Trade-Based Money Laundering: Lessons from Recent Regulatory Orders

Oct 22, 2026

Categories:

Banking On It
Blockchain and Digital Assets
Publications

Authors:

Nancy Eff Presnell

Money laundering is often pictured as suitcases of cash or a series of wire transfers through shell companies. One of the most significant and least understood money laundering channels, however, runs through ordinary commerce: buying and selling goods. Known as trade-based money laundering (TBML), this channel has long been flagged by international standard-setters as a growing vulnerability, and federal regulators are now making clear that they expect financial institutions to detect it, report it, and maintain compliance programs designed for it.

Several enforcement orders, issued in October 2026 against nationally chartered banks, illustrate the point. In a cease-and-desist consent order against a large credit and charge card issuer, the Office of the Comptroller of the Currency (OCC) states its view that the issuer failed to timely identify and report suspected TBML and violated multiple Bank Secrecy Act (BSA)/anti-money laundering (AML) requirements. Separately, the OCC and the Financial Crimes Enforcement Network (FinCEN) issued parallel civil money penalty consent orders against a large national bank that describe, among other things, gaps in monitoring for activity with indicia of potential TBML.

Banks, card issuers, fintech companies, and payment providers should not wait for an examination finding to test their own programs. If your risk assessment, customer due diligence, transaction monitoring, or suspicious activity report (SAR) processes have not been reviewed specifically for TBML risk, the time to act is now. Regulators cited each of these areas in the recent orders. Gaps an institution finds and fixes on its own are far easier and less costly to address than gaps a regulator finds.

What Is Trade-Based Money Laundering?

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

The Financial Action Task Force (FATF), the global standard-setter for AML and counter-terrorist financing measures, identifies three main ways that criminal organizations and terrorist financiers move money to disguise its origins: through the financial system, through the physical movement of cash, and through the physical movement of goods through the trade system. FATF defines TBML as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins."

In practice, TBML usually involves misrepresenting the price, quantity, or quality of imports or exports. When an invoice overstates or understates the true value of goods, value moves between the parties under the cover of a seemingly legitimate commercial transaction. These techniques range from simple to complex, and they are often combined with other laundering methods to further hide the money trail.

Why Is TBML So Hard to Catch?

FATF has identified several features of international trade that make it attractive to bad actors:

- **Volume.** The sheer scale of global trade flows hides individual transactions.
- **Complexity.** Multiple foreign exchange transactions and varied trade financing arrangements make transactions hard to trace.
- **Commingling.** Legitimate and illicit funds are frequently mixed.
- **Limited oversight.** Most customs agencies have limited resources for detecting suspicious trade transactions.

FATF has also warned that as controls on other laundering techniques become more effective, TBML is expected to become increasingly attractive. Put simply, as traditional channels are tightened, illicit value is likely to shift toward trade.

TBML is not limited to letters of credit and traditional trade finance. In the cease-and-desist order, the suspected TBML activity

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

involved a combination of suspicious card charges and the associated repayments of those charges. The other recent orders point in the same direction. The OCC's civil money penalty order states that examiners reviewed a small sample of accounts in the bank's credit card portfolio and identified 10 accounts with potential TBML. According to that order, the bank's review of those accounts at the OCC's request led to SARs on hundreds of millions of dollars in suspicious transactions. The FinCEN order similarly describes money order deposits, cross-border wires, and credit card activity tied to potential TBML. Institutions should take note that TBML risk can surface in consumer and commercial payment products, not only in a trade finance department.

What TBML Red Flags Did Regulators Identify?

The FinCEN order describes several patterns that it characterizes as red flags for potential TBML and related illicit activity, including:

- **Structured money orders.** According to the order, groups of sequentially numbered, round-dollar money orders totaling just under $3,000 were deposited repeatedly. The order views this pattern as an apparent effort to evade the identification requirements that apply at $3,000.
- **Third-party payments.** The order states that customers in the used and salvaged vehicle trade relied heavily on payments from third parties, limiting visibility into the true source of funds. It also cites FinCEN's earlier TBML advisory identifying third-party payments and negotiable instruments as potential indicators of illicit activity.
- **Activity inconsistent with the customer profile.** The order describes a customer onboarded as a small-to-medium business with expected annual sales of $1 million to $4 million that received hundreds of millions of dollars in wires involving high-risk jurisdictions.
- **Many-to-one payment patterns.** According to the order, dozens of unrelated originators sent wires referencing the same buyer identification number.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- **Card and payment activity with no apparent commercial purpose.** The order cites high volumes of back-to-back credit card purchases, payments on cards held in the names of unrelated third parties, and wires to overseas counterparties with generic descriptions such as "for goods."
- **Used and salvaged vehicle exports.** The order notes that used and salvaged vehicles have been publicly linked to TBML because they can be used to move value across borders.

How Can Institutions Detect TBML?

FATF's recommendations emphasize a risk-based approach to combating money laundering, terrorist financing, and proliferation financing. Read together, the recent orders reflect the regulators' view that an effective TBML program requires the steps outlined below.

- **Assess risk across the actual business.** Conduct an institution-wide risk assessment covering products and services, customer types (including insiders), transaction types, geographic exposure, and delivery channels, with particular attention to the products that drive volume. Refresh at least every 12 months or sooner if risk changes significantly.
- **Know the customer and the purpose of the relationship.** Use customer due diligence to establish clear risk categories, apply enhanced due diligence to higher-risk customers, and update risk ratings based on the institution's own monitoring, not only after outside inquiries such as law enforcement subpoenas. Compare actual activity against the customer's expected profile, which is one of the most useful TBML signals. When risk is elevated, consider enhanced monitoring, product restrictions, or other controls, not only account closure.
- **Tune transaction monitoring for TBML red flags.** Monitor across all business units, including negotiable instrument deposits, with rules and thresholds suited to the institution's risk profile and specific TBML indicators that actually generate alerts. Govern any alert suppression, rescoring, or de-duplication, test thresholds periodically, require senior

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

management approval of changes, and independently validate models. Automated controls, not outside referrals, should drive most investigations.

- **Investigate and report promptly.** Staff investigations to prevent case backlogs, and file SARs timely, completely, and accurately, with a sufficient description of the activity and the basis for filing. Track SAR decision rates and escalate when management reporting shows potentially suspicious activity going unreported.
- **Monitor insider activity.** Maintain a dedicated insider program with monitoring rules, reporting to senior management and the board, and disciplinary referrals for misconduct.
- **Test, staff, train, and act on escalations.** Maintain qualified independent testing and respond to its findings, assess staffing and skills against the program's needs, and provide risk-based, role-specific training for board members and personnel. When compliance recommends exiting or restricting a high-risk relationship, ensure that recommendation receives appropriate weight against business-line interests.

What Is the Cost of Noncompliance?

In both OCC orders, the banks neither admitted nor denied the OCC's findings, which can be taken to reflect the agency's view. The FinCEN order, by contrast, states that the bank admitted the order's statement of facts and violations, solely to resolve that matter. Admission or not, regulator-directed remediation can be costly, prolonged, and closely supervised. The recent orders illustrate what remediation involves, including:

- **Board-level oversight.** Under the OCC's cease-and-desist order, the board must appoint a compliance committee with a majority of independent directors and submit an action plan with specific corrective actions, timelines, and responsible individuals for the OCC's review.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- **Program-wide rebuilding.** The order requires the bank to rebuild nearly every element of its program, including its risk assessment, customer due diligence, financial crimes risk management, suspicious activity review, independent testing, staffing, training, and insider controls, with the board reviewing the effectiveness of each at least annually.
- **Look-back reviews.** Independent consultants must review past activity to determine whether SARs should have been filed or prior filings corrected. The OCC may expand the scope or time period at its discretion, and the FinCEN order requires a multi-year look-back across credit card, negotiable instrument, and high-risk cross-border activity.
- **Multiple independent consultants.** The FinCEN order separately requires the bank to retain, at its own expense and subject to FinCEN's veto, consultants to test its suspicious activity monitoring, test its customer and foreign correspondent due diligence, and review the governance of the data underlying its AML program. Each review carries scope reports, progress reports, and implementation plans, with deadlines extending years beyond the order.
- **Significant operational cost.** The FinCEN order describes the bank's own estimate that recalibrating its monitoring thresholds would double monthly investigation volumes and require hundreds of additional personnel.

Financial institutions, fintech companies, and payment providers should review their AML programs now with TBML specifically in mind. Doing so proactively costs far less than a regulator-directed remediation. For help evaluating your institution's TBML exposure or responding to any regulatory concerns, contact the author or an attorney with our Data, Digital Assets and Technology team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons