Anti-Money Laundering and Sanctions Compliance Policy October 2021

1. Purpose & Scope

1.1. Reaffirm to all employees our commitment to a culture of integrity, honesty, and accountability everywhere we operate. Therefore, we strive to protect our business and employees from being used by criminals to obtain material resources for their illegal activities.

1.2. Establish the basic principles and framework for preventing, detecting, investigating, reporting, and, if applicable, apply the appropriate penalties to any conduct that violates anti-money laundering laws.

1.3. This Policy applies to all Nemak employees, suppliers, and clients, as well as to any individual that acts on behalf of Nemak, such as representatives, agents, consultants, advisors, etc.

a) It is worth noting that our teams in sensitive areas are more exposed to being used by criminals to money laundering activities.

b) All employees must read this Policy and, when required, attend mandatory training and confirm that they have not and shall not engage in non-compliant behavior.

c) Suppliers, customers, and individuals that represent Nemak will be notified of the existence of this Policy and will be required to observe it.

2. Definitions

- **Anti-Money Laundering Laws:** all applicable anti-money laundering and terrorism financing laws, including anti-money laundering laws in Mexico such as the *Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita*; in United States such as the U.S. Bank Secrecy Act, the Money Laundering Control Act, the Money Laundering Suppression Act and the Patriot Act; in the European Union such as the EU Directive on the prevention of the use of the financial system for money laundering or terrorist financing of 2015, amended by Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018, and the sanctions laws and similar anti-money laundering and terrorism financing laws in effect in the countries where Nemak does business.
- **Cash Payment:** Refers to payments in cash, including coins, banknotes, and money orders.
- **Customer:** Any individual entity that purchases goods from Nemak, including OEMs and entities that purchase Nemak's by-products and production scrap.
- **Supplier:** Any individual or entity that offers goods and/or services to Nemak, including one-time suppliers and regular suppliers.
- **External Party**: Refers to both customers and suppliers.
- **One-time supplier**: Suppliers that will be used eventually and on a temporary relationship.
- **Regular supplier**: Suppliers with whom Nemak regularly maintains a business relationship and which Nemak has considered the possibility of keeping a business relationship for a prolonged period.
- **Employees**: Members of the Board of Directors and committees, as well as executives, directors, officers, employees, and interns of Nemak.
- **Sensitive areas**: Shall include employees involved in transactional services, sales department, finance, treasury, accounting, or credit departments.
- **Ultimate Beneficiary**: Any entity or individual that owns or controls an external party and/or the entity or individual on whose behalf a transaction is being made. This includes an entity or individual that has, directly or indirectly, 25% or more stock ownership in the external party, or exercises control over a company, partnership, corporation, trust or other legal vehicles.

©Nemak | Public

- **Money Laundering**: The process of disguising the nature and source of money or other property connected with criminal activity, such as drug trafficking, human trafficking, terrorism, corporate fraud, bribery, or corruption, by integrating illicit money or property into the stream of commerce so that it appears lawful through legitimate businesses, meaning its true source or owner cannot be identified.
- **Sanctioned person**: Any person or entity that is (i) listed on the Specially Designated Nationals and Blocked Persons List or the Consolidated Sanctions list maintained by the Office of Foreign Assets Control ("OFAC"), or any similar list maintained by OFAC, the U.S. Department of State, the European Union, any European Union member state, the United Kingdom, the United Nations Security Council, or any other applicable governmental authority that implements sanctions programs; (ii) operating, organized or resident in a country or territory that is subject to comprehensive sanctions broadly restricting or prohibiting dealings with, in or involving that country or territory (as of the date hereof, this includes Cuba, the Crimea region of Ukraine, Iran, North Korea, Syria, and "the government of Venezuela" as defined by Exec. Order No. 13884, 84 Fed. Reg. 38, 843 (Aug. 7, 2019) or (iii) prohibited or restricted by sanctions laws from engaging in trade, business or other activities.
- **Sanctions Laws**: means the laws, rules, regulations and executive orders promulgated or administered to implement economic sanctions or anti-terrorism programs by (i) any U.S. governmental authority (including OFAC), including Executive Order 13224, the Patriot Act, the Trading with the Enemy Act, the International Emergency Economic Powers Act and the laws, regulations, rules and/or executive orders relating to restrictive measures against Iran; (ii) the European Union or any European Union member state; (iii) the United Kingdom; (iv) the United Nations Security Council or any other legislative body of the United Nations; and (v) any jurisdiction in which Nemak operates.

3. General Guidelines

3.1 Anti-money laundering laws

Are designed to prevent and detect money laundering and dealings with sanctioned persons. Therefore, we strive to ensure that all our business activities comply with anti-money laundering laws applicable in the countries where we conduct our business and thus, that no illegal funds are received by Nemak.

3.2 Nemak is committed to:

Doing business only with external parties that carry out legal activities and that share these standards when conducting their business.

3.3 Money Laundering Stages

Money laundering activities are highly complex, involve multiple stages, and often include several financial institutions and even countries. This Policy intends to avoid that any of these stages involve Nemak or its employees. While the specifics of the process may vary depending on the purpose of the scheme, it typically includes three stages:

a) **Placement**: First, illegal proceeds must be inserted into a financial institution, often in the form of cash deposits to banks. Most entities that own illegal proceeds conduct their transactions in cash. Since moving large amounts of cash usually piques the interest of financial institutions and law enforcement agencies, this stage is especially risky for criminals.

b) **Layering**: In this step, the money is moved through multiple financial transactions. The purpose is to make the money difficult to track and can include wire transfers, moving money from accounts opened in different names, and using accounts in different countries to transfer funds. It can also involve the purchase of expensive items, turning the money into something else – an expensive home, a yacht, a plane, jewels, etc.

©Nemak | Public

c) **Integration**: Finally, the money is moved from its hiding place into the economy. The integration step can involve the sale of the expensive item (like the yacht) or using the money in a legitimate business with funds transferred from the last bank in the chain. When this step is completed, the money is very hard to trace and can be used without much likelihood of being caught.

3.4 Global Business Code for Suppliers

Before engaging in a business relationship with Nemak, all suppliers are required to confirm having read and understood our Global Sustainability Code for Suppliers and our Code of Conduct, and to confirm their commitment to comply, to communicate it to its personnel, and to report any violation to the Codes of which they become aware.

3.5 The Concept of "Knowledge" in Money Laundering

Generally, anti-money laundering laws criminalize the act of knowingly conducting a transaction with the proceeds of a crime. In some countries, the government may interpret "knowledge" by proving that the defendant is engaged in "willful blindness." Willful blindness is a deliberate failure to make a reasonable inquiry of wrongdoing despite suspicion or an awareness of the high probability of its existence. This could mean that even if an employee does not have actual knowledge of the illegal nature of the proceeds involved in a transaction, Nemak may still be accountable for money laundering offenses if circumstances raised enough suspicions of money laundering activities, but no actions were taken by Nemak to follow up on the suspicions.

3.6 Spotting Red Flags

Nemak employees should be alert to out of the ordinary or suspicious behavior ("red flags") when doing business with external parties, creating or changing Vendor Master Data, completing a Vendor Information Packet, changing any Supplier Accounting Data or Bank Data, conducting emergency purchases, advance payments, manual payments, onboarding process, due diligence checks, as well as monitoring continued engagement with external parties.

Annex 1 contains a list of red flags that, if observed, should be reported to the Governance and Compliance Department. When a red flag is reported, the Governance and Compliance Department and the Legal Department will investigate the situation and take further action consistent with this Policy, the rest of Nemak's internal policies, and relevant anti-money laundering laws.

3.7 Accepted Forms of Payment

All payments made by Nemak should comply with our Global Purchasing, Manual Payments, and Accounts Payable policies, and should be made after such goods and/or services are received. When receiving payments, Nemak should carry out payment acceptance due diligence measures to reduce the risk of receiving monies involved in money laundering activities or originated from sanctioned persons. External parties should be notified that acceptable forms of payments are limited to wire transfer from/to a bank account in the external party's name, or check drawn on a bank account in the name of Nemak / external party.

3.8 Cash Payments

The making or receiving of cash payments is prohibited. Nemak may make or accept a cash payment subject to prior written approval of the Governance and Compliance Department, if allowed by the applicable local law. The Governance and Compliance Department may only approve the making or receiving of cash payments if all the following conditions are met: (i) the cash payment is legal and commercially reasonable considering local business concerning the external party, and such reasons and details are well documented; (ii) Nemak obtains ownership information of the external party, except for external parties that are publicly traded companies, government-owned companies, or officially accredited educational institutions; provided, however, that Nemak shall attempt to obtain ownership, ultimate beneficiary information, or a certificate issued by the

©Nemak | Public

secretary of the board of directors or similar figure; (iii) the cash payment is made in compliance with the notification and record-keeping requirements of applicable local laws and regulations and it is not made in such a way that it appears intended to avoid such requirements; and (iv) controls are in place to detect any red flags involving the cash payment (see Annex 1).

The Governance and Compliance Department may establish one or more thresholds for small cash payments, to be applied to transactions with specified external parties in specific geographic regions, for which Nemak employees need not seek prior written authorization for each transaction. In addition to the requirements (i) through (iv) above, a decision to establish such thresholds should consider: (a) whether such cash payments are common and commercially reasonable considering the business line and transactions at issue in the country in which they are made; and (b) whether non-cash payment options are available for such transactions. No cash payments above the thresholds shall be permitted when made by one-time customers.

3.9 Compliance with Sanctions programs

Sanctions laws aim to control exports to restrict access to products, services, and information that could be used by criminals in ways that advance their illegal activities. Sanctions laws and anti-money laundering laws share the same objective of restricting criminals' access to any type of material resources. Our company's global reach puts us under the jurisdiction of many sanctions laws worldwide. The sanctions laws restrict or prohibit carrying out any type of transaction with sanctioned persons. Exports are the most affected transaction by sanctions laws.

Export is any item, technology, or data that is transferred from one country to another. An export can exist even if there is no actual sale or compensation involved.

Failure to comply with sanctions laws may lead to severe civil and criminal penalties for Nemak employees. Civil penalties may include significant monetary penalties, freezing or blocking of assets, and reputational harm.

Nemak shall have no business affiliation or commercial dealings with, or investments in, any sanctioned person, or any individual or entity that is subject to any action, litigation, proceeding, claim, or investigation under any sanctions laws or in violation of any sanctions laws.

All external parties must be screened to confirm that the external party is not a sanctioned person. Some screening will be easier when sanctions programs target the entire country or jurisdictions of destination such as Cuba, Crimea, Iran, North Korea or Syria. However, less restrictive sanctions programs are applied to other countries or entities that are less apparent. Furthermore, lists of sanctioned persons are regularly updated by the governmental agencies that administer such programs. These are a few guidelines that should be followed when screening an external party:

a) Does the external party seem to have high-risk factors? See Annex 1.
b) Is the external party seeking to purchase our products newly established?
c) Does the external party conduct most of its business in countries that are restricted by sanctions laws?
d) Where is the item being delivered? What is the item's final destination? Is the location of the country high-risk for corruption or fraud, i.e. related to customs, import restrictions, or government licensing?
e) Could the item sold be used for a different purpose other than Nemak's expected end-use? Could this end-use be within a concerning activity such as nuclear production or technology, missile technology, and chemical or biological weapons?
f) Who is receiving the item sold? Does the company rely on a network of distributors, brokers, or agents that may be "invisible" to Nemak?

©Nemak | Public

This screening control aims to reduce the risk of doing business with a high-risk external party. Employees should check with the Legal Department about any potential external party that could be deemed a sanctioned person to perform an adequate analysis.

3.10 Anti-money laundering laws are complex

Employees must keep in mind that anti-money laundering laws can be complex. Concerning export controls, these are particularly complex because most of them apply to countries that import our products and where Nemak has no presence. Employees in sensitive areas must always apply professional skepticism and awareness regarding fraudulent activities. Separating legal from illegal conduct often requires an in-depth evaluation of the specific facts surrounding the situation, along with a thorough understanding of the applicable law. Employees are not expected to be experts on anti-money laundering laws. Employees should check with the Legal Department about any potential money laundering activity in order to perform an adequate analysis.

3.11 Internal Audit

The Internal Audit Department shall include, within its audit programs, periodic review of Nemak's compliance with this Policy. The audit will include a written report, which will be sent to the Global Audit & Legal Director. Any deficiencies identified will be accompanied by written plans to address the deficiencies.

3.12 Disciplinary measures

Employees or external parties in breach of this Policy are subject to disciplinary actions ranging from a warning to termination of employment or contract. The severity of such disciplinary actions will depend on the seriousness of the offense.

Nemak will not pay any fine imposed on any Nemak employees nor any attorney's fees as a result of any money laundering activity, dealings with sanctioned persons, or breach of this Policy.

Nemak operates in different countries and is therefore subject to anti-money laundering laws in several jurisdictions. Doing business with money launderers, sanctioned persons or other criminals could result in severe consequences, including expensive investigations, reputational damage, freezing or blocking of assets, and disqualification from doing business. This could also lead to significant economic penalties and imprisonment of individuals.

Our company takes money laundering and sanctions compliance very seriously. We expect employees to report all known or suspected violations of this Policy. Immediate reporting of money laundering activities can be critically important both to our company and our employees because the timing of the report is considered when assessing a potential violation or penalty.

We maintain a robust compliance program designed to minimize the exposure to money laundering activities, violation of sanctions laws, and financial crimes, and we rely on the eyes and ears of our employees or any individuals who raise concerns if they see or hear anything they consider "not quite right."

Remember that your best resource in confirming any suspicion or gaining additional information is our Governance and Compliance Department.

Employees may raise concerns or report violations as follows:

- **Within the business unit or global staff area**
  Generally, an employee's Human Resources manager will be able to resolve any concerns or questions that such employee might have.
- **Nemak Governance and Compliance Department**
  Employees may report concerns to Nemak's Governance and Compliance Department by sending an e-mail to: governance@nemak.com.

©Nemak | Public

- **Integrity and Transparency Helpline**
  Nemak has a toll-free Integrity and Transparency Helpline in the countries listed below. Any individual may submit anonymous reports to the Integrity and Transparency Helpline, or else, may indicate that they wish to be contacted.

Argentina	0800-444-5685
Austria	0800-293-215
Brazil	0800-892-2016
China	+86-21-2068-9511
Czech Republic	800-701-160
Germany	0800-180-8939
Hungary	06-800-16476
India	000-800-100-5794
Mexico	01-800-265-2532
Poland	00800-112-4028
Spain	900-937-915
Slovakia	0800-606-251
USA / Canada	1-866-482-1957
Russia	880-0301-7408
Turkey	00-800-142-030-100

  A report may also be submitted via e-mail to:
  transparency@alfa.com.mx

- **No retaliation**
  Nemak will not retaliate against any individual who raises concerns in good faith regarding actual or suspected misconduct related to this Policy. Such retaliation would be grounds for discipline against whoever intends to exercise it, including potential termination of employment. According to its obligations under applicable law and the enforcement processes established in Nemak's internal policies, Nemak will keep confidential the identity of anyone reporting possible wrongdoing to the extent reasonably possible. No one will have his or her job terminated, demoted, suspended, harassed, or discriminated against solely because they reported a possible violation.

4. Contact Information

For questions or comments about this Policy, please contact Nemak's Governance and Compliance Department by sending an e-mail to: governance@nemak.com.

5. Revisions

0, October – 2021

6. Created / Approved by

Nemak Legal Department – October – 2021

7. Annex(es)

7.1 Annex 1 - Non-Exhaustive List of Red Flags

©Nemak | Public

Annex 1
Non-Exhaustive List of Red Flags

1. The external party shows an unwillingness to provide identification documents or any other data requested during the onboarding or due diligence check or such information is incomplete, wrong, or misleading;
2. The external party uses a false address;
3. The external party displays expired identifications;
4. The external party provides inconsistent information;
5. The external party has a complex shareholding structure that is not reasonably justified;
6. The external party's operations drastically change over time in volume or amount;
7. The external party shows unusual concerns related to the disclosure of any data requested;
8. The external party unreasonably scrutinizes the requirements of documentation and handling of information;
9. The external party refuses to provide information regarding its subsidiaries and affiliates, if and when requested;
10. The external party has multiple accounts under the same name for no apparent reason;
11. The external party or an individual or any of its subsidiaries or affiliates has a negative background, such as criminal records, civil penalties of any kind, or investigations regarding tax fraud, money laundering activities, and/or organized crime;
12. The external party demands that payment is made urgently and without regard to our internal policies;
13. The external party refuses to or is unable to identify a legitimate source of its funds;
14. The external party transacts with important public figures, such as public officials or other politically exposed persons;
15. The external party attempts to send or receive a payment in cash, or cash equivalents, in excess of USD 5,000, or its equivalent in local currency, or any other threshold, as outlined the Policy.
16. The external party makes payments through the accounts of different individuals or entities rather than through its accounts;
17. The external party's payments are done through a credit institution of a different nationality than that of the external party;
18. The external party frequently engages in transactions where payments equal the maximum amount allowed for withdrawals at financial institutions;
19. The external party seeks to bribe, threaten or persuade Nemak employees to avoid any obligation related to this Policy or anti-money laundering laws;
20. There are deposits in foreign currency made by multiple individuals for the same transaction;
21. The external party requests unjustifiably high or low prices for products or services which are not within market standards;
22. The external party requests or ensures that goods are transported through more than one jurisdiction for no apparent reason;
23. The external party frequently changes its payment instructions;
24. The external party requests or proposes excessive modifications to letters of credit or similar documents;
25. The external party provides false invoices or invoices with miscellaneous charges that have not been previously approved by Nemak;
26. The external party makes an unusually large amount of overpayments or requests a refund to be sent to an unknown external party as a result of a canceled purchase order;

©Nemak | Public

27. The external party's representative seems not to know basic facts about the external party's business, which raises suspicion as to whether he or she is actually employed by the external party;
28. The external party requests Nemak to issue an invoice that does not accurately reflect an invoiced price or other material terms of the transaction;
29. The external party structures a transaction to circumvent the notification requirements of authorities or governments, for example by paying one invoice with numerous money orders or cashiers' checks in amounts under the notification requirements; or
30. The external party has a broker, attorney, or another agent to facilitate the transactions, and Nemak has no proper info.

©Nemak | Public