CODE OF ETHICS POLICY

The successful operation and reputation of Seaboard Corporation and its consolidated subsidiaries (collectively, the "Company") depend upon the professional work performance and the ethical conduct of its directors, officers, and employees. The Company's reputation for integrity and excellence requires careful compliance with the spirit and letter of all laws and regulations, as well as a commitment to the highest standards of personal and professional conduct.

This organization was built by people with sound character and a long history of good and ethical commercial practices. There is an attitude of trust and respect between the Company and its customers, employees, business partners, suppliers, and shareholders. Continuing to earn that trust and protecting the Company's reputation is extremely important. Directors, officers, and employees have a duty to support the goals and objectives of the Company, and to act in a way that will always merit the continued confidence of those who have placed reliance on the Company.

Accordingly, the Company adopts the following Code of Ethics:

HONEST AND ETHICAL CONDUCT

The Company wants its directors, officers and employees to exhibit and promote the highest standards of honest and ethical conduct by:

- Encouraging and rewarding professional integrity thereby eliminating coercion, fear of reprisal, or alienation from the Company itself, which can act as barriers and inhibit responsible and ethical behavior.

- Avoiding, prohibiting and eliminating any conflict of interest or appearance of a conflict of interest between the Company and what could result in personal gain for a director, officer or employee of the Company, as defined in the attached Conflict of Interest policy.

- Supporting a process for employees of the Company to inform senior management of practices which deviate from honest and ethical behavior.

- Demonstrating their personal support for such policies and procedures.

- Acting in the best interests of the Company in order to preserve the Company's reputation as a professional company operating with integrity and good character.

When faced with an ethical dilemma, ask yourself…

- ✓ *Is it legal?*
- ✓ *Does it comply with this Code and other Company policies?*
- ✓ *Is it consistent with the Company's values?*
- ✓ *Have I done my due diligence?*
- ✓ *Is this action really in the Company's interest?*
- ✓ *How would the media react?*

FINANCIAL RECORDS AND PERIODIC REPORTS

Directors, officers and employees should, to the extent applicable within the scope of their job functions, ensure that:

- Business transactions are properly authorized and completely and accurately recorded on the Company's books and records in accordance with Generally Accepted Accounting Principles (GAAP) and established Company financial policy.

- The retention or proper disposal of Company records shall be in accordance with established Company policies and applicable legal and regulatory requirements.

- Reports and documents the Company files with, or submits to, the Securities and Exchange Commission, or other mandated public communications and disclosures, contain full, fair, accurate, timely and understandable information.

ANTI-COMPETITIVE CONDUCT

Directors, officers and employees should not enter into any agreement, understanding or arrangement with any competitor about prices, territory restrictions, refusals to sell, allocation of business, or collaborative bidding, or engage in any other type of anti-competitive practice in violation of applicable laws or regulations.

COMPLIANCE WITH APPLICABLE LAWS, RULES AND REGULATIONS

Directors, officers and employees should comply with applicable laws and regulations in the course of all conduct on behalf of the Company, including the United States Foreign Corrupt Practices Act (FCPA) of 1977.

RELATED POLICIES

In addition to the general policies above, the Company adopts the following additional conduct-related policies as part of the Code of Ethics:

- Conflict of Interest and Confidentiality

- Seaboard Corporation Code of Conduct and Ethics for Senior Financial Officers

- Trading Seaboard Securities

- Sanctions and Anti-Terrorism (OFAC) Compliance

- OFAC Restricted Party Screening Procedures

- Anti-Corruption

These policies are attached. As a condition of employment, each employee of the Company must be familiar with these policies and agree to abide by their provisions. Violations of the content or spirit of this Code of Ethics and its related provisions are unacceptable and may lead to disciplinary action up to and including termination of employment or separation of ongoing business relationship with the Company.

REPORTING VIOLATIONS

If anyone has knowledge of a violation of this Code, that person should report the matter to one or more of the following: the person's immediate supervisor or the Company's Chief Compliance Officer. Alternatively, the matter may be reported anonymously online by visiting www.seaboard.ethicspoint.com; by calling the Company's dedicated toll free number, (866) 676-8886, for calls originating from the United States; or by calling the applicable phone number associated with the specific country, as set forth at the aforementioned website, for international calls. Matters may also be emailed to SBD_Ethics@seaboardcorp.com. The Company will not allow any retaliation against an employee who acts in good faith in reporting any such violation or suspected violation.

****

This Code of Ethics covers a wide range of business practices. It does not address every issue that may arise but provides general guidance about the Company's expectations of proper conduct and basic ethical and legal responsibilities. All consolidated subsidiaries of Seaboard Corporation are expected to adopt this Code of Ethics or a similar policy containing only such changes as are approved by Seaboard Corporation's Chief Compliance Officer. Any questions as to the meaning of any provisions of this Code of Ethics policy, or whether intended conduct is a violation of this policy, should be addressed to the Company's Chief Compliance Officer.

CONFLICT OF INTEREST AND CONFIDENTIALITY

Seaboard Corporation and its subsidiaries (collectively, the "Company") require directors, officers and employees to conduct their non-work activities in a manner that does not conflict with the interests of the Company or detract from the performance of their work-related responsibilities. Directors, officers and employees shall follow the general guidelines set forth below. The failure of any employee to adhere to these general guidelines may result in discipline, including termination of employment.

1. Conflicts of Interest.

   A. No director, officer or employee of the Company shall have, directly or indirectly, any financial or other interest in any entity that does business with the Company. The foregoing shall not prohibit the ownership of not more than 2 percent of the stock of any entity that does business with the Company which is listed upon a national stock exchange or actively traded in the over-the-counter market.

   B. Officers and employees shall not be employed by another entity or individual, participate in self-employment, or serve another entity in any manner where such activity will require an excessive amount of time or materially interferes with the officer's or employee's ability to perform his job function on behalf of the Company. Officers and employees whose job functions involve interaction with entities or individuals with whom the Company does business shall not conduct similar business with such entities or individuals for such officer's or employee's own personal affairs or business, receive any personal financial or other benefits, or take any corporate opportunity of the Company without first obtaining approval from the Company's Board of Directors. Directors, officers and employees should disclose any such actual or potential conflicts of interest to the Company's Board of Directors, which will determine the appropriate resolution thereof. All directors, officers and employees must recuse themselves from any Board of Directors discussion affecting their personal, business or professional interests.

   C. All officers and employees shall be required to complete a form disclosing: (i) all conflicts of interest which such officer or employee has knowledge of, or reasonably expects may arise; and (ii) all board of director or officer positions such officer or employee holds with trade associations or for-profit organizations. The Company may require a person with an existing or potential conflict of interest to dispense with such activities or positions. The failure of any person to complete such form disclosing all known existing or potential conflicts of interest or the failure to dispense with conflicts of interest, when requested by the Company, may result in discipline by the Company, including termination of employment.

   D. Any request for a waiver of any provision of this Conflict of Interest Policy must be in writing and addressed to the Board of Directors. Any waiver of this Conflict of Interest Policy must be approved by the Board of Directors and disclosed promptly to the extent required by applicable rules of the SEC and NYSE American Company Guide.

   E. Officers and employees have a duty to avoid possible conflicts of interest. For example, if a situation arises where an employee's or affiliated party's personal interest conflicts with the interests of the Company, or an employee uses his or her position with the Company to achieve personal gain, a conflict of interest may exist. Such a conflict of interest may harm the integrity of both the Company and the employee.

F. Conflicts of interest may not always be clear-cut, so if you have a question, you should consult with your supervisor or manager or, if circumstances warrant, the General Counsel or Chief Compliance Officer of the Company. Situations that may present a conflict of interest will be evaluated for propriety on an individual basis.

2. Personal Gain.

A. All of the business affairs of the Company with all parties, including government officials, suppliers, customers, unions, trade associations and competitors, shall always be conducted on an ethical, legal and arm's length basis.

B. Directors, officers and employees shall not accept payments, gifts, or favorable business arrangements or treatment for the purpose of securing preferential consideration from the Company or as an inducement to the Company to enter into any transaction. Examples of such prohibited conduct include taking material gifts, gratuities, favors, loans, guarantees of loans, commissions, excessive entertainment, kickbacks, rebates, and other types of inducements, whether financial or of any other nature.

C. Common business practice permits the offer or acceptance of certain courtesies of nominal value, usually in the form of meals and entertainment, provided objectivity of the parties will not be unduly affected.

3. Confidential Information.

It is vital that we protect the privacy of the Company's confidential information. Confidential information includes proprietary, technical, business, financial, joint venture, customer and employee information that is not available publicly. It is the employee's responsibility to know what information is confidential and to obtain clarification when in doubt. The failure of any employee to adhere to these general guidelines may result in discipline, including termination of employment and/or benefits arising from employment and/or legal action by the Company.

A. Employees must not disclose confidential information to any person outside of the Company, unless authorized to do so. This includes, as prohibited, any disclosure of confidential information to family and friends. Where confidential information is entrusted to persons outside of the Company, efforts must be made to ensure the continuing protection and confidentiality of that information. Within the Company, confidential information should be disclosed only on a "need to know" basis.

B. Employees must not use confidential information for unauthorized purposes. They must also take reasonable care to protect confidential information against loss, theft, unauthorized access, alteration or misuse.

C. Employees leaving the Company who have had access to Company confidential information have a continuing responsibility to protect it and maintain its confidentiality. The Company expects that employees joining it from other companies will not disclose the confidential information of those other prior employers.

CODE OF CONDUCT AND ETHICS
FOR SENIOR FINANCIAL OFFICERS

INTRODUCTION

This Code of Conduct and Ethics for Senior Financial Officers ("Code of Conduct and Ethics") has been adopted by the Board of Directors of the Company to promote honest and ethical conduct, proper disclosure of financial information in the Company's periodic reports, and compliance with applicable laws, rules, and regulations of the NYSE American Company Guide ("NYSE American") and the Securities and Exchange Commission ("SEC") by the Company's senior officers who have financial responsibilities.

APPLICABILITY

As used in this Code of Conduct and Ethics, the term Senior Financial Officer means the Company's Chief Executive Officer, Chief Financial Officer, Principal Accounting Officer, Controller, or persons performing similar functions (each a "Senior Financial Officer").

PRINCIPLES AND PRACTICES

In performing his or her duties, each of the Senior Financial Officers must:

- Maintain high standards of honest and ethical conduct and avoid any actual or apparent conflict of interest as defined in the NYSE American and the rules and regulations of the SEC, and any Company Conflicts of Interest and Code of Ethics Policy, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;

- Report to the Audit Committee of the Board of Directors promptly any conflict of interest that may arise and any material transaction or relationship that reasonably could be expected to give rise to a conflict;

- Provide, or cause to be provided, full, fair, accurate, timely, and understandable disclosure in reports and documents that the Company files with, or submits to, the SEC and in other public communications;

- Comply and take all reasonable actions to cause others to comply with applicable rules and regulations of the NYSE American and the SEC; and

- Promptly report violations of this Code of Conduct and Ethics to the Company's Audit Committee.

WAIVER

Any request for a waiver of any provision of this Code of Conduct and Ethics must be in writing and addressed to the Board of Directors. Any waiver of this Code of Conduct and Ethics must be made by the Board of Directors and will be disclosed promptly by means approved by the SEC and the NYSE American.

COMPLIANCE AND ACCOUNTABILITY

The Audit Committee will at least annually assess compliance with this Code of Conduct and Ethics and the performance of the Senior Financial Officers, and report material violations to the Board of Directors, and recommend to the Board appropriate action.

This Code of Conduct and Ethics shall be posted on the Company's website at www.seaboardcorp.com.

POLICY WITH REGARD TO TRADING
SEABOARD SECURITIES

1. In General.

In the course of their employment with Seaboard Corporation or its subsidiaries (collectively, the "Company"), directors, officers and employees frequently come into possession of confidential and highly sensitive information concerning the Company, its customers, suppliers or other corporations with which the Company has contractual relationships or may be negotiating transactions. Much of this information has a potential for affecting the market price of securities issued by the corporations involved. Under some circumstances, federal securities law imposes potentially substantial civil and criminal penalties on persons who improperly obtain, use or provide material, non-public information, in connection with a purchase or sale of securities.

Also keep in mind, the Securities and Exchange Commission ("SEC") may seek substantial civil penalties from any person who, at the time of an insider trading violation, "directly or indirectly controlled the person who committed such violation," i.e., an employer. As noted above, civil penalties for persons who control violators can equal the greater of $1,000,000 or three times the profit gained or losses avoided. Employers may also be subject to criminal penalties of $2,500,000 for insider trading violations committed by employees. Accordingly, when the maximum criminal penalty is combined with the maximum civil penalty, employers of persons who trade on the basis of insider information may be liable for up to $3,500,000 – even for employee violations that yield a small profit gained or loss avoided.

The statute provides that any "controlling person" may be liable for civil penalties up to the amount specified above if the controlling person both (i) knew or recklessly disregarded the fact that the employee was likely to engage in a violation; and (ii) failed to take appropriate steps to prevent that violation before it occurred. Moreover, in recent years, the SEC and governmental prosecutors have been vigorously enforcing the insider trading laws against both individuals and institutions.

Given these factors, the Company has determined to provide specific guidance concerning the propriety of various personal transactions, and to impose specific procedures in certain cases to attempt reasonably to ensure that neither the Company nor any of its directors, officers and employees violates insider trading laws.

2. Material Non-Public Information.

The federal securities laws and regulations have been held to prohibit the purchase or sale of a security at a time when the person trading in that security possesses material non-public information concerning the issuer of the security, or the market for the security, which has not yet become a matter of general public knowledge and which has been obtained or is being used in breach of a duty to maintain the information in confidence. Whether the information is proprietary information about the Company or information that could have an impact on the Company's stock price, employees must not pass the information on to others. The penalties discussed above apply, whether or not you derive any benefit from another's actions.

"Material non-public information" includes information that is not available to the public at large which could affect the market price of the security and to which a reasonable investor would attach importance in deciding whether to buy, sell, or retain the security. Examples of information that might be deemed material include the following: annual or quarterly financial results, dividend increases or decreases, the declaration of a stock split or the offering of additional securities, earnings estimates, changes in previously announced

earnings estimates, significant expansion or curtailment of operations, a significant increase or decline in business, a significant merger or acquisition proposal or agreement, unusual borrowings or securities offerings, major litigation, impending bankruptcy or financial liquidity problems, significant changes in management, purchases or sales of substantial assets, or the gain or loss of a substantial customer or supplier. This list is not exhaustive. Other types of information may be material at any particular time, depending upon the circumstances. It should be noted that either positive or adverse information may be material.

Information is considered to be available to the public only when it has been released to the public through appropriate channels (i.e., by means of a press release or a statement from one of the Company's senior officers) and enough time has elapsed to permit the investment market to absorb and evaluate the information. Once public release has occurred, information will normally be regarded as absorbed and evaluated within two or three days thereafter.

3. Company Policy.

As long as an officer, director or employee has material non-public information relating to the Company or any other issuer, including any of the Company's customers, it is Company policy that the officer, director or employee may not directly or indirectly buy or sell the securities of the Company or any other affected issuer. Equally important, the information may not be passed along to others. This policy shall apply to officers, directors and employees of the Company or its subsidiaries and affiliates.

To avoid potential liability under this policy, all officers, directors and employees of the Company must not purchase or sell securities of the Company or of any other issuer of a security at a time when the officer, director or employee is aware of any material non-public information about the Company or any issuer, regardless of how that information was obtained. The officer, director or employee also must not permit any member of his or her immediate family or anyone acting on his or her behalf, or anyone to whom he or she has disclosed the information, to purchase or sell such securities.

After the information has been publicly disclosed through appropriate channels, a reasonable time should be allowed to elapse (at least three business days) before trading in the security, to allow for public dissemination and evaluation of the information.

Without limiting the generality of the policy stated herein, no director, officer or employee of the Company or its subsidiaries and affiliates, or other employee possessing material non-public information, may make any purchase or sale of securities of the Company (i) from the 25th day of the last month of each fiscal quarter until the beginning of the third business day after the public release of earnings for such quarter; (ii) from the time of the public release of any material information until the beginning of the third business day after such release; (iii) during any period when he or she is aware that the Company expects to make a public release of material information in the near future; and (iv) during any other period when he or she has knowledge of any "material inside information" concerning the Company.

4. Application of Policy to Family Members and Affiliates.

The foregoing requirements also apply to any purchase or sale of securities of the Company by a family member or others sharing the same address or by a corporation, partnership, trust or other entity owned or controlled by a director, officer or employee.

5. Prohibition of Short-Sales.

Federal securities laws prohibit any short sale or any short sale "against the box" of Company securities by any officers, directors or greater than ten-percent shareholders. A short sale is the sale of a security either not owned by the seller, or if owned, not delivered (the so-called short sale "against the box"), which involves the borrowing of shares by the seller's broker for the account of the seller and delivery of the borrowed shares to the buying broker. At some point in the future, the short seller must purchase the securities to cover the short position. Because the short seller hopes that he or she will be able to purchase at a price lower than the price at which the short sale was made, a short seller expects a security to decline in market value from present levels. Since short sales can depress the price of securities, the Company requires that none of its officers, directors or employees ever make short sales of the Company's securities (whether or not such short sales would be permitted under the federal securities laws).

6. Prohibited Practices.

In addition, it is the Company's policy that officers, directors and employees should not engage in any of the following activities with respect to the securities of the Company:

A. Trading in securities on a short-term basis. Any security purchased must be held for a minimum of six months before sale, unless the security is subject to forced sale, i.e., as a consequence of merger or acquisition;

B. Purchases on margin without the prior, written consent of the Company after disclosure to the Company's Board of Directors;

C. Short sales; or

D. Buying or selling put or call options.

SANCTIONS AND ANTI-TERRORISM (OFAC) COMPLIANCE POLICY

1. Objective and Scope.

It is the policy of Seaboard Corporation, its subsidiaries,[1] and applicable affiliates[2] (collectively, "Seaboard" or "Company") to comply with the laws of the U.S. and other applicable laws, which includes rules and regulations of the Office of Foreign Assets Control, a division of the U.S. Department of Treasury ("OFAC"). OFAC administers and enforces U.S. economic trade sanctions in order to achieve national security goals of the U.S. against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the U.S. OFAC regulations prohibit U.S. entities and their foreign branches,[3] U.S. citizens, permanent residents (including green card holders) no matter where they are located, and any persons physically present in the U.S., from engaging in or facilitating transactions or making monetary transfers to certain designated countries and designated entities and persons listed on the OFAC list of Specially Designated Nationals and Block Entities ("SDN List" or SDN(s)), as well as other restricted parties.[4] The list includes numerous parties listed by name (i.e., individuals, companies, vessels, banks).

Seaboard Corporation's Chief Compliance Officer (the "Compliance Officer") has primary responsibility for overseeing this Policy and its implementation, monitoring and execution. The respective General Counsels for Seaboard Marine, Ltd. and Seaboard Foods LLC; the Chief Compliance Officer for Seaboard Overseas and Trading Group; and the respective Chief Financial Officers for Seaboard Energías Renovables y Alimentos S.R.L and Transcontinental Capital Corp. (Bermuda) Ltd. (each, the "Subsidiary Compliance Officer") are responsible for the implementation, monitoring, and execution of this Policy for their respective entities and respective subsidiaries thereof. The Compliance Officer and each Subsidiary Compliance Officer may utilize external legal counsel to further ensure compliance with applicable Sanctions and Anti-Terrorism laws and this Policy.

This Policy requires the Company to institute screening procedures with respect to proposed international counter-parties and any other parties in the related supply chain that are known in the ordinary course of business. This search may include correspondent or beneficiary banks of counter-parties when known (or originating banks with respect to monies being transferred to the Company) that are located in or affiliated

[1] For purposes of this Policy, a subsidiary is defined as any entity as to which Seaboard Corporation owns, directly or indirectly, more than a 50 percent equity interest by vote or value; holds a majority of seats on the board of directors of the entity; or otherwise controls the actions, policies, or personnel decisions of the entity.

[2] For purposes of this Policy, an affiliate is defined as any entity as to which Seaboard Corporation owns, directly or indirectly, 50 percent or less of the equity interests and which is not otherwise a subsidiary. This Policy shall apply to an affiliate if such entity is organized under U.S. laws, has U.S. person employees, transacts in USD, or uses U.S. banking institutions. If such criteria or U.S. nexus does not exist, then the board of directors of such affiliate may determine in its own discretion whether to implement this Policy.

[3] Any corporation, partnership, association, or other organization organized under the laws of the United States or of any State, territory, possession, or district of the United States.

[4] The SDN List is available on OFAC's website at https://www.treasury.gov/resource-center/sanctions/sdn-list/pages/default.aspx. Other OFAC sanctions lists also are available online: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx. A consolidated list that includes all OFAC sanctions list, as well as other U.S. restricted party lists are available at https://www.trade.gov/data-visualization/csl-search.

with countries which are the subject of comprehensive or list-based sanctions (or otherwise subject to a sanctions program administered by OFAC) ("High-Risk Countries"). See Section 2 below. This search shall be done by reviewing the SDN List (via the Consolidated Screening List search engine[5]) and by subscribing to a web-based searchable database to confirm that counter-parties, among other parties in the supply chain, are not on the SDN List. For details regarding the screening process, please consult the Restricted Party Screening Procedures ("Procedures").

In the event of the discovery of any violation of this Policy, the violation should be promptly reported to the appropriate Subsidiary Compliance Officer and the Compliance Officer.

All applicable records of OFAC compliance, violations, and audit work papers will be retained according to OFAC requirements (5 years).

Seaboard expects its employees to comply with all applicable laws and to maintain the highest ethical standards of business conduct at all times.

This Sanctions and Anti-Terrorism Compliance Policy (this "Policy") will assist employees in complying with all applicable laws and regulations relating to economic sanctions and anti-terrorism, including but not limited to the Trading with the Enemy Act (50 U.S.C. §§ 1-44, as amended), the International Emergency Economic Powers Act (50 U.S.C. § 1701 et seq.) ("Sanctions Laws"), and the Executive Order No. 13224 on Terrorist Financing, effective September 24, 2001, and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (P.L. 107-56 (2001), 115 Stat. 272) ("Anti-Terrorism Laws"). It applies to all directors, officers, employees and agents of the Company (when acting as an agent for the Company), its subsidiaries and applicable affiliates ("Covered Persons"), and covers dealings with counterparties in both the public and commercial or private sectors.

This Policy requires compliance with all applicable economic sanctions laws and regulations, specifically those administered and enforced by OFAC, the U.S. State Department, and the United Nations Security Council (collectively, "Sanctions"), as well as Anti-Terrorism Laws. The Policy requires that the Company and Covered Persons, not:

A. Sell or transport any products or provide any services to, or otherwise do any business involving, countries or territories, or governments, subject to comprehensive U.S. sanctions (as of the date of this Policy, Cuba, Iran, Syria, North Korea, and the Crimea, Donetsk, and Luhansk regions of Ukraine);

B. Engage in any prohibited business with persons or entities that are designated on U.S., UN, and other applicable international terrorism and restricted party lists; or

C. Engage in any financial transactions with knowledge that they involve proceeds of unlawful criminal activity, or otherwise pose red flags suggesting an attempt to conceal the origin of funds with connections to unlawful activity.

Any exceptions to this Policy (i.e., the transaction is authorized under an OFAC General License or a specific license from OFAC has been obtained) must be consistent with U.S. and other applicable laws, and will be made only with the explicit authorization of the Subsidiary Compliance Officer and the Compliance Officer.

[5] See Consolidated Screening List (trade.gov)

Violations of this Policy can result in civil and even criminal liability for the Company and individual employees, and may result in appropriate disciplinary actions, including possible termination of employment.

Any questions about your obligations to comply with Sanctions Laws, Anti-Terrorism Laws, or this Policy, or if you suspect that any violation has occurred, should be addressed to the Subsidiary Compliance Officer or the Compliance Officer.

2. Overview of U.S. Sanctions.

OFAC is the primary U.S. government agency responsible for administering and enforcing Sanctions, which are laws and regulations that restrict business with certain countries, individuals, and entities in order to advance specific foreign policy and national security priorities.

OFAC maintains several types of Sanctions programs, including:

A. Comprehensive Sanctions. OFAC currently administers comprehensive economic sanctions against Cuba, Iran, Syria, North Korea, and the Crimea, Luhansk, Donetsk, Zaporizhzhia, and Kherson Regions of Ukraine. The Company will not engage in any transactions or dealings with any counterparty or third-party located in a comprehensively sanctioned country, directly or indirectly (i.e., through agents, distributors, resellers, etc.), unless authorized under U.S. law. In addition to the above programs, OFAC maintains an embargo on the Government of Venezuela. (the countries and regions in this paragraph are the "Comprehensively Sanctioned Countries").

As noted above, unless authorized by the Subsidiary Compliance Officer and the Compliance Officer in advance and in writing, the Company will not do any business in countries or territories subject to comprehensive sanctions.

B. List-Based Sanctions. Sanctions also target entities and individuals designated on OFAC's sanctions lists, including the SDN List. Importantly, OFAC considers any entity 50 percent or more owned, directly or indirectly and in the aggregate, by individual(s) or entities identified on the SDN List also to be subject to SDN sanctions, even if the entity is not itself designated on the SDN List.

OFAC's list-based country sanctions target SDNs relating to the following countries: the Balkans (i.e., Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia), Belarus, Burma (Myanmar), Burundi, Central African Republic, Democratic Republic of the Congo, Ethiopia, Hong Kong, Iraq, Lebanon, Libya, Mali, Nicaragua, Republic of the Congo, Russia, Somalia, Sudan, South Sudan, Ukraine, Yemen, and Zimbabwe (for purposes of this Policy, the foregoing countries, together with the Comprehensively Sanctioned Countries" are deemed the "High Risk Countries"). These Sanctions are typically imposed on certain persons and entities in or associated with prior or current regimes in these countries. These jurisdictions are generally considered higher-risk jurisdictions for Sanctions compliance. Customers, agents, suppliers, vendors, resellers, and other third parties located in or affiliated in these High-Risk Countries should be subject to heightened due diligence prior to engagement, which should include a review of beneficial ownership information by local management affiliated with the relevant Seaboard subsidiary or affiliate.

The Company may not engage in any business with an SDN List party, or a party subject to SDN List sanctions due to its ownership, and must block and "freeze" any money received from such a

party (i.e., not give it back to that party), and report the facts and circumstances immediately to the Compliance Officer for further guidance.

C. Sectoral Sanctions. These Sanctions target specific sectors of a country's economy. Currently, the primary sectoral sanctions that OFAC imposes relate to the Russia/Ukraine sanctions programs. Designated persons are added to OFAC's Sectoral Sanctions Identifications List ("SSI List"). Unlike persons added to the SDN List, U.S. persons and companies may engage in most business with parties on the SSI List because only narrow, targeted categories of dealings or transactions are prohibited.

However, given that sectoral sanctions are complex, any business with any SSI-listed party (or an entity that is >50 percent owned by one or more SSI-listed parties) is prohibited, unless authorized by the Subsidiary Compliance Officer and the Compliance Officer and such dealings are not otherwise prohibited by Sanctions or other applicable laws.

D. Secondary Sanctions. Secondary sanctions target non-U.S.-person individuals and entities that provide support for sanctioned jurisdictions, entities, or individuals. Currently, secondary sanctions mainly target certain sectors and activities related to Iran, North Korea, Russia, Syria, and Venezuela. Also, it should be noted that the U.S. Crimea sanctions program authorizes the designation of any individual or entity worldwide determined by the U.S. government to "operate" in the Crimea region.

3. Prohibition Against Facilitation.

U.S. persons are prohibited from providing assistance of any kind that would facilitate transactions with sanctioned countries or persons by third parties outside of the U.S., including financing-related activities, referrals of sales opportunities, approvals, or brokering. Put differently, a U.S. person may not assist a non-U.S. third party in performing transactions with sanctioned countries or persons, even if that third party is able to do so under the laws of the jurisdiction that apply to the third party.

OFAC interprets the sanctions prohibitions discussed above to prohibit U.S. persons from "facilitating" transactions of non-U.S. persons with an SDN. In other words, a U.S. person cannot engage in a transaction through a non-U.S. person that would be prohibited by U.S. sanctions if conducted by the U.S. person. OFAC construes "facilitation" very broadly to include all instances in which a U.S. person "assists" or "supports" a non-U.S. person in transactions directly or indirectly involving an SDN.

OFAC has provided examples of activities that could constitute facilitation which include assisting with business and legal planning; decision-making; approvals; designing; ordering or transporting goods; or providing financial or insurance assistance in connection with such sanctioned country business. U.S. persons also are generally prohibited from approving, reviewing or commenting on the terms of a transaction or deal documents, engaging in negotiations, or otherwise assisting the non-US entity or individual in planning for or moving a transaction forward.

As set forth in OFAC's sanctions programs and rules, prohibited facilitation can arise in many ways:

A. The involvement of a U.S. citizen working for a non-U.S. company in a transaction which would be prohibited under U.S. sanctions. These employees could be held individually liable for participating in the negotiation, the performance or wider decision-making in relation to a prohibited transaction — even where the transaction had been approved and licensed by the relevant domestic authorities;

B. The involvement of U.S. persons in altering operating policies or procedures to permit a foreign subsidiary to do business that a U.S. parent cannot undertake due to sanctions considerations. A U.S. manager may not modify existing business procedures to avoid or avert his involvement, or that of other U.S. persons, in a particular transaction[6]; or

C. U.S. persons also are prohibited from referring to non-U.S. entities or individuals any business opportunities involving sanctioned countries, entities, or individuals to which the U.S. person could not directly respond under U.S. sanctions regulations. Thus, if a U.S. person receives an inquiry involving an SDN, the U.S. person must decline the opportunity and cannot refer that inquiry to a non-U.S. individual or entity to handle.

In addition, select international organizations and other jurisdictions maintain separate sanctions laws and sanctions-restricted party lists, including the United Nations Security Council, the European Union (and its member states), and the United Kingdom. Seaboard's policy is to comply with the sanctions laws of other jurisdictions (i.e., UK and EU) to the extent applicable. Such compliance often entails working with local legal counsel.

4. Overview of Anti-Terrorism Laws.

Anti-Terrorism Laws are complex, but at their core they criminalize activities including conducting or attempting to conduct a financial transaction with the intent to promote a specified unlawful activity, or with knowledge (including willful blindness) that the transaction is designed to conceal or disguise the location, nature, source, ownership, or control of the proceeds of specified unlawful activity. They also criminalize knowingly engaging in monetary transactions in property with a bank, insurance company, or other financial institution derived from specified unlawful activities.

5. Procedures for Compliance with Sanctions.

The Company engages, directly or indirectly, with customers, suppliers, agents, vendors, financial institutions, and other business partners ("Third Parties") outside of the United States. Prior to engagement of such persons or entities to provide services to the Company, the Company will perform restricted party screening of any non-U.S. Third Parties or otherwise confirm that the Third Parties are not subject to any Sanctions. See the Procedures. The purpose of this due diligence is to confirm that such parties and their owners are not the target of Sanctions, and do not involve any countries or parties targeted by Sanctions or export controls restrictions.

Any questions or red flags should be raised to the Subsidiary Compliance Officer or the Compliance Officer. If a country or party subject to Sanctions may be involved in a potential transaction or other agreement, do not proceed and report the situation to the Subsidiary Compliance Officer and the Compliance Officer immediately.

Sanctions and restricted party lists change frequently, and our policy is to stay up to date on changes in this area. The Company will provide periodic updates on developments relevant for the Company's business, and will review this Policy annually.

[6] For example, if certain types of transactions or certain transactions exceeding certain dollar thresholds historically have required U.S.-person approval, the U.S. person may not change its own policies or procedures or those of its non-U.S. affiliate to transfer responsibility for those decisions to non-US persons in order to allow a transaction to proceed.

6. Screening of Third Parties.

The Company will screen all of its non-U.S. third-party advisors, distributors, vendors and financial institutions, against the U.S. sanctioned party lists. For more detailed information on the screening process, please refer to the Procedures.

In order to obtain the necessary information for the screening process, the Company will require that each such non-U.S. third-party provide the following information when High Risk Countries are involved and as otherwise appropriate or feasible:

A. Corporate Entities:

- Legal Name;
- Beneficial Ownership Details of Ultimate Beneficial Owners with at least 25 percent interest (as appropriate);
- Email Address & Entity Website;
- Telephone Number;
- Incorporation Documents or other Entity Registration Documents or Government-issued Business License;
- Business Address for Principal Place of Business;
- Tax or Other Identification Number;
- Trade Manager - Name, Identity and Date of Birth ("DOB").

B. Individuals:

- Name;
- E-mail Address;
- Mobile Number;
- DOB;
- Physical Address;
- Government-issued Photo Identification;
- Taxpayer Identification or Other Government-issued document evidencing nationality and residence.

Steps to Follow When the Screening Results in a "Hit":

If the screening results in a "hit" against a sanctioned parties list, the Company's screening personnel will report the "hit" immediately to the Subsidiary Compliance Officer or the Compliance Officer if it relates to Seaboard Corporation. Then, the screening personnel will follow the following steps to determine if the "hit" is a valid "match" to a sanctioned person:

A. Determine if the "hit" is against Sanctioned Parties list - Confirm whether or not the "hit" is against a person or entity listed in the Restricted Parties List (see https://www.trade.gov/consolidated-screening-list), which includes but is not limited to sanctioned parties; it also includes parties subject to export controls restrictions) or is from an embargoed country, region, or territory. If it is (or you cannot tell what the "hit" is), proceed to the next step.

B. Evaluate the quality of the "hit" - Compare the name in the transaction with the name on the sanctioned parties list. Is the name an individual while the name on the Restricted Parties List is a vessel, organization or company (or vice-versa)? If yes, there is not a valid "match." If no, continue to the next step.

C. Determine the extent of the "match" - Determine how much of the name on the SDN List matches the name in the transaction. If only one of two or more names match (i.e., only the last name matches), you do not have a valid "match." If two or more of the names match, proceed to the next step.

D. Compare your "hit" to the Complete OFAC SDN List or CSL entry - Compare the complete OFAC entry with the information that you have on the matching name in the transaction. A Restricted Party List entry may include a full name, address, nationality, passport, tax ID, place of birth, date of birth and former names/aliases.

E. If there is a Match or an Unresolved hit - If you do not have sufficient information to evaluate the hit against the SDN list or, if you have most of the information and there are a number of similarities or exact matches, contact the Subsidiary Compliance Officer or the Compliance Officer if it relates to Seaboard Corporation.

- With the approval of the Subsidiary Compliance Officer or the Compliance Officer if it directly relates to Seaboard Corporation, you may attempt to obtain more information by contacting the applicable party through the email address provided during the on-boarding or vetting process.

- If the Subsidiary Compliance Officer or the Compliance Officer if it relates to Seaboard Corporation concludes that there is a match, or if the hit remains unresolved, the Company should not proceed with the transaction.

7. Blocking of Property of a Sanctioned Party or Rejecting a Transaction.

Depending on the Seaboard subsidiary involved (i.e., foreign subsidiary not otherwise subject to U.S. jurisdiction), if the Company has possession of assets of a sanctioned party, we are typically obligated to "block" this property and report the transaction to OFAC within ten business days of the blocking action. In doing so, we will obtain any necessary assistance from external legal counsel on "blocking" the property and provide any required "blocking report" to OFAC.[7] The Company then will continue to block the property until OFAC provides further direction or the Company obtains a specific license from OFAC "unblocking" the property.

To block a transaction is to (i) not process the transaction; and (ii) hold/freeze the funds. Rejecting means simply refusing to process the transaction.

A transaction must be blocked when a blockable interest exists, meaning that funds are destined for, or are received from, an SDN. Blocked funds must be held in a separate interest-bearing account. OFAC will ultimately determine the disposition of the funds.

[7] See https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-501/subpart-C/section-501.603; https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-501/subpart-C/section-501.604

A transaction without a blockable interest must be rejected. One example would be an OFAC match on a commercial payment destined for the account of ABC Import-Export in North Korea, whose account is with a bank in South Korea. Neither the beneficiary nor its bank is an SDN, so there is no blockable interest in this transaction. However, under the North Korean sanctions regulations, all trade with North Korea is prohibited. By processing this payment, a U.S. company or financial institution would be effectively facilitating trade with North Korea. Accordingly, the transaction should be rejected.

A blocked or rejected transaction must be reported to OFAC within ten business days of the decision to do so. OFAC provides the online ORS system, where a blocked or rejected transaction report may be filed electronically by completing an online form.[8] Use of ORS is voluntary, and pre-registration is required. Alternatively, an electronic form of the report may be e-mailed to OFAC.

8. Procedures Relating to Terrorism Risks.

To address terrorism risks associated with Third Parties, the Company will conduct appropriate "know your customer" diligence on Third Parties prior to onboarding, including collecting information necessary to verify the Third Party's identity. Covered Persons should report any activities or arrangements that appear suspicious or indicative of terrorism to the Compliance Officer immediately. Covered Persons may not inform any other counterparty regarding any such suspicion as doing so could be a violation of Anti-Terrorism Laws.

9. Potential Red Flags Related to Terrorism.

The following non-exhaustive list of "red flag" indicators and arrangements may generally be considered suspicious under Anti-Terrorism Laws and may arise at any time during a Third-Party relationship:

A. The maintenance of a complex corporate or organizational structure where such complexity does not seem to be warranted;

B. Multiple persons or accounts that share the same name, address, telephone number, or other identification, but otherwise appear unrelated;

C. One person or entity that uses multiple addresses or P.O. boxes for no apparent reason;

D. Transfers of funds to an individual person's bank account instead of an organization or entity's bank account. It is the policy of the Company to transfer funds to an organization's official bank account registered in the name of that organization;

E. Financial activity that generally appears inconsistent with a Third Party's stated objectives or financial circumstances, or the Company's understanding of the Third Party's organization;

F. Accounts funded by one individual or entity and then transferred to an apparently unrelated individual or entity; and

G. Payment is being made by a third party which is not the direct counterparty to the transaction or matter.

[8] See OFAC Reporting System | Office of Foreign Assets Control (treasury.gov)

10. Penalties For Violations.

Adherence to this Policy and the procedures described herein is very important. Violations of Sanctions and Anti-Terrorism laws may result in civil and criminal penalties. The Company will deal with any violations consistent with its disciplinary policies, including possible termination in appropriate circumstances.

11. Recordkeeping and Internal Controls.

The Company requires that records of any restricted party screening and due diligence conducted on Third Parties under this Policy be kept for at least five years. This means all identifying information regarding the Third Party, including reasonable detail of all transactions and payments screened, including financial institutions (i.e., beneficiaries, originators, letter of credit applicants, and their banks; intermediary banks; correspondent banks; issuing banks; and advising or confirming banks). This retention policy extends to all parties or payments that are within the scope of the screening (or due diligence) requirements.

12. Compliance Training.

The Company has a training program that is tailored to the Company's risk profile and reaches appropriate personnel. The Company's training program is intended to accomplish the following: (i) provides job-specific knowledge; (ii) communicates the compliance responsibilities for each employee; and (iii) holds employees accountable for sanctions compliance training through assessments.

The Company will conduct training annually. The Company will take immediate action to provide corrective training to relevant personnel when it learns of a weakness in its procedures. Further, the Company will ensure its training program includes resources and materials that are available and accessible to all relevant personnel.

The Human Resources Department will oversee all communications to, and periodic training of, relevant Covered Persons on processes and requirements documented in this Policy. A certification is attached hereto as Appendix A, which should be completed by all relevant Covered Persons on an annual basis.

The Human Resources department is responsible for collecting such certifications.

13. Program Auditing and Assessment.

The Company will periodically conduct audits to assess the effectiveness of this Policy and to identify any weaknesses and deficiencies. The audit team will include relevant Company personnel with sufficient expertise, resources, and authority to perform its functions.

14. Reporting Requirements and Whistleblower Protection.

Covered Persons must report to the Subsidiary Compliance Officer and the Compliance Officer any knowledge, awareness, or reasonable suspicion of a potential violation of this Policy or applicable Sanctions or Anti-Terrorism Laws. All reports of violations of Sanctions or Anti-Terrorism Laws and/or non-compliance with this Policy will be reviewed as a priority. To ensure that the reported violation can be fully investigated, please provide as detailed an account as possible including any supporting evidence. The outcome of an investigation may range from no further action being taken (i.e., where allegations are not substantiated) to formal disciplinary action against a Covered Person, up to and including termination of employment.

Seaboard prohibits and will not tolerate any retaliation or threatened retaliatory action against any Covered Person who reports a possible violation of Sanctions, Anti-Terrorism Laws, or this Policy. Similarly, any Covered Person who discourages or prevents another either from making such a report or seeking the help or assistance he or she needs to report the matter will be subject to disciplinary action. Retaliation is a violation itself and should be reported to the Compliance Officer.

OFAC RESTRICTED PARTY SCREENING PROCEDURES

1. Applicability.

In accordance with its Sanctions and Anti-Terrorism Compliance Policy and the Code of Ethics, Seaboard Corporation, its subsidiaries,[9] and applicable affiliates[10] (collectively, "Seaboard" or "Company") are committed to compliance with all applicable laws and regulations, specifically those related to U.S. economicsanctions ("Sanctions") and complying with all prohibitions and restrictions related to dealings with persons on sanctions-restricted party lists ("Sanctions Lists"). The following procedures for identifying parties and destinations restricted under the Procedures apply to the Company, including its directors, officers, employees and agents (collectively, "Covered Persons").

2. Summary of Screening Process.

Seaboard supports and is fully committed to the efforts and objective of the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and other agencies of the U.S. Government to sanction certain foreign countries, regimes and individuals that engage in terrorism, international narcotics trafficking, proliferation of weapons of mass destruction and any other threat to the national security, foreign policy or economy of the U.S. For purposes of the implementation, monitoring and execution of these Procedures please contact Seaboard Corporation's Chief Compliance Officer ("Seaboard Compliance Officer"). The respective General Counsels for Seaboard Marine, Ltd. and Seaboard Foods LLC; the Chief Compliance Officer for Seaboard Overseas and Trading Group and the respective Chief Financial Officers for Seaboard Energías Renovables y Alimentos S.R.L ("SERA") and Transcontinental Capital Corp. (Bermuda) Ltd. ("TCCB") (each, the "Subsidiary Compliance Officer") are responsible for the implementation, monitoring, and execution of these Procedures for their respective entities and respective subsidiaries thereof.

Seaboard has implemented a two-step compliance process that is required for all subsidiaries and certain affiliates (regardless of domicile and whether the entity is subject to U.S. jurisdiction).[11] The first step of the compliance process requires the Company and each Subsidiary to screen each new customer[12] and new vendor against the Consolidated Screening List[13] ("CSL List") of restricted parties maintained by the U.S. government before entering into any transaction with such customer or vendor and before approving the conduct of business with such customer or vendor. If it is known or reasonably suspected that a potential new customer or new vendor is or may be related to, controlled by, or is a DBA for an entity or individual on the CSL List, Seaboard is prohibited from transacting any business with such customer or vendor until

[9] For purposes of these procedures, a subsidiary is defined as any entity as to which Seaboard Corporation owns, directly or indirectly, more than a 50 percent equity interest by vote or value; holds a majority of seats on the board of directors of the entity; **or** otherwise controls the actions, policies, or personnel decisions of the entity.

[10] For purposes of these procedures, an affiliate is defined as any entity as to which Seaboard Corporation owns, directly or indirectly, 50 percent or less of the equity interests and which is not otherwise a subsidiary. These Procedures shall apply to an affiliate if such entity is organized under U.S. laws, has U.S. person employees, transacts in USD, or uses U.S. banking institutions. If such criteria or U.S. nexus does not exist, then the board of directors of such affiliate will determine in its own discretion whether to implement the Procedures.

[12] Includes all counter-parties.

[13] See https://www.trade.gov/consolidated-screening-list

such time as the Subsidiary Compliance Officer may approve such transaction. Any hits, matches or findings with respect to the CSL List are to be reported to the Subsidiary Compliance Officer immediately and investigated. The CSL List can be searched at https://www.export.gov/csl-search using a "fuzzy" name search.

If it is determined that additional research into, for example, a new customer or new vendor, before entering into a higher risk transaction is warranted, the Subsidiary Compliance Officer shall be advised, who will direct the screening of such customer or vendor using the Company's more robust OFAC Software Solution (defined below) and/or other screening process and tools as appropriate in the discretion of the Subsidiary Compliance Officer. This first step of the compliance process is intended to ensure that Seaboard does not engage in any type of business relation or transaction that would contravene U.S. government rules and regulations.

The second step of the compliance process requires the Company and/or each Subsidiary to license or purchase a third-party software solution, as determined by each Subsidiary Compliance Officers, and approved by the Seaboard Compliance Officer, that can be used to screen non-U.S. based customers, suppliers, agents, vendors, financial institutions, and other business partners ("Third Parties") against a database consisting of numerous sanctions lists, including the CSL List, and politically exposed persons (an "OFAC Software Solution"). On a periodic basis[14] , the Company and each Subsidiary shall compile one or more files containing all screened customers, banks, vendors, and other business partners in such entity's accounting system (the "Third Party List"). Such files shall be uploaded to the OFAC Software Solution that is used to conduct the screening. A screening report from the OFAC Software Solution shall be reviewed by the Subsidiary Compliance Officer or under his or her direction.[15]

3. Whom to Screen.

The Company, directly and via subsidiaries, engages with Third Parties outside of the U.S. Screening should be conducted on all non-U.S. Third Parties. Results of each screening conducted shall be maintained for a period of five years, with the resolution of potential "hits" documented.

4. When to Screen.

A. Screening should occur before the Company or any Subsidiary enters into any new business relationship or contract/subscription with (or renewals of a contract/subscription), or makes any payments to,[16] a Third Party not already on the Third Party List. All new Third Parties to the transactions must be screened and on a periodic basis thereafter (the frequency of screening shall be determined by each Subsidiary Compliance Officer based on the risk profile of the Subsidiary's business). The Company may not serve as the applicant (i.e., the purchaser of the underlying goods or services) or process transactions under a letter of credit in which any party, including the purchaser's bank providing the letter of credit or any third-party credit provider, is sanctioned. All parties to a letter of credit transaction will be screened.

[14] The frequency shall be determined by the Subsidiary Compliance Officer and approved by the Seaboard Compliance Officer.

[15] It is acceptable to screen Third Parties as to which a relationship is first being established prior to engaging in business and periodically, but not utilizing the two-step process suggested.

[16] Most cross-border payments involve some type of electronic funds transfer (EFT) – typically wire transfers or international ACH.

B. All electronic payments sent to or received from non-U.S. Third Parties, including their banking institutions, should be screened if either sent to, or received from, a high-risk country (see list of high-risk countries in "Sanctions and Anti-Terrorism Compliance Policy") (electronic payments originating with Seaboard should provide a notation regarding the purpose of payment in the memo field).

C. Any changes made to any Third Party's data, such as the name, address, or country ofdomicile, should trigger re-screening.

D. Re-screening of Third Parties should be conducted on a periodic basis with respect to Seaboard Marine, Seaboard Overseas and Trading Group, and Seaboard Foods, TCCB and SERA unless otherwise directed by the Seaboard Compliance Officer.

5. How to Screen.

A. Step 1: Restricted Country Screening:

If the Third Party has an address (billing, shipping, or otherwise) in any comprehensively or near-comprehensively sanctioned country or region (Cuba, Iran, North Korea, Syria, or the Crimea, Donetsk, Luhansk, Kherson, and Zaporizhzhia regions of Ukraine), do not proceed, and contact the Subsidiary Compliance Officer.

If the Third Party is located in Russia or Belarus, the Subsidiary Compliance Officer will direct internet searches, and related due diligence, be conducted for the owners or partial-owners of the Third Party. The Subsidiary Compliance Officer shall at his discretion mandate procedures for other high-risk countries or regions to the extent necessary or appropriate. Such owners and partial-owners will be screened, along with the Third Party, as identified in STEP 2. Under U.S. Sanctions, an entity ownedby a person on OFAC's Specially Designated Nationals and Blocked Persons List (the "SDN List") or Sectoral Sanctions Identifications List ("SSI List") (defined as a direct or indirect ownership interest of 50 percent or more by one or more prohibited parties) is also blocked, regardless of whether that entity is separately named on OFAC's SDN or SSI List.

In the event that the Subsidiary Compliance Officer determines that a transaction should be executed with a Third Party located in a comprehensively sanctioned country or a high-risk country, such as Russia or Belarus, typically because of either an applicable general license issued by OFAC and/or in consultation with external counsel, no such transaction shall be authorized without the express approval of the Subsidiary Compliance Officer and the Seaboard Compliance Officer. Any other financial institution that Seaboard uses to send or receive funds, or that otherwise transacts on its behalf, will be notified in advance of any transactions where such payments involve a restricted country, including the authorization or reasons supporting such payment as compliant with applicable laws and regulations.

B. Step 2: Restricted Party Screening:

- Screen each Third Party against Sanctions Lists. The person conducting screening will go to the following consolidated, restricted party screening lists:

  U.S. Government Consolidated Screening List: CSL Search (trade.gov).

  i. Enter the name of the party for screening into the "Name" field, select "Fuzzy Name" as "On," (leaving all other drop-down options for Address, Sources, and Countries unselected for the initial screen).

  ii. Select "Search" and see if any resulting parties are identified by the search engine, or "No Result" is returned.

- Determine if any "hits" are valid matches:

  A "hit" against a Sanctions Lists includes any potential "match" between a Third Party and a party on a Sanctions Lists that comes back as a result of running that Third Party through screening.

  i. Once you have established that there is a hit against one of the Sanctions Lists, you must evaluate the quality of the hit. Compare the name of the Third Party with the name on the Sanctions List. Is the Third Party an individual while the name on the Sanctions List is a vessel, organization or company (or vice-versa)?

     (a) If yes, you may not have a valid match. For example:

     If the Third Party is a company and the name on the Sanctions List is an individual, double check that the company is valid (i.e., look for a website or address online) and that the Third Party did not provide an individual's name as a company name.

     (b) If the Third Party is an individual, but the name on the Sanctions List is a company, confirm that the sanctioned company is not also owned or controlled by a sanctioned individual of the same name.

     (c) If no, please continue to ii below.

  ii. How much of the listed entity's name is matching against the name of the Third Party? Is just one of two or more names matching (i.e., just the last name)?

     (a) If yes, you may not have a valid match. For example:

     If the sanctioned person is John Smith and the Third Party is Bill Smith, this is not likely a valid match.

     (b) If no, please continue to iii below.

iii. Compare the complete Sanctions List entry with all of the information you have on the matching Third Party. An entry often will have, for example, a full name, address,nationality,passport, tax ID or cellular number, place of birth, date of birth, former names, and aliases.

(a) If multiple parts of the name match but you are missing information, continue to (b) below. For example:

- If the sanctioned person is John Paul Smith and the Third Party is John Smith (with no middle name provided), you need more information before determining whether there is a valid match.

- For companies with similar but not quite matching names (i.e., Apple Inc. and Apple Computers Inc.), continue to (b) below to verify the companies are different.

(b) If no, consider whether there is information regarding the Third Party that differs from the sanctioned party. For example:

- Was the sanctioned individual born in 1965 and the Third Party was born in 1985? If so, you likely do not have a valid match.

- For entities, verify whether the street address or country location is different for the sanctioned company and the counterparty. For example: If the sanctioned company and the Third Party are at different locations, you likely do not have a valid match.

iv. If you do not find clearly different information between the sanctioned party and the Third Party, please continue to v below.

v. Are there a number of similarities or exact matches?

(a) If yes, please contact the Subsidiary Compliance Officer.

- Any indication that a Third Party may be a sanctioned person shouldbe reported within 24 hours to the Subsidiary Compliance Officer.

- The Company may not proceed with any business, directly or indirectly, with such a Third Party until the potential match is "cleared."

- If the Third Party cannot be cleared because it is in fact on a SanctionsList, or is subject to sanctions through ownership by persons or entities on a Sanctions List, <u>do not proceed with the transaction without the express permission of the Subsidiary Compliance Officer</u>.

(b) If no, you do not have a valid match. Any uncertainty regarding a possible match should raised with the Subsidiary Compliance Officer.

- Resolving possible matches.

  When warranted, the Subsidiary Compliance Officer will conduct a further review to determine whether there is a valid match. As noted above, no business may be conducted with a Third Party before the Subsidiary Compliance Officer has confirmed that any possible hits have been "cleared."

  The employee reviewing a potential match is responsible for creating and maintaining records of all screenings conducted and all activities undertaken to "clear" potential matches. This can be done using the template provided at Appendix A below or may be done through use of a clearing notice or explanation in the OFAC Software Solution (so long as the record can be retained and accessed for five years). As set forth in the Sanctions and Anti-TerrorismPolicy, all records will be maintained for a period of five years. This policy includes the retention of any requests from the Company's banks to provide additional information in connection with their sanctions compliance evaluation of specified transactions.

6. Questions?

If you have any questions about these Procedures (or the Sanctions and Anti-Terrorism Policy), please contact your Subsidiary Compliance Officer or the Seaboard Compliance Officer.

APPENDIX A - RECORD OF RESTRICTED PARTY SCREENING CLEARANCE

Third Party Counter-party (or other transactional/contractual party) **Name:**		
Name of Sanctioned Party Match:		
Restricted Party Cleared?	Yes □	No □
Reason for Clearance:		
Different Type of Party (explain difference, i.e., counterparty is an individual while sanctioned party match is an entity or vessel, and provide supporting websites or documentation):		
Different Address (provide the addresses):		
Different Date of Birth (provide the dates of birth):		
Other Reason (please explain, i.e., different industry):		

Reviewing Employee Name:	**Employee Signature:**	**Review Date:**

Referred to the Subsidiary Compliance Officer: Yes □ No □

If yes, have the Subsidiary Compliance Officer complete the below.

Subsidiary Compliance Officer Signature:	**Review Date:**	**Comments:**

***The Company will retain this form for five years from the latest review date above.*

ANTI-CORRUPTION POLICY

INTRODUCTION

Policy Summary

It is the policy of Seaboard Corporation and all of its subsidiaries (together "Seaboard" or the "Company") to comply with all applicable laws related to the prevention of bribery and corruption, including the U.S. Foreign Corrupt Practices Act of 1977, as amended (the "FCPA" and, collectively, "Anti-Corruption Laws"). This Anti-Corruption Compliance Policy (this "Policy") will assist Employees (as defined below) in complying with Anti-Corruption Laws.

In accordance with Anti-Corruption laws, this Policy prohibits all directors, officers, and employees of the Company (collectively, "Employees") and third-party business partners acting on behalf of the Company with government officials (with Employees, "Covered Persons") from:

- giving, offering, or promising anything of value, directly or indirectly, to any government official or any commercial party for the purpose of improperly obtaining or retaining a business advantage;
- entertaining requests or demands from any person for improper payments, including soliciting, receiving, offering, or paying remuneration (including any kickback, bribe, or rebate) for referrals for business; and
- soliciting, agreeing to receive, or accepting anything of value for any purpose.

The FCPA provides a narrow exception for "facilitation" or "expediting" payments," which are payments made in furtherance of a routine governmental action that involves non-discretionary acts. Although true facilitation payments are not illegal under the FCPA, they are illegal in many countries. This Policy allows facilitation or expediting payments only when lawful.

If confronted with a request or demand for an improper payment or other violation of this Policy, Covered Persons must immediately reject the request or demand and report it to the applicable Division General Counsel ("Division General Counsel"). For Seaboard Marine, Steve Irick, (305) 863-4477, for Seaboard Overseas and Trading Group, Hinton Johnson, (913) 304-3627, for Seaboard Foods, James Hubler, (913) 217-6062, or alternatively to the Company's Chief Compliance Officer ("CCO"), Zach Holden, (913) 676-8939, or the Company's General Counsel (the "General Counsel") David Becker, (913) 676-8925. Similarly, if any Covered Person knows or believes that an improper payment has been or will be made, the Covered Person must also report such payment to the Division General Counsel, CCO or General Counsel.

Failure to comply with Anti-Corruption Laws or this Policy may result in:

- severe civil, regulatory, and/or criminal penalties for the Company and for individuals involved in making prohibited payments or with prior knowledge of such payments;
- serious public relations and reputational concerns for the Company and individuals involved; and
- disciplinary action by Seaboard, including termination of employment.

The DOJ/SEC FCPA Resource Guide can be found at the following website link:

http://www.justice.gov/criminal/fraud/fcpa/guidance/.

If there is any question about whether a particular activity or transaction is permitted under Anti-Corruption Laws, consult with the applicable Division General Counsel or if the applicable Division doesn't have a General Counsel, the CCO or the Company's General Counsel.

Worldwide Application

This Policy applies to all directors, officers and employees of the Company, including all consolidated subsidiaries, whether domestic or foreign (*see* definitions of "Employees" and "Covered Persons" above). Employees must use reasonable efforts to ensure that third parties representing the Company adhere to the principles expressed in this Policy.

It is the policy of the Company to comply with all laws and regulations applicable to it in any jurisdiction in which it has operations or otherwise conducts business, including all local laws. Covered Persons in foreign jurisdictions should be aware of any applicable local laws and are required to follow the more restrictive anti-bribery laws (for instance, in the United Kingdom).

From time to time, Seaboard may revise or issue supplements to this Policy.

Other Company Policies

Except as specified below, this Policy does not limit, and shall not be construed to limit, any other Company policies, including the Code of Ethics Policy.

Application of Policy to Affiliated Companies

The Company also will use good faith efforts to cause affiliates, which are not consolidated subsidiaries of the Company (i.e., companies as to which the Company has 50 percent or less voting power and thus are "affiliates" or "Affiliated Companies"), to devise and maintain a system of internal accounting controls consistent with the Company's obligations under Anti-Corruption Laws.

Policy Statement

The Company does not permit or condone bribes, kickbacks or other improper payments, transfers or receipts.

That means:

- Covered Persons cannot give—or offer to give—anything of value to a government official in exchange for receiving an improper business advantage.

- In the same way, Covered Persons cannot receive—or ask to receive—anything of value in exchange for providing an improper business advantage.

- A bribe does not have to be completed. Simply promising to give a bribe or agreeing to receive one is prohibited.

- In addition, Employees cannot use a third-party, intermediary, or "middleman" to participate in bribes, kickbacks, or improper conduct. Even if done indirectly or through someone or some entity outside of Seaboard, it is still prohibited to offer, request, give, or receive anything of value in exchange for an improper business advantage—no matter who actually conducts the activity. This includes:

    i. Outside vendors or business partners (i.e., consultants, distributors, agents, etc.);

    ii. Close relatives (spouse; the individual's and the spouse's grandparents, parents, siblings, children, nieces, nephews, aunts, uncles, and the spouse of any of these people; or anyone who shares the same household);

    iii. Close friends, associates or business partners;

    iv. A company in which the individual has a direct or indirect ownership interest; and

    v. An organization with which the individual is associated (i.e., a charity).

The prohibition against bribery applies to anyone who can provide an improper advantage, including government officials, persons working in the private sector, and Employees.

What is "Bribery"?

"Bribery" means offering, providing or receiving anything of value with the intent of improperly influencing any person to take an action to obtain an improper business advantage. This includes, for example, improper influence over:

- the decision whether to accept an application, official form, or any other type of paperwork;
- the grant or revocation of regulatory approvals, such as product registrations, permits, licenses, certifications, or any other award which allows the recipient to undertake a specified activity;
- the award of a commercial tender, procurement or sales contract;
- the decision to enforce, or not enforce, a particular law or regulation against a company or individual;
- the decision to enforce, or not enforce, contractual terms;
- the decision to require, or not require, a payment to be made or how much is to be paid (i.e., taxes); and
- the sponsoring or approval of a change in existing law.

What is "Anything of Value"?

"Anything of value" broadly includes any type of benefit to the recipient, such as:

- money (all currencies including bitcoin, and method of delivery such as cash, check, wire, electronic, mobile transfer);
- cash equivalents such as gift, store, discount, mobile phone, or stored value cards;
- loans;

- gifts;
- meals, entertainment, and other hospitality;
- travel, including flights and accommodation;
- offers of employment or an internship;
- a contract for the procurement or sale of goods or services;
- a contract for the procurement, sale, or lease of property;
- a charitable donation or contribution to a community project;
- a political contribution to any government official;
- a commercial sponsorship;
- confidential information;
- investment opportunity; and
- any other form of personal favor.

Who is a "Government Official"?

"Government official" is defined broadly, and can include:

- an officer, employee or anyone acting on behalf of any government body including a department or agency at any level (national, regional, or local). Examples include a government minister, regulator, judge, city mayor, police officer, soldier, and customs official;

- an employee of state-owned or controlled enterprises;

- an employee of public international organizations such as the United Nations and World Bank;

- a political party, party official or candidate for political office; and

- a person holding an appointment, position, or office created by custom or convention, such as an Indigenous community leader or member of a royal family.

Gifts and Entertainment

All Covered Persons must exercise caution when providing gifts, travel, or entertainment of any kind, or receiving the same from customers, vendors, agents, and other business partners, and consult the Division General Counsel, the CCO or General Counsel with any questions regarding the appropriateness of an activity or offering.

Provision of Gifts. The use of Company funds or assets for gifts, gratuities, or other favors to government officials or any other individual or entity (in the private or public sector) that has the power to decide or influence the Company's commercial activities is prohibited, unless all of the following circumstances are met:

- the gift is permitted under both local law and the guidelines of the recipient's employer;
- the gift is presented openly and with complete transparency;
- the gift is properly recorded in the Company's books and records;
- the gift does not involve cash or cash equivalents;
- the gift is provided as a token of esteem, as a courtesy, or in return for hospitality, and is consistent with local custom; and
- the item has no more than a nominal or inconsequential value.

Gifts that do not fall specifically within the above guidelines must be approved in advance by the Division General Counsel, the CCO or General Counsel.

Receipt of Gifts. Covered Persons must also not accept or permit any family members to accept, any gifts, gratuities, or other favors from any customer, supplier, or other person doing or seeking to do business with the Company, other than items of nominal value. Any gifts that are not of nominal value should be returned immediately and reported to the Division General Counsel, the CCO or General Counsel. If immediate return is not practical, such gifts should be given to the Company for charitable disposition.

Meals, Entertainment, Travel, and Lodging. The Company prohibits Covered Persons from offering meals, entertainment, travel, and lodging as a means of influencing another person's business decision. Expenses for meals, entertainment, travel, and lodging for government officials or any other individual or entity (in the private or public sector) that has the power to decide or influence the Company's commercial activities may be incurred without prior approval by the Division General Counsel, the CCO or General Counsel only if all of the following conditions are met:

- The expenses are bona fide and directly related to a legitimate business purpose (such as promotion of products) and the events involved are attended by appropriate Company representatives;
- The cost of the meal, entertainment, travel, or lodging is of reasonable value; and
- The meal, entertainment, travel, or lodging is permitted by the rules of the recipient's employer (if applicable).

All expense reimbursements must be supported by receipts, and expenses and approvals must be accurately and completely recorded in the Company's records.

Political Contributions and Charitable Donations

Covered Persons may not make political or charitable donations, whether in their own name or in the name of the Company, to obtain or retain business or to gain an improper business advantage. Any political or charitable contributions by the Company must be permitted under the law, permissible pursuant to the terms of this Policy, made to a bona fide organization, and, in the case of political contributions or charitable contributions connected to any government official or government entity, made with the prior approval of the Division General Counsel, the CCO or General Counsel.

Facilitation Payments

"Facilitation" or "expediting" payments are payments made in furtherance of a routine governmental action that involves non-discretionary acts. For example, obtaining routinely issued permits, licenses or other official documents, expediting lawful customs clearances, obtaining entry or exit visas, obtaining security through police or military protection, mail pick-up and delivery, providing phone service and performing actions that are wholly unconnected to the award of new business or the continuation of prior business or provide a commercial advantage.

Although true facilitation payments may be legal under certain circumstances under the FCPA, they are illegal in many countries and can open the door to more serious corruption issues. In other countries, it may be the local business practice to make small, nominal payments to low-level foreign public officials to facilitate or expedite a routine government action. With limited exception, the Company strongly discourages Covered Persons from making any facilitation payments and any such facilitation payments should only be made to foreign officials for the following purposes:

- To expedite the granting of a permit or license that you are otherwise entitled to receive;

- Processing government papers, such as visas and work orders;

- Providing telephone service, power, and water supply, loading and unloading cargo, or protecting perishable products or commodities from deterioration; or

- To expedite or ensure the provision of standard government and quasi-government services such as police and military protection, mail services, utility services and other government services generally provided by the government to similar businesses.

Routine government action does not include, among other actions, any decision by a foreign official whether, or on what terms, to award new business to or to continue business with the Company, or any action taken by a foreign official involved in the decision-making process to encourage a decision to award new business to, or continue business with, the Company. Extreme caution should be used when determining whether a payment fits within the facilitation exception; as such, if there is any question regarding the propriety of a facilitation payment please consult with the Division General Counsel, the CCO or General Counsel.

All facilitation payments must be accurately documented and appropriately reflected in the Company's books and records. The documentation should include the amount, recipient, and a specific explanation of the reason for the payment.

Indirect Payments

Payments that are prohibited from being made directly under this Policy are also prohibited from being made indirectly through a third party. Thus, Employees cannot pay a third party if they know or should know that any portion of the payment is reasonably likely to be used in a way that would violate this Policy or Anti-Corruption Laws. See "*Procedures for Dealing with Third Parties*" below for additional information.

Emergency Health and Safety Payments

This Policy does *not* prohibit payments made to avoid a risk to an individual's health or safety; provided, the payment must be fully and correctly recorded in the books and records of the Company so that there is the ability to timely show the amount of all payments made during a given time period, the purpose, to whom the payment was made, and proper accounting classification.

Procedures for Dealing with Third Parties

Certain arrangements with and payments by the Company or Employees to consultants, contractors, advisors (including certain financial advisors, legal advisors and accountants), partners (including joint venture partners), agents, distributors, and other representatives and intermediaries of the Company (collectively, "*Third Parties*") may violate Anti-Corruption Laws and subject the Company and Employees to liability and/or reputational harm. Consequently, no Third Party should be retained, unless appropriate due diligence has been conducted with respect to the business and reputation of the Third Party.

Prior to the engagement of a Third Party, appropriate due diligence should be conducted on the Third Party's business, ownership and reputation, including its Anti-Corruption policies, practices and compliance.

The appropriateness and extent of the due diligence will vary depending on the totality of the circumstances. For example, more careful due diligence may be required for Third Parties that (i) will interact with government officials on the Company's behalf; (ii) are not well known or not subject to rigorous regulatory oversight or (iii) are located in a country that has a reputation for widespread government corruption (i.e., jurisdictions that score low on various "corruption perception" indices such as the corruption index published by Transparency International at www.transparency.org).

The Company may be liable for improper payments and actions by Third Parties, and must therefore take reasonable precautions to ensure that Third Parties conduct business ethically and comply with this Policy. To the extent the Company engages with non-U.S. Third Parties, the Company will employ appropriate procedures to mitigate risk of noncompliance by such Third Parties, such as performing due diligence and including language regarding compliance with anti-corruption laws in written agreements as warranted.

Any third-party agent relationship which involves interaction with government officials on the Company's behalf will be subject to additional scrutiny and must be approved in advance and in writing by the Division General Counsel, the CCO or General Counsel.

Procedures for Joint Ventures

Before entering into a joint venture, partnership or similar arrangement (any such arrangement, a "*Joint Venture*"), appropriate due diligence should be conducted on the Joint Venture partner, and reasonable efforts must be undertaken to include in written agreements with such Third Party appropriate provisions with respect to Anti-Corruption compliance.

In addition, management of the Joint Venture must take appropriate steps to ensure that the Joint Venture complies with Anti-Corruption Laws and adopts and abides by Anti-Corruption policies and practices that are appropriate to the business, including implementing and maintaining appropriate internal controls and compliance systems and providing Anti-Corruption training to employees, as appropriate.

Documentation and Records

All payments made by the Company or Covered Persons to or for the benefit of any government official (including cash payments, gifts, payment of meal, travel, lodging or entertainment expenses, charitable contributions, political contributions, or otherwise) must be accurately documented in reasonable detail and reported in the Company's books, records and accounting systems.

Recordkeeping And Internal Controls

The Company requires that all expenditures made by the Company are accurately reflected in the Company's financial records and that all payments made with Company funds, or on behalf of the Company, have been properly authorized. Covered Persons must follow all applicable standards, principles, laws, and practices for accounting and financial reporting. Employees should use best efforts to ensure that all transactions, dispositions, and payments involving Company funds or assets are properly and accurately recorded in the Company's financial records. Third Parties are responsible for ensuring that all invoices submitted to the Company contain sufficient detail and supporting documentation to allow for proper and accurate recording in the Company's financial records.

The General Counsel, and each Division General Counsel with respect to its Division, has primary responsibility for overseeing this Policy and its implementation and execution. The General Counsel, the CCO and each Division General Counsel will maintain the standards described in this Policy and will establish additional processes and guidelines as necessary. The General Counsel, the CCO and each Division General Counsel may also utilize legal counsel to further ensure compliance with applicable Anti-Corruption Laws and this Policy. The General Counsel,

the CCO and each Division General Counsel, in cooperation with legal counsel (where applicable), will review and approve any matters to the extent required by this Policy.

Dissemination of Policy Certification and Training

This Policy shall be disseminated to each Director and Officer of the Company, each salaried employee of the Company working in accounting, internal audit or finance, and each employee of the Company holding the position of "manager" or higher. These persons will be requested annually to sign a certification as to compliance with the principles underlying this Policy in the form of Annex A hereto. The Human Resources department is responsible for collecting such certifications. All signed certifications should be forwarded to the Company's Human Resources Department or the relevant Division's Human Resources Department for record retention purposes.

In addition, certain employees of the Company will periodically be requested to receive Anti-Corruption training. The Human Resources Department will oversee communications with, and periodic training (as warranted) of, relevant Covered Persons on processes and requirements documented in this Policy. The Human Resources Departments for the Company and each Division, in consultation with the Company's General Counsel, CCO or Division General Counsel, shall compile a list of employees of the Company to receive training, which shall include, at a minimum, the directors and officers of the Company, the General Manager and Financial Director at each foreign office of the Company, and those employees of the Company who may have reason to interact with any foreign government official in the performance of their duties.

The Human Resources Departments for each Division, in consultation with the Division General Counsel, shall also compile a list of the Affiliated Companies as to which this Policy shall be disseminated, and the employees at each such Affiliated Company that the Company should endeavor to sign a certification as to compliance with the Policy and to receive Anti-Corruption training.

Identifying and Reporting Violations

Any activity that violates, is believed to violate, or is reasonably expected to violate, Anti-Corruption Laws or this Policy shall be reported to the applicable Division General Counsel, the CCO or the General Counsel. Alternatively, the matter may be reported online by visiting www.seaboard.ethicspoint.com; by calling the Company's dedicated toll free number, 866-676-8886, for calls originating from the United States; or by calling the applicable phone number associated with the specific country, as set forth at the aforementioned website, for international calls. Matters also may be emailed to SBD_Ethics@seaboardcorp.com. Any question regarding a particular transaction, the engagement of a particular Third Party, or the application or interpretation of this Policy should be directed to the applicable Division General Counsel, the CCO or the General Counsel.

The Company will undertake to protect the confidentiality of any such report or question, subject to any applicable laws, regulations and legal proceedings. Retaliation against any Company employee who reports a violation or potential violation of this Policy is strictly prohibited and any such retaliation will be cause for corrective action, including termination of employment.

****

If you have any questions or concerns about these procedures, promptly contact the applicable Division General Counsel, the CCO or the Company's General Counsel.