Money laundering is often described as a way to disguise the source of criminal proceeds. In practice, it can be connected to many white-collar crimes: embezzlement, fraud schemes, bribery, tax evasion, and other offenses that generate or move money. A business, bank account, payment platform, or property purchase may be used to make that money look legitimate.

Understanding the connection matters for employees, customers, and others who notice suspicious activity. U.S. law also provides a whistleblower route for certain reports about violations of openclassactions.com anti-money-laundering rules. This article explains common crime patterns, what Suspicious Activity Reports (SARs) are, and the basics of the Anti-Money Laundering (AML) and Bank Secrecy Act (BSA) whistleblower program.

How Money Laundering Connects to White-Collar Crime

Money laundering generally involves disguising the origin, ownership, or movement of proceeds from unlawful activity. The crime that produced the proceeds is often called a predicate offense. For example, a fraud scheme may create illegal funds; laundering may then involve routing those funds through accounts or businesses to conceal where they came from.

Not every unusual transaction is money laundering, and a suspicious transaction is not proof that a crime occurred. Investigators look at the full context, including records, relationships among parties, explanations for transactions, and whether conduct appears deliberate.

Common Examples of White-Collar Crimes Tied to Money Laundering

Embezzlement and employee theft

Embezzlement occurs when someone entrusted with money or property misappropriates it. An employee might divert company payments into a personal account, create fake vendors, or manipulate invoices. The person may then move the proceeds through several accounts, purchase assets, or disguise transfers as legitimate business expenses.

Example: A finance manager creates a fictitious supplier, approves invoices, and sends company funds to an account controlled by a relative. Transfers to other accounts or purchases made with those funds may be attempts to hide their source.

Fraud schemes

Fraud schemes can include investment fraud, business email compromise, identity theft, mortgage fraud, insurance fraud, and online scams. Fraudsters may use shell companies, nominee account holders, payment processors, or multiple bank accounts to receive and distribute victims' money.

Example: A fake investment operation collects payments from customers, then sends the funds through accounts held in different names before using them to pay earlier investors or buy property. The movement can make the money harder to trace, even if some transfers are presented as ordinary business activity.

Bribery, kickbacks, and corruption

Bribes and kickbacks may be concealed as consulting fees, commissions, gifts, or payments to a company with no genuine role in a transaction. Laundering concerns arise when the recipient uses intermediaries or false documentation to conceal who paid the money and why.

Tax crimes and concealed income

Tax evasion and money laundering are separate offenses, but they can overlap. Someone hiding income from tax authorities may use undeclared accounts, false invoices, or business entities to conceal funds. Conversely, a person may attempt to disguise criminal proceeds by reporting them as ordinary income or business revenue.

Securities and market-related fraud

Insider trading, market manipulation, and investment fraud can generate illegal gains. People may attempt to conceal those gains through accounts held by relatives or companies, layered transfers, or purchases of high-value assets. The fact that a transaction involves investments does not alone establish laundering; the underlying conduct and intent matter.

Trade-based money laundering

Trade-based laundering uses commercial transactions to move or disguise value. Examples may include misstating the price, quantity, or type of goods on invoices, or using transactions with little apparent business purpose. Legitimate companies can also make documentation errors, so investigators consider patterns and surrounding evidence rather than treating one discrepancy as conclusive.

Structuring and other transaction patterns

Structuring generally means breaking up transactions to evade reporting requirements. For example, a person might make repeated deposits below a reporting threshold to avoid triggering a bank's currency transaction reporting obligations. Structuring can be a crime even when the money itself came from a lawful source. It is distinct from ordinary deposits and should not be inferred merely because someone made multiple transactions.

What Banks Do: BSA Controls and Suspicious Activity Reports

The Bank Secrecy Act (BSA) requires covered financial institutions to maintain certain records and operate programs designed to detect and report potential financial crime. Customer due diligence (CDD) refers to steps institutions take to understand customers and the nature of their relationships, including identifying and assessing relevant risks.

When a financial institution identifies activity that meets applicable reporting criteria, it may be required to submit a Suspicious Activity Report to the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury. SARs are used by authorities as leads and intelligence. A SAR is not a finding that a customer committed a crime, and the existence of a SAR does not itself prove wrongdoing.

SARs are confidential. Financial institution personnel generally must not disclose whether a SAR was filed or reveal its contents to the subject of the report. Employees with concerns should use appropriate internal escalation channels or report information to the relevant authorities, rather than sharing a SAR or confidential customer information with unauthorized people.

The AML/BSA Whistleblower Program: Legal Origin and Timeline

Congress created BSA whistleblower provisions through the Anti-Money Laundering Act of 2020, part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. Congress later strengthened the program through the Anti-Money Laundering Whistleblower Improvement Act, included in the National Defense Authorization Act for Fiscal Year 2023, signed on December 23, 2022.

The 2022 law expanded the potential award framework and strengthened protections associated with eligible reporting. In general, a qualifying whistleblower may be eligible for an award when original information leads to a successful enforcement action resulting in monetary sanctions above the statutory threshold. The law provides an award range tied to the sanctions collected, subject to statutory requirements and agency procedures. It does not guarantee an award, and an individual's eligibility depends on the facts and applicable rules.

FinCEN's website, fincen.gov, is the key official resource for current information about BSA reporting and the whistleblower program. Program procedures and guidance can change, so consult current FinCEN materials before submitting information.

Who May Qualify—and What Is "Original Information"?

The program is generally intended for individuals who voluntarily provide useful information about covered violations. Depending on the circumstances, an eligible person may include an employee, contractor, customer, or someone outside the organization. The statute excludes certain categories of people or conduct, and eligibility can be affected by a person's role, involvement in the violation, or how the information was obtained. Do not assume that job title alone determines eligibility.

"Original information" generally means information based on independent knowledge or independent analysis that is not already publicly known or otherwise excluded by law. A report should be specific enough to help authorities investigate. It may identify transactions, dates, people, accounts, business entities, or records that support the concern. A rumor without a factual basis may be less useful, while a well-documented observation does not need to prove the entire case.

Voluntary reporting is important. A person who has already been contacted by authorities or is subject to a reporting requirement may face different rules. A lawyer experienced in whistleblower matters can help assess timing, confidentiality, eligibility, and potential retaliation concerns before a report is made.

What Types of Violations May Be Relevant?

The AML/BSA whistleblower framework can cover information about violations of the BSA and certain related laws. Depending on the facts and statutory scope, relevant conduct may include:

- **SAR-related violations:** A covered institution fails to file required reports, files them improperly, or unlawfully discloses confidential SAR information.
- **Structuring:** A person deliberately breaks up transactions to evade required reporting.
- **CDD failures:** A financial institution fails to meet applicable customer due diligence obligations.
- **Recordkeeping violations:** Required transaction or customer records are not maintained, or records are falsified or concealed.
- **Sanctions violations:** Certain conduct involving sanctions administered by the U.S. government may fall within the expanded whistleblower framework. The precise coverage depends on the law and the facts.
- **Other BSA program failures:** For example, conduct that undermines required controls or reporting obligations.

These are not interchangeable categories. A financial institution's compliance weakness is not automatically a crime, and a whistleblower report is not a substitute for an authority's investigation. The relevant question is whether the facts indicate a covered violation and whether the information meets program requirements.



Observed concern Why it may matter Practical caution Repeated transfers with no clear business purpose May help reveal movement or concealment of funds Transfers alone do not establish a crime Fake vendors or altered invoices May point to embezzlement, fraud, or trade-based laundering Preserve only records you are authorized to access Transactions deliberately divided to avoid reporting May indicate structuring Do not assume a threshold pattern proves intent Failure to follow reporting or recordkeeping duties May raise BSA compliance concerns Distinguish a mistake from knowing or systematic misconduct

What to Do Next: A Practical Checklist

1. **Write down what you observed.** Note dates, transaction types, people or entities involved, and why the activity seemed unusual. Separate firsthand knowledge from assumptions.
2. **Preserve information lawfully.** Do not access systems or records you are not authorized to use, remove confidential files, or disclose a SAR. Ask a lawyer how to handle sensitive records.
3. **Use appropriate reporting channels.** Depending on the facts, this may include an internal compliance or ethics channel, FinCEN, or another relevant government agency. Review official instructions at FinCEN.gov.
4. **Consider independent legal advice.** A whistleblower attorney can assess eligibility, original-information requirements, confidentiality, possible retaliation protections, and timing.
5. **Avoid public accusations.** Sharing allegations or customer information online can create legal and privacy risks and may compromise an investigation.

The Bottom Line

Embezzlement, fraud schemes, bribery, tax crimes, securities fraud, and trade-based manipulation can all generate funds that someone may try to conceal or disguise. Financial institutions use BSA controls and SARs to help identify and report suspicious activity, but a SAR is a lead—not proof of guilt.



The AML/BSA whistleblower program offers a potential reporting path for people with original information about covered violations, including certain SAR, structuring, CDD, recordkeeping, and sanctions matters. Eligibility and awards depend on the law and the specific facts. When in doubt, document what you personally know, protect confidential information, check current FinCEN guidance, and seek independent legal advice before taking sensitive action.