NAVISTAR®

Corporate Policy

Money Laundering Prevention

General Information:

Section:	**05 - Business Conduct**	**Version:**	**1.0**
Policy Number:	**05-09**	**Effective Date:**	**March 31, 2009**
Policy Contact:	**MaryEllen Kummar**	**Reference Policies:**	
Approved By:	**Jim Moran**		

Objective:

The possibility exists that those we do business with may attempt to launder money that was acquired through illegal means via a transaction with Navistar. Taking part in such transactions can result in criminal penalties, in addition to damage to Navistar's reputation. The purpose of this Policy is to provide guidance to Navistar employees to assist them in detecting, investigating, and reporting potential money laundering activity.

Defined Terms:

Cash Equivalent: Instruments that are considered the equivalent of cash, including foreign currency, cashier's checks, money orders, bank drafts, and traveler's checks, and must be treated like cash for reporting requirements.

OFAC: The Office of Foreign Asset Control, which is part of the U.S. Department of Treasury. OFAC is responsible for administering and enforcing economic and trade sanctions against certain nations, entities, and individuals.

Money Laundering: The process used to move cash or other funds generated from illegal activities to conceal the initial source of the funds. The most common source of money laundering is cash accumulated as a result of illegal narcotic sales, but also includes money derived from other criminal activities such as robbery, kidnapping, fraud, counterfeiting, and bribery. Funds derived from such activities are typically in the form of cash and need to be "cleaned" before the criminal can safely use the funds.

Policy Statements:

Employees must follow the documented new customer and payment procedures in their areas in an effort to avoid participating in money laundering activity. Those employees that maintain customer data and those that process payments must be particularly diligent to abide

by such procedures. Requirements for maintaining customer data and receiving proper forms of payment as they relate to money laundering avoidance are detailed below. The money laundering red flags which employees should be mindful of when performing these functions are also provided.

Customer Data

Employees must follow the documented business unit procedures outlining the steps to be taken before accepting new customers, including performance of OFAC screening. Customer files will be audited to assure compliance with business unit policies. In the event that a customer's identity cannot be verified, contact your supervisor or the Law Department for further guidance.

Customer Red Flags

The following customer red flags require employees to perform further investigation to determine whether the red flags indicate actual money laundering. Refer to the section "Investigating and Reporting," below, for additional guidance.

Commercial Customers

- No interest in price discounts
- Unwilling or unable to give basic information about the Company or its customers
- Known in marketplace for questionable business practices
- No business infrastructure, e.g., no office, phone number, letterhead, record keeping
- Unusual spikes in purchases, given the economic environment or the customer
- No response at main business phone number
- Dun & Bradstreet reports with no history on file
- No financial reports available (income statement, balance sheet)
- Unusual product mixes
- Customer offers to pay with large sums of cash
- Customer seeks to pay with money orders, traveler's checks, cashier's checks, foreign drafts, third party checks, or checks written on the account of an unrelated third party
- Customer has a messenger or unrelated third party pay for the goods

Forms of Payment

Employees must follow the established business collection routines and controls which help detect and report suspicious forms of payment. Generally, the following forms of payment are acceptable:

- Checks from the customer of invoice (name and address of invoiced customer on check) written out to your business
- Wire transfers from a reputable banking establishment that can be verifiably traced back to the customer of invoice's permanent account

Forms of Payment Red Flags

The following forms of payment red flags require employees to conduct additional investigation to determine whether the red flags indicate actual money laundering activity. Refer to the section "Investigating and Reporting," below, for additional guidance.

- Large amounts of cash in suspicious circumstances is a red flag, but can be a safe form of payment if the U.S. currency reporting requirements are followed (see U.S. currency reporting requirements below)
- Money orders, cashier's checks, traveler's checks, and foreign bank drafts
- Third-party payments (checks, wire transfers) that cannot be linked, directly or indirectly, to the customer's business or made in a context not considered a customary business practice for the industry
- Multiple instruments to pay a single invoice
- Repeated or routine overpayments of invoices

Investigating and Reporting

Red flags do not necessarily mean that your customer is engaged in money laundering activity. However, in these instances (e.g., red flags regarding your customer's business or its forms of payment) appropriate follow-up is required to confirm that your customer is not involved in money laundering or other criminal activity. Each instance requires general follow-up before concluding the transaction as noted in the steps below. Depending on the situation and the results of the investigation, additional specific follow-up may be required.

- Request more information from your customer
- Request supporting documentation
- Check references
- Visit the customer's business location
- Request corrective action be taken when concerns arise, e.g., confirm that your customer will no longer pay with unrelated third-party checks
- Refuse to do business with those persons who do not appear legitimate or who ignore or are insensitive to money laundering risks
- Refuse to do business with customers who do not provide required information or if the information provided appears false, inconsistent, or does not make sense
- Document all inquiries and findings and record in your customer file

For questions or consultation regarding potentially suspicious activity, whether it is at customer set-up or through payment, contact the Law Department.

U.S. Currency Reporting Requirements

Employees are responsible for identifying instances when more than $10,000 in cash or cash equivalents in one or more related transactions is received and promptly reporting such receipts to the IRS using IRS Form 8300. For further information on Form 8300 guidelines, refer to your business unit procedures, contact your supervisor, or visit the IRS website.

Roles and Responsibilities:

Employees are responsible for reading, understanding, and complying with the statements in this Policy.

Employees are responsible for reporting incidents of potential money laundering to the Law Department.

The Tax Department is responsible for ensuring that employees comply with U.S. currency reporting requirements.

The Law Department is responsible for providing money laundering prevention training to all applicable employees.

The Law Department is responsible for providing guidance with regard to investigating and reporting cases of potential money laundering activity.

Revisions and Approvals:

Date	Version	Approver	Change Description

Appendices and Attachments:

N/A