



## Disclosure to Customers

**Privacy Statement** We collect non-public personal information about you from the following sources: Information from your application or other forms; information about your transactions with our affiliates, others; or us and information we may receive from consumer reporting agency. We do not disclose any nonpublic personal information about our customers or former customers to any one, except as permitted by law. We restrict access to your personal and account information to those employees and our affiliates who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safeguards to guard your non-public personal information.

**Business Continuity** During times of local or national emergencies, the office may be closed and every attempt to return to normal business operation will be made. Our Business Continuity Plan addresses varying degrees of business disruption. Telephone calls to the office's main telephone number will be forwarded to a remote location for handling. Our Business Continuity Plan is subject to modification and any updates are available upon request. If a customer would like to receive a copy of our plan please send a written request to Tourmaline Partners, LLC, 680 Washington Blvd., 10th Floor, Stamford, CT 06901.

**Customer Identification Program** Important Information About Procedures for Opening a New Account: To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also request a copy of your passport, motor vehicle operator's license or other government issued identifications.

**FINRA BrokerCheck** FINRA BrokerCheck, allows investors to learn about the professional background, business practices, and conduct of FINRA member firms or their brokers. The telephone number of FINRA BrokerCheck is 800-289-9999, the website address <http://www.finra.org>. An investor brochure is also available upon request.

**Complaints** Complaint's regarding your account may be directed to the Tourmaline Partners, LLC, , 680 Washington Blvd., 10th Floor, Stamford, CT 06901; Attention Compliance Department. The telephone number is 203-302-7300.

**SEC Rule 606** The Company shall, on request and free of charge, disclose the identity of the venue to which your orders were routed for execution in the six months prior to the request, whether the orders were directed orders or non-directed orders, and the time of the transactions, if any, that resulted from such orders. Additional information may be found at: [sec.gov/tm/faq-rule-606-regulation-nms](http://sec.gov/tm/faq-rule-606-regulation-nms) Tourmaline Partners, LLC is a member of FINRA and SIPC.

**Tourmaline Partners, LLC is exempt from the requirement to hold an Australian financial services license under the Corporations Act 2001 (Cth) in respect of financial services performed. Tourmaline Partners, LLC is regulated by the Securities and Exchange Commission under United States laws which differ from Australian laws.**

## PRIVACY POLICY

The Securities Exchange Commission's adoption of Regulation S-P, the "privacy rules" promulgated under Section 504 of the Gramm-Leach-Bliley Act, requires all broker-dealer firms to provide all of its customers and consumers a disclosure statement, outlining the firm's procedures and policies regarding the safeguarding of "non-public personal information" that is obtained during the normal course of business.

Tourmaline Partners, LLC understands your Privacy is important and the Company has always been committed to maintaining your confidentiality. This notice will help you understand what types of non-public personal information we may collect, how we use it and how we protect your privacy. We recognize that you expect your personal information to be handled in a professional, confidential manner and we have adopted the following policies to safeguard your privacy and to explain the circumstances, under which we may collect, maintain, and use any non-public personally identifiable information that you provide us.

We collect information about you to help us serve your financial needs, provide customer service, offer new products or services, and fulfill legal regulatory requirements. The type of information we collect may include:

- Information we receive from you on applications or other forms (for example, your name, address, social security number, assets, and income).
- Information about your transactions with us or others (for example, your account balance, payment history, or parties to transactions).
- Information that we receive from a consumer reporting agency such as your creditworthiness and credit history.

We do not share non-public personal information about you with unaffiliated third parties with whom we have no contractual business relationship for their independent use unless (1) you give us permission, (2) it is necessary to complete a transaction on your behalf, (3) it is necessary to protect you against fraud, comply with a subpoena or other court order or is otherwise required or permitted by law. We do not sell information about you to outside unaffiliated companies.

Furthermore, we restrict access to your personal and account information to those employees who need to know that information to provide products and services to you and maintain strict physical, electronic, and procedural safeguards to guard your nonpublic personal information.

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

We reserve the right to change these privacy policies at any time. You will receive

appropriate notice of changes to our Privacy Policy.

Questions concerning this Privacy Policy may be directed to us at 203-302-7300, or by e-mail at [jo@tourmalinellc.com](mailto:jo@tourmalinellc.com).

### **Reg S-P Amendments**

Amendments to Regulation S-P were adopted by the SEC on May 15, 2024, to broaden the scope of information covered by Regulation S-P's requirements and are effective August 2, 2024. The Firm has two years from June 3, 2024 (the date of the publication in the Federal Register) in which to comply with the amended rule. The rule also applies to funding portals, investment companies, Registered Investment Advisers, and transfer agents.

### **Books and Records**

The Firm will maintain its books and records in the following manner with respect to Regulation SP:

- policies and procedures required to be adopted and implemented until three years after the termination of the use of the policies and procedures
- written documentation of any detected unauthorized access to or use of customer information including the Firm's response to and recovery from unauthorized access to or use of customer information for three years from the date that the records were made
- written documentation of any investigation and determination made regarding whether notification is required including the basis for any determination made, any written documentation from the US Attorney General related to a delay in notice and a copy of any notice transmitted for three years from the date when the records were made
- written documentation of any contract or agreement entered into until three years after the termination of such contract or agreement.

### **Notice Requirements**

A clear and conspicuous notice to customers that accurately reflects the Firm's privacy policies and practices must be provided to customers not less than annually during the continuation of the customer relationship (at least once in any 12 consecutive month period during which the relationship exists, on a consistent basis).

The Firm would not be required to deliver an annual privacy notice under the following conditions:

- If it provides nonpublic personal information to nonaffiliated third parties only in

accordance with regard to CFR 248.13 (an exception to the opt-out requirements for service providers and joint marketing), 248.14 an exception for processing and servicing transactions at consumer's request) and 248.15 (other exceptions to notice and opt out requirements)

- If it has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer and in the most recent privacy notice.

If the Firm no longer meets the requirements for an exception (if applicable) to delivering the annual privacy notice the Firm must comply with the following requirements:

- If the Firm is required to provide a revised privacy notice, it must provide an annual privacy notice in accordance with the timing requirement, treating the revised privacy notice as an initial privacy notice.
- If the Firm is not required to provide a revised privacy notice, it must provide an annual privacy notice within 100 days of the change in its policies or practices that causes it not to meet the exemption.

If the Firm no longer meets the requirements for an exception (if applicable) and provide the annual notice to its customers, and it once again meets the requirements for an exception, it does not need to provide an additional annual notice to its customers until such time as it no longer meets the requirements for an exception.

## **Safeguarding Customer Information**

The Firm has a Cybersecurity Policy in place and a Privacy Policy in place, which in tandem are created to safeguard customer information, unauthorized access to customer information, safeguard the disposal of customer information. Our privacy policy ensures the security and confidentiality of customer information. Our Cybersecurity program has been implemented with the intention of protecting against any anticipated threats or hazards to the security and integrity of customer information and to protect against any unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

The Firm has developed and will implement the following procedures to protect customer information:

1. Information and documentation obtained by the Firm will be kept confidential and on a "need to know" basis. Access will only be given to individuals who are required to process account opening or to gain knowledge of the customer's profile for trading or investing purposes.
2. The Firm will protect its customers from threats or hazards to the integrity of

customer information by ensuring that it is following its Cybersecurity protocols, which are periodically reviewed and tested and through educating its employees about identifying potential threats and hazards to Senior Management. Any potential threats or hazards identified will be investigated and the results documented.

3. Senior Management of the Firm will be responsible for responding to any unauthorized access to or use of customer information that could possibly result in substantial harm or inconvenience to any customer. Any potential unauthorized access to customer information will be investigated and analyzed to determine how it occurred, who if anyone is responsible for the unauthorized access and then take the necessary steps to remedy the situation. The Firm will maintain documentation of the event(s) that occurred, the results of the investigation and the remedial steps taken to rectify the error.

### **Response to Unauthorized Access to or Use of Customer Information.**

The Firm will train its Associated Persons on ways to detect and respond to any unauthorized use of customer information. Associated Persons will be responsible for reporting any possible unauthorized use of customer information to Senior Management of the Firm at its earliest detection. The Firm will respond as follows:

1. Senior Management of the firm will assess the incident to determine if there was a breach of confidentiality and unauthorized access to customer information has occurred. The Firm will identify the systems through which the information has been accessed without authorization and work with the IT department (if the Firm has one) or with the outside third-party vendor, if appropriate, to fix the source of the breach. All events and their resolutions will be documented.
2. The Firm will put into effect any additional controls needed to prevent any further unauthorized access to our use of customer information including enhancement of its technology and additional education of its Associated Persons.
3. The Firm will notify each individual whose sensitive customer information was or is reasonably likely to have been accessed and used without prior authorization, unless the Firm determines after investigation of the incident, that sensitive customer information has not been and is not reasonably likely to have been used in a manner that results in substantial harm or inconvenience.
4. If it is determined that there has been a breach in sensitive customer information, the Firm is required to provide the customer with a clear and conspicuous notice or ensure that such notice is provided to each affected individual whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. The notice will be transmitted in writing to the customer by a means that will ensure that the customer will receive it.

5. In the case where the incident has revealed that unauthorized access has occurred or is reasonably likely to have occurred, but the Firm is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the Firm will provide notice to ALL individuals whose sensitive customer information resides in the customer information system that was (or reasonably likely to have been) accessed or used without authorization. If the Firm reasonably determines that a specific individual's sensitive customer information which resides in the customer information system was not accessed or used without authorization, then the Firm IS NOT required to provide notice to THAT individual under the rule.

## **Timing**

The Firm will provide notice to the customer as soon as possible, but not later than 30 days after becoming aware that unauthorized access to our use of customer information has occurred or reasonably likely to have occurred, unless the US Attorney General determines that the required notice poses a substantial risk to national security or public safety and may delay providing such notice for a time period specified by the AG, up to 30 days following the date when it was required to be provided. If the AG determines that the notice continues to pose a threat and notifies the SEC of such determination in writing, it may be delayed by an additional 30 days. Under extraordinary circumstances, the notice may be delayed for a final additional period of up to 60 days if the AG determines that such notice continues to pose a substantial risk to national security and notifies the SEC in writing. Beyond the final 60 day delay if the AG indicates that further delay is necessary, the SEC will consider the request and may possibly grant the delay.

## **Content of the Notice**

The following must be included in the notice:

- A description in general terms of the incident and the type of sensitive customer information that was or believed to have been accessed or used without authorization.
- If possible, provide the date of the incident, the estimated date of the incident or the date range within which the incident occurred
- Include contact information for the Firm through which the individual can inquire about the incident. These would include:
  1. A telephone number or toll-free number if available
  2. An email address or equivalent method or means
  3. A postal address
  4. Name of the specific office to contact for further information and assistance
  5. If the individual has an account with the Firm, recommend that the

- customer review their account statements and report immediately any suspicious activity to the Firm.
6. Explain what a fraud alert is and how the customer may place a fraud alert in their credit reports to alert them that the customer may be a victim of fraud, including identity theft.
  7. Recommend that the individual periodically obtain credit reports from each credit reporting company and delete the information related to the fraudulent transaction detailed
  8. Include information about the Federal Trade Commission's online guidance and [usa.gov](http://usa.gov) regarding steps to protect against identity theft, encourage the customer to report the incident of identity theft to the FTC's website to obtain information about identity theft and to report suspected incidents of identity theft.

## **Service Providers**

The Firm's CCO and Head of IT (if any) will be responsible for enforcing the Firm's policies and procedures and are responsible for the oversight (including due diligence and monitoring) of service providers, which includes ensuring that the Firm notifies affected individuals.

The Firm will ensure that its Service Providers will

1. Protect against unauthorized access to or use of customer information and;
2. Will provide notification to the Firm as soon as possible, but no later than 72 hours after becoming aware that a breach of security has occurred, which has resulted in unauthorized access to a customer information system maintained by the Service Provider.

The Firm will review its contract with its Service Providers to determine whether there is a clause requiring 72 hours' notice after a breach in security, or if not, to request that one be included.

If the Firm receives notification from its Service Providers that there has been a breach of security, the Firm must initiate its response program which is noted above. The Firm may enter into a written agreement with its Service Provider to notify the affected individuals on the Firm's behalf, although the Firm is still responsible for ensuring that the notification has been provided.

The Firm will ensure that customer information is properly disposed of and take reasonable steps to protect against unauthorized access to or use of the information in connection with its disposal.

The Firm will train its personnel on the protection of confidential customer information, including the use of encryption, password protection, not leaving personal customer information on paper in any public area, safeguarding customer information in locked cabinets and ensuring that any paper document with personal customer information on it, to be disposed of, is shredded. All computers with customer information displayed on them should be locked when Associated Persons are away from their desks.

Apart from its written policies and procedures that the Firm has adopted in response to the rule, it will maintain records for a time period of six years, the first two in an easily accessible place. The Firm's policies and procedures related to the disposal of customer information and the safeguarding of customer information must be maintained, or at any time within the past six years were in effect, must be maintained in an easily accessible place.

## **Business Continuity Planning**

Tourmaline Partners, LLC has developed a Business Continuity Plan which describes how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur. With that in mind, we are providing you with this information on our business continuity plan.

**Our Business Continuity Plan** We plan to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a financial and operational assessment, protecting the firm's books and records, and allowing our customers to transact business. In short, our business continuity plan is designed to permit our firm to resume operations as quickly as possible, given the scope and severity of the significant business disruption.

Our business continuity plan addresses: data back-up and recovery; all mission critical systems; financial and operational assessments; alternative communications with customers, employees, and regulators; alternate physical location of employees; critical supplier, contractor, bank and counter-party impact; regulatory reporting; and assuring our customers prompt access to their funds and securities if we are unable to continue our business.

Our clearing firm, Goldman, Sachs & Co. retains a back-up of many of our important records. While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the disruption, we have been advised by our clearing firm that their objective is to restore its own operations and be able to complete existing transactions and accept new transactions and payments within one business day. Your orders and requests for funds and securities could be delayed during this period.

**Varying Disruptions** Significant business disruptions can vary in their scope, such as only our firm, a single building housing our firm, the business district where our firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our firm or a building housing our firm, we will transfer our operations to a local site when needed and expect to recover and resume business within one business day. In a disruption affecting our business district, city, or region, we will transfer our operations to a site outside of the affected area, and recover and resume business within one business day. In either situation, we plan to continue in business, transfer operations to our clearing firm if necessary, and notify you through our web site ([www.tourmalinellc.com](http://www.tourmalinellc.com)). If the significant business disruption is so severe that it prevents us from remaining in business, we will assure our customer's prompt access to their records.

If you have questions about our business continuity planning, you can contact us at 203-302-7300.