

THE
BUMBLE BEE[®]
SEAFOOD COMPANY

Code of Conduct - 2023



ANOVA

BUMBLE BEE[®]
SEAFOODS

Beach Cliff[®]



BRUNSWICK[®]


Code of Conduct – 2023

Compliance Department

CEO STATEMENT:

This is the Bumble Bee Code of Conduct.

It can inform you of the basic expectations we have of our Team Members.

It cannot take the place of applying good judgement and acting with integrity.

We are a company where character counts. Thank you for showing up in the right ways.

~Jerry Chou, CEO

CONTENTS:

ABOUT THE CODE OF CONDUCT

Introduction to the *Code of Conduct*

Responsibilities of our leaders

Responsibilities of all Team Members

Investigations of Business Conduct Concerns Guidance

ENVIRONMENT, HEALTH AND SAFETY

Health and Safety

Weapons-free Workplace

Protecting the Environment

COMPLIANCE WITH THE LAW

Anti-Bribery

Antitrust and Competition Law

Anti-Money Laundering

Import-Export Law

Supply Chain Security

**Human Rights, Forced Labor, and Human Trafficking
Advertising and Labeling**

TEAM MEMBER INTERACTIONS

RECORDS, REPORTS, CONTRACTS, AND AUDITS

**Records and Reports
Responsibilities of Financial Officers
Approving records and signing contracts
Responsibilities Concerning Audits**

PERSONAL RESPONSIBILITIES

**Conflicts of Interest
Gifts, Meals, Entertainment, and Travel
Outside Businesses and Activities
Political Activities and Charitable Organizations**

PRIVACY

Privacy and Personal Information

COMPANY INFORMATION AND PROPERTY

**Protecting Company Information
Protection and Use of Company Property
Email, Internet, Telephones, Cellular Phones, and Voicemail
Personal Use of Company Property**

COMMUNICATIONS

**Business Communications
Business Emails
Public Statements**

ABOUT THE CODE OF CONDUCT

Introduction to the *Code of Conduct*

Our *Code of Conduct* (or “*Code*”) is a guide that contains the basic rules for how to do business both legally and ethically with our consumers, business partners, and one another.

Our *Code* is for the Team Members of Bumble Bee Foods, LLC, Clover Leaf Seafoods Corp., Connors Bros. Marine Corp., Anova Holding Company (parent of CTS, ATS and PT Seafood and PT Asindo) and their subsidiaries. Our *Code* refers to these businesses as the “Company.”

Our *Code* may also apply to others who act on behalf of the Company—for example, consultants and business partners.

Responsibilities of our leaders

A leader is anyone in our Company who occupies a position of trust and manages other Team Members. In any organization, leaders set the tone of behavior that others follow. This is referred to as the “Tone at the Top.” Leaders must set a positive “Tone at the Top” by ensuring that what they do conforms to our *Code of Conduct*, the law, regulations, and Company policies.

Leaders must encourage Team Members to voice business conduct questions or concerns.

Leaders must never retaliate against any Team Member for raising concerns in good faith. Examples of retaliation include:

- Taking an adverse action against a Team Member—for example, a transfer to a less desirable position, or assigning an undeserved low performance rating.
- Denying a benefit—for example, purposefully denying a request for training.
- Shunning or socially ostracizing a Team Member.
- Attempting to identify a Team Member who anonymously submitted a business conduct concern.

Responsibilities of all Team Members

All Team Members must:

- Read and abide by our *Code of Conduct*.
- Be familiar with the laws, regulations, rules, and policies under which they operate.
- When directed, review our *Code* and Company policies through PolicyTech – the Company’s online policy management system.
- When in doubt, ask business conduct questions.
- Timely report business conduct concerns. When in doubt of whether or not to report a concern, Team Members must always err on the side of reporting.
- Never retaliate against another for raising good faith questions or concerns.
- Fully cooperate with Company investigations.

Investigations of Business Conduct Concerns

The Chief Compliance Officer, management, or both, will evaluate reported business conduct concerns, and will conduct investigations when appropriate.

After the investigation concludes, our management will take action to resolve any proven allegations. If an investigation shows that the law, regulations, *Code of Conduct*, or Company policy was violated, a Disciplinary Committee will determine what – if any – sanctions should be imposed. The Committee will consider the nature of the conduct, the facts that support any violations, and all mitigating factors. The Committee will then forward its findings to the decision-maker for resolution.

Significant violations of our *Code* can have severe consequences—up to and including termination of employment.

The Company will keep investigations as confidential as possible. Reasons to disclose information learned during an investigation include defending Company personnel actions, complying with legal demands for information (for example, a subpoena or discovery request), and demonstrating to the reporter of a concern or regulator that a matter was promptly and thoroughly investigated.

Refer to our *Disciplinary Policy* for more information.

Guidance

Business conduct issues may be complicated, and our *Code of Conduct* and policies may not provide a clear answer. If confronted with a business conduct issue, a good starting point is to ask,

“What’s the right thing to do?”

If still unsure, it’s time to ask questions.

Team Members should seek advice from management, Human Resources, the General Counsel, or the Chief Compliance Officer.

Team Members may also seek guidance through EthicsPoint, an independent professional reporting service retained by our Company. Questions and concerns may be submitted online or by phone anonymously if they choose. EthicsPoint may be accessed online at:

- www.bumblebee.ethicspoint.com
- The [People Hub \(navexone.com\)](http://navexone.com)
- The Compliance page on the Fishbowl

Refer to our *Report a Concern Policy* for more information.

ENVIRONMENT, HEALTH AND SAFETY

Health and Safety

The safety and well-being of our Team Members is the Company’s first priority.

Team Members must:

- Be familiar with the environmental, health, and safety policies at their respective employment sites.
- Report workplace safety concerns to management so that they may be remedied as soon as possible.
- Immediately report workplace injuries to management.

Weapons-free Workplace

Good judgement must be applied to bringing items unrelated to work into the workplace. Bumble Bee prohibits bringing into any work premises materials that pose a reasonable threat or significant distraction to our Team Members.

To ensure a safe environment for Team Members and visitors, the Company prohibits the carrying, transporting, storage, or presence of firearms, other weapons, or ammunition in our facilities or on our property.

Possession of a valid concealed weapons permit is not an exemption to this rule.

This rule does not apply to law enforcement personnel engaged in official duties on Company premises.

Protecting the Environment

Protecting the environment is a Company priority. To prevent harm to the environment, Team Members must immediately report any known breach of our Company's environmental standards to management.

Team Members must never knowingly harm the environment.

Team Members should use our Company-provided recycling containers at its facilities.

COMPLIANCE WITH THE LAW

Anti-Bribery

Bribery is illegal. Team Members may not pay, offer, or solicit bribes or kickbacks – no matter how small – for any reason. Bribes include money or anything of value.

Team Members must never offer or accept money or anything of value from any government official or employee. Violation of certain laws – for example, the United States Foreign Corrupt Practices Act and the Canadian Corruption of Foreign Public Officials Act – may result prison sentences and fines against individuals and significant fines against companies.

Team Members must never make a “facilitation payment” – that is, giving a small amount of money or anything of value to a government official to perform, or expedite performance of an existing duty.

Refer to our *Anti-Bribery Policy* for more information.

Antitrust and Competition Law

Antitrust and competition laws promote fair competition to ultimately benefit consumers. The law strictly forbids any agreements that unreasonably restrain trade. This includes agreeing with competitors to:

- Fix prices
- Cease doing business with a particular customer
- Allocate customers
- Allocate territories

Violation of antitrust and competition laws may result prison sentences and fines against individuals and significant fines against companies.

Refer to our *Antitrust and Competition Law Policy* and our *Competition Contact Reporting Policy* for more information.

Anti-Money Laundering

Money laundering means hiding the source of illegally obtained money. It is illegal. Criminals typically “launder” illegally obtained money through banks and businesses.

Our Company is committed to assisting government agencies to prevent money laundering.

Team Members – particularly those involved in financial transactions and processing – must be vigilant of suspicious financial activity and ensure that all of our business is conducted with legitimately derived funds. Team Members must timely report suspicious activity to our managers, the General Counsel, or the Chief Compliance Officer.

Import-Export Law

Our Company imports raw materials, ingredients, and finished goods, and exports finished products as well. Team Members whose duties may involve international sourcing, production, or distribution must coordinate with the Import Department to ensure compliance with all trade laws and regulations.

Supply Chain Security

In 2001, the United States Department of Homeland Security, Customs and Border Protection, began its Customs Trade Partnership Against Terrorism – or “CTPAT” – program. The purpose of CTPAT is to improve United States border security and strengthen international supply chains through collaboration between the United States Customs and Border Protection and businesses. As an active participant in the CTPAT program, the Company requires suppliers to:

- Maintain adequate security at all facilities and have supply chain security procedures that prevent the shipment of contraband into the United States – including illegal drugs, explosives, and chemical or bio-hazardous materials.
- Maintain written security procedures and proof of adequate controls to prevent the storage or shipment of contraband.
- State the country of origin on goods, packaging, bills of lading, and invoices.

The Chief Compliance Officer is responsible for the Company participation in the CTPAT program. Any suspected breach of supply chain security should be promptly reported to the Chief Compliance Officer, Legal, or management.

Human Rights, Forced Labor, and Human Trafficking

The Company follows the principles of the United Nations Universal Declaration of Human Rights. In keeping with this declaration, the Company is committed to preventing the use of any slave labor, prison labor, child labor, or human trafficking in its supply chain.

The Company Sustainability Department proactively manages potential human rights impacts under its due diligence program. To that end, Team Members must report any suspicion of any activity impacting human rights at once to management, the Vice President of Sustainability and Resourcing, the General Counsel, or the Chief Compliance Officer.

Refer to our *Supplier Code of Conduct* and the *United Nations Universal Declaration of Human Rights* at https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf for more information.

Advertising and Labeling

Customers and consumers expect our ads and product labels to be accurate. Our Company's statements about our products must be true and correct, and conform with all applicable laws, rules, and regulations. Product representations – on labels or in any type of communication – must be truthful, accurate, and based on scientifically accepted testing procedures.

TEAM MEMBER RELATIONS

Our individual diverse perspectives make us stronger and enable us to achieve our Company goals. Team Members must therefore respect, appreciate, and value individual differences, and treat one another with dignity and respect.

Hiring, supervision, work assignments, compensation, and promotion must be based on an individual's demonstrated abilities and potential, but never on age, race, color, religion, creed, gender, national origin, citizenship, language, political belief, marital or family status, pregnancy or childbirth, sexual orientation, or disability.

“Workplace harassment” and “bullying” are defined below and are disallowed.

- “Workplace harassment” is broadly defined as unwanted behavior that a reasonable person would consider abusive. It includes “quid pro quo” and hostile work environment sexual harassment.
- “Bullying” is described as one or more people repeatedly and intentionally causing hurt, humiliation, or harm to another person or group of people who feel helpless to respond. Bullying is not a single episode of social rejection, nastiness, or spite, or a random act of aggression, a mutual argument, or disagreement

Refer to our *Harassment and Retaliation Policy* and *Anti-Discrimination Policy* for more information.

RECORDS, REPORTS, CONTRACTS, AND AUDITS Records and Reports

Our Company must maintain complete and accurate business records—particularly those that it publicly files. Team Members must ensure that Company books and records for which we are responsible accurately reflect our business transactions in accordance with the law, applicable regulations and accounting principles, and Company policy.

Team Members must be familiar with the Company's *Records Management Policy*, and follow all directives from the Information Technology Department, General Counsel, or Chief Compliance Officer to retain documents—including emails and documents in electronic storage.

Team Members must never:

- Falsify any record.
- Withhold any information from the accounting department.
- Maliciously destroy any record.

Refer to our *Records Management Policy* for more information.

Responsibilities of Financial Officers

Our Financial Officers include the Chief Executive Officer, Deputy Chief Executive Officer, Finance Vice President, Controller, Treasurer, and any other management-level Team Members performing duties involving finance and accounting.

Financial Officers must provide information that is accurate, complete, objective, relevant, timely, and understandable. Financial Officers must comply with all applicable governmental laws, rules and regulations, and—where applicable—generally accepted accounting principles.

Approving records and signing contracts

When Team Members approve any Company contract, document, expense, or time and attendance entry, they certify its accuracy.

Only authorized personnel may contractually bind our Company—either orally or in writing.

A “higher level of review” is required for all travel expenses, corporate credit card expenses, time and attendance, and relocation expenses.

“Self-approval” of a corporate credit card expense, purchase order, or time and attendance entry is not permitted.

Refer to our *Contract Signing Authority Policy* and *Corporate Credit Card Policy* for more information.

Responsibilities Concerning Audits

Audits are helpful tools for our Company. They assist in ensuring that we are recording our business activities accurately and show us how to improve. An audit serves as a mirror check to see what we are doing right, and how we can do better.

Our Company routinely engages independent auditors to examine our books and records. Also, an internal auditor may examine several functions, including – for example – travel and corporate credit card expenses.

To ensure accuracy and completeness in the audit process, Team Members must cooperate with our Company’s accounting department, independent auditors, and any internal auditor, and fully respond to their questions.

PERSONAL RESPONSIBILITIES

Conflicts of Interest

We owe our primary business loyalty to our Company. We must avoid any relationship – financial or otherwise – that would cause our loyalty to be questioned. A simple definition of a conflict of interest is “divided loyalty.” We must also avoid circumstances that would show a perceived conflict of interest – even if a real conflict of interest does not exist.

Conflicts of interest appear in many forms. For example, a conflict of interest may exist if a member of a Team Member’s family has a financial interest in a competitor or business partner, or a Team Member wants to hire a friend.

A conflict of interest may impair a Team Member’s ability to make objective decisions on behalf of our Company and may have legal and regulatory consequences. A conflict may also affect our Company’s business reputation, as well as the morale of our fellow Team Members.

Having a conflict of interest is not necessarily wrong. In most instances, our Company can make adjustments to address a conflict. But to address a conflict, the Company must be aware of it. So, upon learning of an actual, potential, or perceived conflict of interest, Team Members must promptly report it to the Chief Compliance Officer, or through Conflict of Interest Reporting System.

Refer to our *Conflict of Interest Policy* for more information.

Gifts, Meals, Entertainment, and Travel

If reasonable under the circumstances, and if reasonable in value, providing or receiving gifts, meals, entertainment, and business travel is acceptable.

A key in determining whether a gift, meal, entertainment, or cost of travel is unreasonable is whether it can be viewed as being given with “corrupt intent” – that is, an ulterior unlawful motive.

Here are some scenarios that Team Members must avoid:

- Providing a gift, meal, or entertainment that is – or may be perceived to be as inappropriately high in value.
- Frequently providing or receiving gifts, meals, and entertainment from the same third party.

- Providing expensive gifts, meals, and entertainment close in time to contract negotiations or any other significant business event.
- Providing gifts, meals, entertainment, or travel to a government official or employee without first consulting with the General Counsel and Chief Compliance Officer.
- Failing to report providing or receiving business gifts, meals, or entertainment above the minimum threshold level.

Refer to our *Gifts, Meals, and Entertainment Policy*; *Travel Policy*; *Corporate Credit Card Policy*; and *Anti-Bribery Policy* for more information.

Outside Businesses and Activities

Team Members must not accept outside positions in any organization or another business that takes away from the time, attention, and business judgment required to perform our Company duties.

Team Members who are or wish to become an officer of a trade organization must report their status in these organizations using the Company's Conflict of Interest Reporting System.

Refer to our *Conflict of Interest Policy* for more information.

Political Activities and Charitable Organizations

Team Members are free to donate their own time and money to political and charitable organizations of their choice.

The Company's Corporate Giving Committee must review all Company charitable contributions to ensure that giving is in line with our Company's charitable targets and goals.

Because in rare circumstances a charitable contribution may be disguised as a bribe, we must ensure that contributions are aligned with our *Anti-Bribery Policy*.

Refer to our *Anti-Bribery Policy* for more information.

PRIVACY

Privacy and Personal Information

“Personal Information” and is protected under domestic and international privacy laws. Personal Information includes any information that would tend to identify a particular person – for example, names, addresses, zip codes, email addresses, IP addresses, telephone numbers, and birth dates. Some jurisdictions – for example, California – go further and attach even more importance to categories defined as “Sensitive Personal Information.”

Our Company has *Privacy Policies* for the United States as well as Canada. The Company also has a *Privacy Policy for Team Members and Applicants for Employment* for the United States. These policies contain information on information our Company collects, and how it is collected, used, disclosed, and safeguarded.

Team Members must be familiar with the specific *Privacy Policies* that affect their business location.

As with confidential information, Team Members must protect Personal Information and – where appropriate – Sensitive Personal Information – in the Company’s possession.

Questions on the collection, use, disclosure, or storage of Company information should be directed to the Chief Compliance Officer, who also serves as the Company’s Privacy Officer, or the Legal Department.

Refer to our *Privacy Policies* for more information.

COMPANY INFORMATION AND PROPERTY

Protecting Company Information

Team Members must safeguard our Company’s “Confidential Information.” Confidential Information includes all non-public Company information that – if disclosed – may be of use to competitors, or harmful to our Company. This particularly includes our Company’s confidential strategy information (for example, marketing and sales plans), personnel information, and unpublished financial information.

Team Members:

- Must carefully handle and store Confidential Information to prevent theft, loss, or unauthorized disclosure.
- Must never disclose Company Confidential Information to anyone without a need to know.

- Must never use Confidential Information for personal gain.

The obligation to protect Confidential Information survives our tenure of employment. That is, Team Members must safeguard and not disclose any Company Confidential Information upon retirement or termination of employment.

Before disclosing Confidential Information, Team Members should engage the Legal department to ensure that appropriate protections are in place—for example, a Non-Disclosure Agreement.

Protection and Use of Company Property

Team Members must take steps to safeguard and protect Company property from theft, loss, or waste. Unless specifically stated below or in another policy, the Company's property must only be used for Company business.

Team Members must never use Company property – or allow it to be used – for illegal activity, personal financial gain, or the benefit of another.

Because of the appearance of impropriety, Team Members may not sell any personal property to the Company or receive a personal loan from our Company.

Email, Internet, Telephones, Cellular Phones, and Voicemail

Our Company owns all information contained on the communication devices issued to Team Members, as well as its computer networks.

Team Members should make every effort to use Company-issued communication devices – including computers, telephones, and cellular telephones – to conduct business. Team Members should be aware that conducting business on personal devices could subject those devices to search in the event of an investigation or litigation.

Team Members have no expectation of privacy in any information contained or transmitted on Company property or communication systems. Our Company retains the right to control computer access, and to monitor and review use – at random or for cause – to ensure compliance with law, regulations, rules, Company policies, and this *Code*.

Team Members must protect all Company information stored in, or accessible on Company computers from unauthorized or inadvertent disclosure. Robust pass-wording is a must.

Team Members must operate all computer resources in a professional, respectful, lawful, and ethical manner.

Personal Use of Company Property

Our Company allows reasonable personal use of Company-provided email, internet, telephones, cellular phones, and voicemail that:

- Does not violate any law, regulations, rules, Company policies, or this Code.
- Does not interfere with work responsibilities.
- Does not overburden Company resources.

COMMUNICATIONS

Business Communications

Our business communications in the workplace and marketplace must always be courteous and professional. This includes communications by any means—person-to-person, telephone, email, and text messages.

Although Team Members may react emotionally to events, and others' behavior and words, we must always strive to be objective, and keep feelings in check.

Refer to our *Social Media Policy* for more information.

Business Emails

Emails generated using Company email addresses are Company records. Team Members may only use the Company's email systems to conduct business. Team Members must never use a private email system (for example, Gmail or Yahoo Mail) for any business communications.

Any information sent or received using the Company's email system is the property of the Company.

Use of the Company's email system for personal matters should be avoided.

Public Statements

Only authorized spokespersons may issue public statements on behalf of the Company.

If a Team Member is a presenter at conferences or trade association meetings, it is a best practice to preface remarks that views expressed are not necessarily those of our Company.

“Social media” – that is, websites and applications that enable users to create and share information – serves as an avenue for personal expression. When using social media, Team Members must be clear about who they are representing. When commenting personally on matters that may relate to the Company, it is a best practice to preface a social media post using this or a similar disclaimer:

“The opinions expressed here are my own, and do not represent the views of my employer.”

Refer to our *Social Media Policy* for more information.

Code of Conduct | 2023



ANOVA

BUMBLE BEE[®]
SEAFOODS

Beach Cliff[®]



BRUNSWICK[®]

