ALPHAWAVE SEMI

Anti-Money Laundering Policy

Purpose

Alphawave Semi is committed to preventing money laundering in accordance with UK and Canadian legislation and we take seriously the responsibility of ensuring our business is not used for the purposes of money laundering and are committed to best practice in this area.
The purpose of this policy is to establish the framework that the company will follow in order to support law enforcement authorities' activities to detect proceeds from serious crimes and help prevent money laundering and recycling of illegally obtained money.
The Company requires all directors, employees, consultants or any person or body acting on the Company's behalf to adhere to this policy in order to prevent the use of our company and its products and services being used for the purposes of money laundering. Adherence to the policy is critical to ensure that Alphawave Semi as a whole, comply with our obligations in respect of preventing money laundering.

Background

Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime.
Money laundering schemes vary in complexity, but generally there are three distinct stages in the money laundering process: placement, layering and integration:

- **Placement** - Placement is the process of placing criminal property into the financial system. It might be done by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) deposited at different locations.
- **Layering** - Layering is the process of moving money that has been placed in the financial system in order to obscure its criminal origin. It is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts.
- **Integration** - Once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds. This process involves investing the money in legitimate businesses and other investments such as property purchases or setting up trusts.

Counterparty Due Diligence

As part of our commitment to prevent money laundering, the Company must ensure that it completes adequate counterparty due diligence on all of its customers, vendors, and other counterparties to reduce the risk of the Company being used by a counterparty who wishes to launder money.

The counterparty due diligence process that must be followed by Procurement & Vendor Onboarding teams is:

1. *Ascertainment of Counterparty Identity*
   The counterparty's identity should be verified on the basis of documents, data or information obtained from a reliable and independent source, e.g. checking with the organisation's website to confirm the business address, checking Companies House etc.
2. *Establishment of Ultimate Beneficiary*
   The beneficial owner of the counterparty should be identified. The beneficial owner is the natural person who ultimately owns or controls the counterparty or the natural person on whose behalf a transaction or activity is being conducted. The threshold for ownership or control is 25%.

The counterparty should be asked to provide details of any shareholder that holds more than 25% of that counterparty. If a corporate entity as opposed to a natural person holds more than 25% of the shares, the beneficial ownership of that corporate entity should be confirmed.

3. *Establishment of the purpose of the business relationship*
   If the counterparty is a new one, the rationale for wanting to transact with us should be established.
   The counterparty should be asked to explain the reason for the transaction in question and, in this context, you should pay attention to the "red flags" set out below.
   It should be borne in mind that individuals, companies and specific assets can be subject to sanctions. If there are any concerns that these may apply, such concerns should be reported to the Group Director of Risk Management & Internal Audit.
   Records of the due diligence completed must be kept in accordance with the Group's Document Retention policy.
4. *Potential Sanctions Issues*
   If a counterparty is located in a jurisdiction subject to sanctions, additional due diligence must be completed in accordance with the Trade Compliance policy.
   It should be borne in mind that individuals, companies and specific assets can be subject to sanctions. If you have any concerns these may apply, via the company designated email address.
   There is also the option for issues to be directly raised with an independent director as well, if the individual wishes not to include anyone from the company within the report.

Red Flags

The following circumstances should be seen as "red flags" in relation to the risk of the Company being used for the purposes of money laundering. Any of the below, or any wider concerns in relation to a transaction/contract, should be reported via the company designated email address or to the Group Director of Risk Management & Internal Audit for purposes of determining whether enhanced due diligence and/or making appropriate confidential notification(s) to the relevant authority / authorities is warranted.

- A counterparty provides minimal, vague or fictitious information about itself or the reasons for wanting to do business.
- A counterparty is overly secret or evasive about its ultimate beneficial owner.
- The counterparty's proposed business activity is inconsistent with its wider business profile.
- A counterparty provides false or counterfeited documentation.
- A counterparty is using an agent or intermediary without good reason.
- A counterparty is actively avoiding personal contact without good reason.
  A customer counterparty wishes to pay or receive payment in cash. Cash receipts from customers and cash payments should be actively discouraged. No payment to the Company will be accepted in cash if it exceeds £1,000. Cash payments made by the Company are only authorised where they amount to less than £1000. An exception to this may be made in specified circumstances in relation to cash advances to employees. In such cases, the Group Policy on cash advances to employees must be followed.

Reporting

If any employee or associate suspects money laundering offences are being committed this should be reported to the confidential e-mail address *ombudsman@awavesemi.com* or by contacting the Chief Financial Officer to share your concerns. You can prefer to remain anonymous on this call but if you are willing to provide your name this will aid the independent investigation of your concerns. Employees or associated persons who report instances of fraud in good faith will be supported by the Company. The Company will ensure that the individual is not subjected to detrimental treatment as a consequence

of his/her report. Any instances of detrimental treatment by a fellow employee because an employee has made a report will be treated as a disciplinary offence.

Any instruction to cover up wrongdoing is itself a disciplinary offence. If told not to raise or pursue any concern, even by a person in authority such as a manager, employees and associated persons should not agree to remain silent. They should report the matter to our Non-Executive Board Director and member of the Audit Committee *Victoria.Hull@awavesemi.com* or via telephone +44 7740 830046. Also see the Anti-Bribery and Whistleblowing Policy for more information.

Training

All Company employees in a procurement, compliance or legal role, and any other relevant personnel as determined by Senior Managers are required to complete anti-money laundering training. This training should cover, at a minimum, the meaning of anti-money laundering requirements and the risks of non-compliance. The training must be completed every 18 months.

The company's Senior Managers are responsible for ensuring participation in this training which will be tracked via the firm's outside counsel, Linklaters, and for maintaining documentation of the training.

Further information

The CFO is responsible for monitoring compliance with this policy and is contactable by email.

Related Policies & Documents

Business Code of Conduct, Anti-Fraud & Dishonesty Policy, Anti Money Laundering Policy, Policy Against Trafficking of Persons and Slavery, Whistleblowing Policy, Anti-Bribery Policy.

Document Version Control

Version	Date Drafted	Drafted by	Reviewed by	Date Reviewed	Next Review date
V1.0	Mar-21	BDO	D. Aharoni	May-22	May-23