ■ affiliates from using your information to market to you; and ■ sharing for non-affiliates to market to you. State laws and individual companies may give you additional rights to limit sharing.
What happens when I limit sharing for an account I hold jointly with someone else?	Your choices will apply to everyone on your account.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *Our affiliates and associated parties include companies with a "Tricadia," "Mariner," "Tiptree," "Telos" or "Back Office Services Group" name.*
Non-affiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *Tricadia does not share with non-affiliates so they can market to you.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *Tricadia does not engage in joint marketing.*

Attachment B

TRICADIA CAPITAL MANAGEMENT, LLC
TRICADIA EUROPE LLP
(collectively with their affiliates, the "Firm")

Privacy & Marketing Policy – UK and EU

Last updated 24 May 2018

PRIVACY & MARKETING POLICY – UK and EU

Purpose

This policy is to ensure that the Firm's marketing activities are compliant with applicable data protection laws ('**DP Laws**').

Scope

This policy applies to all marketing by the Firm's officers and employees and, as appropriate, those operating on its behalf. This policy is drafted for compliance with UK and EU laws, namely the GDPR and UK PECR's implementation of the e-Privacy Directive. It does not cover US federal or state laws. If any marketing activity is to target customers outside the EEA, further advice must be sought.

Interpretation

In this policy, we use definitions from the GDPR unless otherwise stated.

'**Anonymised data**' means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

'**DPIA**' means the PIA that must be carried out in certain situations, contain certain information, and over which there are other obligations, as set out in the GDPR.

'**EEA**' or '**European Economic Area**' means the EU and Iceland, Lichtenstein and Norway.

'e-Privacy Directive' means the EU Directive on privacy and electronic communications (Directive 2002/58/EC).

'**GDPR**' means the EU General Data Protection Regulation, 2016/679 which has effect as from 25 May 2018. As a regulation, the GDPR will take effect throughout the EU without the need for further implementation by Member States such as the UK.

'**Personal Data**' means any information relating to an identified or identifiable natural person, namely one who can be identified, directly or indirectly from that information alone or in conjunction with other information 'in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'[4]. While '**personal data**' is a defined term in EU law, we use it here to also cover '**personally identifiable information**' as defined in US law, and other similar legal definitions.

'**PIA**' means a privacy impact assessment, which is a written assessment of the risks to the rights and freedoms of data subjects through any processing of their personal data. A DPIA is a sub-set of PIAs.

'**Processing**' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

[4] Examples of personal data are from the EU General Data Protection Regulation ('GDPR').

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

'**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'**Pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. '**Pseudonymised data**' means personal data that has been pseudonymised.

'**Special Categories of Personal Data**' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'Transfers' means the transfer of personal data either to '**third countries**' meaning countries outside the EU or '**international organisations**' meaning an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

'**UK PECR**' means the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended.

The Policy

All marketing activities by or on behalf of the Firm must comply with applicable DP Laws (and other applicable laws).

Privacy by Design, Privacy by Default

Marketing activities must incorporate privacy by design and privacy by default principles – including the principles of data minimization, accuracy, storage limitation and integrity and confidentiality. In particular, PIAs (including DPIAs) must be carried out regarding proposed marketing activities as appropriate and in accordance with our PIA & DPIA Policy and related procedure.

Data Subject Rights

The Firm's Data Subject Rights Policy and related procedure sets out how the Firm will respond when data subjects exercise their rights under the GDPR, including regarding marketing. The Data Protection Policy and the Consent Procedure set out how the Firm will comply with consent requirements.

Pseudonymisation & Anonymisation

Where appropriate, and the Firm recognises this will not be in all cases, we will give due consideration to pseudonymising or anonymising personal data used in marketing activities.

National and the Firm's Do Not Contact Registers

The UK's DP Laws establish national do-not-contact registers for telephone calls (the Telephone Preference Service ("TPS') and the Corporate Telephone Service ('CTPS')) and fax (the Fax Preference Service ('FPS')). If a person registers their phone number (including a work phone number) on the TPS, CTPS or FPS, it is illegal to phone or send a fax to that number. In addition, in order to comply with its obligations under DP Law, the Firm shall maintain a Do Not Contact register recording all marketing opt-outs, including by individuals at their business contact details.

Contact details used in marketing activities must be cleansed as required by applicable DP Laws against the relevant national preference services such as the UK's TPS, CTPS and FPS and the Firm's Do Not Contact register.

Automated calls & faxes

The Firm's policy is that we will not make automated marketing calls nor send marketing faxes.

Children

The Firm's policy is that we will not market to any person under the age of 18, nor will we process any personal data relating to a person under the age of 18 in the course of or in relation to our marketing activities.

Special Categories of Personal Data

The Firm's policy is that we will not process any Special Category of Personal Data in the course of or in relation to our marketing activities.

Personal Data related to Criminal Convictions and Offences

The Firm's policy is that we will not process any personal data related to criminal convictions and offences in the course of or in relation to our marketing activities.

Processors & Transfers

It is highly likely that a supplier of services to the Firm for our marketing activities will process personal data and therefore be a 'processor'. No supplier for marketing activities may be used unless they have passed the Processor (Vendor) due diligence set out in the Processor (Vendor) Policy and related procedure. Personal data should not be transferred outside of the EEA unless in accordance with our Personal Data Transfer Policy.

Approved Codes of Conduct & Certifications

The GDPR allows for approval of codes of conduct (Article 40) and certification mechanisms (Article 42). Adherence to an approved code or certification mechanism may be used as an element by which to demonstrate compliance with various requirements in the GDPR. If

necessary or appropriate, the Firm will review such codes and certification mechanisms for relevance and fit for our marketing operations.

Unsubscribe

Should you want to unsubscribe from any marketing communication or have the personal details that we hold for you, deleted, please contact unsubscribe@tricadiacapital.com. The Firm will process this within 24 hours.

Breach

If you become aware of a breach of this policy, you must report it promptly to Andrew Schinder, Chief Compliance Officer of Tricadia Capital Management, LLC, at dataprivacy@tricadiacapital.com.

Enforcement

All Firm employees bear responsibility for their own compliance with this policy. Breach of this policy is ground for disciplinary proceedings against an employee, which may result in disciplinary action including termination of employment. Breach of this policy by any non-employee such as a temporary worker, contractor or supplier may be a breach of their contract with the Firm and grounds for damages or termination.

Ownership

The Chief Compliance Officer of Tricadia Capital Management, LLC (assisted as necessary by other member's of Tricadia's Legal/Compliance Department, including the Chief Compliance Officer of Tricadia Europe LLP) is responsible for maintaining this policy, related training and awareness programs.

Attachment C

PRIVACY PROTECTION, CYBER SECURITY AND IDENTITY THEFT PREVENTION

ACKNOWLEDGMENT

I have read and understand Tricadia's Privacy Protection, Cyber Security and Identity Theft Prevention Policy (the "Privacy Policy"). I recognize that the Privacy Policy applies to me and I agree to comply in all respects with the requirements described therein. If I become aware of any inconsistencies between the stated requirements and the firm's practices, I will immediately inform my manager and the Legal/Compliance Department of such inconsistency. I understand that any material and willful or negligent violation of the Privacy Policy may result in serious disciplinary actions being brought against me, up to and including possible dismissal from Tricadia.

_____ _____

Name Title

_____ _____

Signature Date