A company's claim that it has fixed a compliance problem does not answer the most important questions: How long did the problem last? Who knew about it? Did the fix address the cause, or only the latest finding? And what lexinter.net records show what happened over time?

Those questions matter in Bank Secrecy Act (BSA) compliance. BSA requirements generally call for covered financial institutions to maintain anti-money laundering (AML) programs, monitor activity, and report certain suspicious transactions. Transaction monitoring systems and suspicious activity reports (SARs) are central tools, but a system can exist on paper while failing in practice.

If failures were repeated or widespread, a remediation claim should be tested against evidence—not accepted as a conclusion. This article explains how systemic compliance failures may come to light, what changed with federal whistleblower incentives, and how to build a careful documentation timeline. It is general information, not legal advice.

What "We Fixed It" Does—and Does Not—Establish

A company may have corrected a software rule, cleared a backlog, updated a policy, or retrained staff. Those actions can be important. They do not, by themselves, establish that the underlying problem has been resolved or that earlier failures were isolated.

For example, a transaction monitoring system may have used thresholds that missed certain activity. A bank may then change those thresholds. But a fuller review would ask whether alerts were missed before the change, whether alert backlogs were handled appropriately, whether escalation procedures worked, and whether suspicious activity was reported when required.

The same distinction applies to SAR filing. A newly filed SAR may address one case; it does not automatically resolve questions about prior activity, delayed filings, deficient investigations, or a broader pattern of inadequate controls. Nor does a SAR filing, by itself, prove wrongdoing. SARs are confidential reports of suspicious activity, not findings of guilt.

Look for the underlying cause

Effective remediation usually requires more than a quick adjustment. Depending on the issue, relevant steps may include a lookback, independent testing, staffing changes, revised escalation criteria, quality controls, and validation that the fix works. The details matter: a control that works in a test environment may still fail under actual operating conditions.



For employees, the practical point is to distinguish what the company says it changed from what records show it changed, when it changed it, and whether the change addressed the full scope of the problem.

How BSA Problems Have Traditionally Come to Light

For many years, a major route to discovering BSA and AML weaknesses was examination and supervision. Federal and state regulators review covered institutions, test controls, inspect records, and may identify weaknesses in transaction monitoring, SAR processes, governance, or staffing. Examiners can require corrective action and refer matters for further consideration.

The Financial Crimes Enforcement Network (FinCEN) administers the BSA and receives SARs and other financial intelligence. It is not the same agency as the Department of Justice (DOJ), which prosecutes federal crimes, or the Securities and Exchange Commission (SEC), which oversees securities markets and can enforce securities laws. The Commodity Futures Trading Commission (CFTC) regulates derivatives markets and has its own enforcement authority. Which agency is relevant depends on the institution, conduct, and applicable law.

Examiner-driven discovery remains important. But an examination is a point-in-time review, and regulators cannot continuously observe every institution, system, or transaction. A control failure may have operated for years before an examination, internal audit, or law enforcement inquiry surfaced it.

Why a pattern over time matters

A single missed alert may result from human error. Repeated misses tied to the same system setting, management decision, staffing shortage, or ignored escalation can suggest a different problem. A pattern over time can help distinguish an isolated mistake from a systemic compliance failure.

That distinction can affect how regulators assess the adequacy of a compliance program, the quality of remediation, and whether conduct was concealed or allowed to continue. It does not mean every repeated error establishes a violation. The facts, legal duties, and evidence still matter.

Whistleblower Incentives and Formal Reporting Pathways

Federal policy has increasingly emphasized formal channels for people with relevant information to report potential violations. The Anti-Money Laundering Act of 2020 (AMLA) created a whistleblower award framework for certain information leading to successful enforcement actions. Congress later amended and strengthened that framework in legislation enacted in 2022.

FinCEN—the Treasury bureau that administers the BSA and receives financial intelligence—handles the AML whistleblower program. Under the amended structure, an eligible whistleblower may receive an award of at least 10% and no more than 30% of monetary sanctions collected in qualifying actions, if the statutory requirements are met. The award framework applies where monetary sanctions exceed $1 million. Meeting that threshold does not guarantee an award: eligibility, the quality and originality of the information, the outcome of the action, and other statutory factors matter.

The $1 million threshold is not a promise of a "huge payout." It is a statutory condition tied to qualifying enforcement actions and sanctions. The amount, if any, depends on the case and the applicable rules. The 2022 changes also addressed protections and procedures, including anti-retaliation remedies. Whistleblower programs are governed by detailed requirements, so a person considering a report should check current FinCEN guidance and consult qualified counsel about eligibility and safe handling of information.



Use the right channel

Different agencies handle different laws and markets. FinCEN is the primary federal agency for BSA administration and the AML whistleblower program. DOJ handles federal criminal prosecutions. The SEC and CFTC have separate whistleblower programs for matters within their respective jurisdictions. A report involving AML controls may also raise other legal issues, but that does not make every agency interchangeable.

Employees may also have internal reporting options, such as compliance, audit, an ethics hotline, or a board committee. Internal reporting can create a record and give the company a chance to respond. It does not necessarily replace reporting to a regulator, and it may not be the right first step in every situation. Retaliation concerns, imminent risks, confidentiality, and the possibility that records could be altered are reasons to seek individualized advice before acting.

Anti-Retaliation Protections and Emerging Case Law

Whistleblower protections are intended to discourage employers from punishing workers for protected reporting. Depending on the statute and circumstances, prohibited retaliation may include termination, demotion, threats, harassment, or other adverse treatment. The AMLA amendments expanded the framework for anti-retaliation claims and available remedies, but protection is not automatic in every workplace dispute.

Coverage can turn on issues such as whether the person made a protected report, to whom it was made, what information was provided, and whether the employer's action was connected to that report. Deadlines and procedural requirements may also apply. A person should not assume that an internal complaint, a regulator submission, or a general concern automatically satisfies every legal requirement.

Case law in this area continues to develop. Courts may be asked to interpret the boundaries of protected activity, the required connection between reporting and retaliation, and how statutory procedures apply. Outcomes are fact-specific, and a decision in one context may not control another. Anyone facing possible retaliation should preserve relevant records and obtain advice promptly rather than relying on broad summaries of a developing legal landscape.

Build a Documentation Timeline

When the issue is a pattern over time, chronology can be more useful than a pile of disconnected documents. A careful documentation timeline can help an attorney or regulator understand what was observed, what was reported, how the company responded, and whether the claimed fix matches the evidence.

Timeline item What to record Why it may matter Control or system issue When you observed it, the process involved, and the specific behavior—not assumptions about intent. Helps identify whether the problem was isolated or recurring. Internal reports Date, recipient, channel, and a factual summary of what you raised. Shows what the organization was told and when. Company response Actions promised or taken, responsible teams, and stated completion dates. Allows comparison between assurances and actual remediation. Potential retaliation Changes in duties, access, evaluations, discipline, or employment status, with dates and context. May help counsel assess whether conduct followed protected reporting.

Keep records lawfully and carefully

Do not take confidential customer information, copy restricted databases, access systems without authorization, or remove company records in violation of policy or law. Do not disclose SARs or information that would reveal whether a SAR was filed; SAR confidentiality rules are strict. A worker can record personal observations and preserve materials they are authorized to retain, but the right approach depends on the facts. Ask counsel before collecting or sharing sensitive records.

Use neutral, precise language. Separate what you personally observed from what someone told you, and label estimates or uncertainties. Preserve original dates and context where lawful. Avoid editing records to make them seem more conclusive than they are.

What This Means in Practice

If your company says "we fixed it," focus on verifiable questions rather than the phrase itself:

- What specific control failed, and for how long?
- Was the issue limited to one case, or did the same weakness appear repeatedly?

- Did the company review potentially affected activity from the earlier period?
- Were transaction monitoring rules, alert handling, and SAR decisions independently tested?
- Does the documented remediation match the problem identified?
- Were concerns escalated, and did anyone face adverse treatment after reporting them?

Do not assume that a long-running failure proves a crime, or that a recent fix erases prior conduct. Both conclusions require evidence and legal analysis. A documented timeline, careful handling of confidential information, and advice from counsel can help you evaluate next steps without overstating what you know.

Systemic compliance failures are often revealed through accumulated evidence: recurring control gaps, repeated warnings, unresolved audit findings, and remediation that does not reach the root cause. The practical task is to preserve a clear, lawful account of that pattern over time—and to use the appropriate reporting pathway for the issue.