Sanctions evasion rarely arrives labelled as such. In day-to-day bank compliance work, it may appear as a payment with an unusual intermediary, a customer whose ownership is difficult to establish, or a routine trade transaction that no longer fits the customer's known business. One anomaly is not proof of evasion. The work is to recognise patterns, test reasonable explanations and make a timely, documented escalation when the facts warrant it.

This article focuses on practical issues for professionals working with US sanctions and Bank Secrecy Act (BSA) obligations. It is general information, not legal advice. A bank's duties depend on its role, the applicable sanctions programme, the transaction and the facts.

What sanctions evasion can look like

Sanctions evasion involves conduct intended to circumvent or violate restrictions imposed by a sanctions authority. In banking, a customer or third party may try to hide a sanctioned person, jurisdiction, vessel, goods or other interest in a transaction. Evasion can involve deliberate deception, but a red flag alone does not establish intent or prove a sanctions breach.

Patterns that may call for closer review include:

- **Payment-chain concealment:** a party, bank or jurisdiction is removed from payment information, or payment instructions change in a way that obscures who benefits.
- **Opaque ownership or control:** a customer uses layers of companies, nominee directors or recently changed ownership without a credible commercial explanation.
- **Unusual intermediaries:** a transaction involves a third party with no apparent role, or funds pass through jurisdictions or institutions inconsistent with the stated trade route.
- **Trade-document inconsistencies:** descriptions of goods, shipping routes, counterparties or end users do not match across invoices, payment messages and other available records.
- **Changed customer behaviour:** a customer suddenly uses new counterparties, payment corridors or business lines that do not fit its established profile.

These examples are indicators, not a checklist for proving wrongdoing. A business may have legitimate reasons to use intermediaries or change routes. Compliance teams should assess the whole transaction and customer context, rather than treating one factor as conclusive.

Sanctions concerns and BSA violations are related, but not identical

Sanctions and AML controls often meet in the same transaction, but they answer different legal questions. Sanctions rules may prohibit dealing with certain persons, property, jurisdictions or interests. The BSA, by contrast, imposes requirements that include maintaining an AML programme and filing certain reports. A suspicious transaction may raise both kinds of concern, but a sanctions alert is not automatically a BSA violation.

When does a concern become a potential BSA violation?

For practical purposes, distinguish between a suspicious event and a possible failure to meet a legal or regulatory obligation. Examples that may warrant BSA review include a failure to maintain an effective AML programme, a material breakdown in required controls, or a failure to file a required suspicious activity report (SAR) when applicable. Whether a particular failure violates the law depends on the governing requirements and facts; not every control gap, delayed review or missed red flag has the same legal significance.

A sanctions-evasion pattern could be relevant to a SAR decision where the activity meets applicable reporting standards. SAR filing is not a finding that a customer committed a crime, and staff should not treat a filing as proof of guilt. Separate sanctions obligations, including whether a transaction must be blocked or rejected, require their own analysis under the relevant programme and rules.

Human error versus willful misconduct

This distinction matters. A single mis-keyed field, an isolated missed alert or a reasonable judgement call made with incomplete information may point to human error or a process weakness. It does not, by itself, establish deliberate misconduct. The assessment changes if records suggest someone knowingly bypassed a control, suppressed an alert, altered a file or discouraged a required escalation.

Look at what the person knew at the time, what procedures applied, what action they took, whether they raised the issue and whether similar events repeated. Do not infer intent from a bad outcome alone. Conversely, a series of dated warnings followed by deliberate overrides may warrant a more serious investigation than an isolated mistake.

Escalation: make the concern specific and timely

Escalation should move a concern to the right internal decision-makers without prejudging the conclusion. Follow the bank's procedures, which may direct staff to a manager, AML or sanctions team, compliance hotline, legal department or another designated channel. If a manager is implicated, use an alternative route. Record when the concern was raised and who received it.

A useful escalation explains the facts and the unresolved question. For example: "On 14 March, payment reference 4821 for Customer A included an intermediary not shown in the customer file. The invoice names Company B as the buyer, while the payment message names Company C. The customer's explanation, received on 16 March, does not address the difference. Please review the ownership and payment chain." This is more useful than "possible sanctions evasion" with no dates, transaction details or supporting basis.

Do not delay an escalation while trying to prove a case yourself. At the same time, avoid making unsupported accusations, accessing records outside your authority or alerting a customer to a confidential SAR process. A bank's internal process and any external reporting or blocking obligation may have different decision-makers and timelines.

Evidence and documentation that holds up

Good documentation lets another reviewer understand what happened, what was known, what steps were taken and why. It also helps distinguish a reasonable decision from an unexplained gap. Preserve records through approved systems and policies; do not create private copies or alter original material.

What to write down

- **Dates and identifiers:** transaction date, amount, currency, payment reference, customer name and relevant account or case number.
- **Observed facts:** the exact mismatch, unusual route, alert result or document discrepancy—separating what you saw from what you infer.
- **Source material:** where the information came from, such as a payment message, customer file, invoice, screening result or dated internal note.

- **Steps taken:** searches, checks and questions made, with dates and outcomes. Note unsuccessful checks as well as successful ones.
- **Escalation trail:** who was contacted, when, through which approved channel, and any response or decision.
- **Unresolved issues:** what remains unclear and what further review may be needed.

For instance, a dated case note might say: “18 April, 10:20: Screening alert reviewed against the customer’s legal name and date of incorporation. Potential match not confirmed; ownership information remains incomplete. Referred to sanctions team at 11:05 under case 77104.” That is more reliable than a later recollection that “the alert was checked”. Preserve relevant records in accordance with retention, confidentiality and legal-hold requirements.

Timing pressure and limitation periods

There are two clocks to keep in mind: operational deadlines and legal limitation periods. Operationally, sanctions decisions and suspicious activity reviews can be time-sensitive. A transaction may be pending, funds may be moving, or records may be overwritten under normal retention cycles. Follow the bank’s procedures promptly and seek direction from the appropriate team. Do not assume that an internal referral pauses a legal or regulatory deadline.

Legal limitation periods are a separate issue. Their length and starting point depend on the claim, the statute, the alleged conduct and other facts. A whistleblower considering a claim should not assume that a general limitation period applies or that reporting internally stops time from running. The BSA contains whistleblower provisions, and the rules for awards and retaliation protections are not interchangeable. A question about a possible claim should be put promptly to a lawyer familiar with the applicable whistleblower law.

The National Law Review has published coverage on filing an AML/BSA whistleblower lawsuit. Treat any article as a starting point, not a substitute for checking current law, court rules and the specific facts. When a deadline may matter, record the dates of the conduct, the internal escalation, any alleged retaliation and any external submission, then get independent legal advice without delay.



Anonymous versus identified submissions

“Anonymous” can mean different things: raising an internal concern without giving your name, asking an employer to keep your identity confidential, or submitting information to a government agency through a process that permits anonymity in some circumstances. These are not the same. A bank’s hotline rules and a regulator’s submission requirements may differ, and an anonymous report can be harder to follow up if the reviewer cannot ask questions.

Under the US BSA whistleblower framework, the route for submitting information and pursuing an award or retaliation protection can involve identity and procedural requirements. Do not assume that an unsigned message preserves eligibility for every protection or award. The National Law Review’s article may help orient a reader to the issue, but check the relevant statutory and agency requirements with a qualified lawyer.



Before choosing a route, consider confidentiality, retaliation risk, access to supporting records and whether the concern can be investigated without further questions. Keep a personal, lawful record of dates and communications, but do not remove confidential bank or customer information or breach data-handling rules. If you fear retaliation, document specific actions—such as a dated change in duties, a disciplinary notice or a threat—and seek advice https://www.lawyer-monthly.com/2026/10/top-10-bsa-whistleblower-tips-for-2027/ about safe reporting channels and deadlines.

Using FFIEC materials in compliance work

The Federal Financial Institutions Examination Council (FFIEC) provides supervisory resources, including the BSA/AML Examination Manual. These materials can help staff understand how examiners assess risk management, internal controls, independent testing, training and suspicious activity reporting. They are useful context for programme design and examination readiness, but they are not a substitute for the governing statute, regulations, sanctions rules or advice on a specific case.

Use FFIEC guidance to ask practical questions: Are alerts reviewed under a documented process? Are decisions and rationales retained? Do procedures cover relevant products and payment channels? Are repeat control failures tracked to remediation? A sound programme should make escalation possible and protect the integrity of the review—not merely generate more alerts.

A practical closing checklist

1. Describe the transaction and the mismatch using dates, identifiers and source records.
2. Separate confirmed facts from assumptions, and consider plausible explanations.
3. Escalate promptly through an approved channel; use an alternative route if the normal one is compromised.
4. Document actions, decisions, hand-offs and unanswered questions in the approved system.
5. Keep sanctions analysis, BSA reporting decisions and any whistleblower concern distinct, while recognising where they overlap.
6. If retaliation or a legal deadline is a concern, record the relevant dates and seek independent advice promptly.

In short, sanctions evasion may surface as a pattern of concealed parties, inconsistent documents or unexplained changes—not a single definitive clue. Effective compliance work depends on proportionate review, careful escalation and records that show what was known and done at the time. That approach helps teams take serious concerns seriously without confusing a mistake, an unresolved red flag and deliberate misconduct.