Yes—but usually not because a bank's software missed an alert in isolation. A transaction monitoring system failure can become lexinter.net the basis for a Bank Secrecy Act (BSA) enforcement action when it points to a broader failure to identify, investigate, or report suspicious activity. The details matter: the institution's risk profile, the duration and reach of the problem, what management knew, and whether suspicious activity reports (SARs) were filed when required.

For years, regulators and law enforcement agencies uncovered many monitoring weaknesses through examinations, investigations, and reviews of institutional records. Today, employees and other insiders also have formal ways to report suspected violations—and, in some circumstances, may qualify for financial awards. Those pathways have made internal monitoring failures more likely to come to government attention.

This article explains how a system gap can support enforcement, how the whistleblower framework works, and what institutions should consider when they discover systemic alert failures.

What Counts as a Transaction Monitoring System Failure?

Transaction monitoring systems help financial institutions identify activity that may require investigation under the BSA. They may use rules, scenarios, thresholds, data models, or a combination of methods to flag transactions for review. A system does not have to detect every suspicious transaction. It does, however, need to be reasonably designed for the institution's risks and supported by effective controls.

A "failure" can mean more than a software outage. Common examples include:



- Scenarios or thresholds that do not reflect the institution's products, customers, or geographic risks.
- Data feeds that omit relevant transactions or customer information.
- Alerts that are improperly suppressed, routed, or closed.
- Backlogs so extensive that investigators cannot review alerts promptly.
- Staffing or training gaps that undermine investigations.
- Repeated failures to file SARs when the institution has identified facts that meet the reporting standard.

Not every alert that is not escalated is evidence of a violation. A bank may investigate an alert and reasonably conclude that the activity is not suspicious. The concern is whether the overall system and its governance are adequate—not whether a particular alert, viewed in hindsight, should have produced a SAR.

How BSA Enforcement Has Developed

Examiners and investigators have long found the gaps

Historically, many BSA enforcement matters began with examination or investigative work. Examiners reviewed risk assessments, alert queues, case files, SAR decisions, and management oversight. They could identify whether an institution's controls matched its actual business and whether known problems had been corrected.

Enforcement can involve more than one government body. The Office of the Comptroller of the Currency, the Federal Reserve, and other banking regulators supervise institutions and can take supervisory or enforcement action within their authority. FinCEN—the Treasury Department bureau that administers the BSA and receives SARs—can impose civil penalties and other remedies for BSA violations. The Department of Justice (DOJ) handles federal criminal prosecutions, including cases involving willful violations or related crimes. These roles can overlap, but they are not interchangeable.

Public enforcement actions have repeatedly focused on institutions that failed to maintain an effective anti-money-laundering program, including weaknesses in monitoring and SAR filing. A system defect may be important evidence, but the legal theory often concerns the institution's broader failure to comply with BSA obligations.

What examiners look at

When reviewing monitoring, examiners commonly ask whether an institution understood its risks, translated those risks into appropriate controls, tested the controls, and acted on identified weaknesses. They may compare transaction data with alert rules, examine aged cases, review tuning and validation, and trace whether management received accurate information about backlogs or missed activity.

A narrow defect may be manageable if it is detected quickly, assessed, and remediated. A prolonged weakness that affects a significant portion of activity is harder to characterize as an isolated technical problem—especially if warning signs were documented and left unresolved.

When Can Monitoring Gaps Support a BSA Enforcement Action?

There is no single formula. The question is usually whether the facts show a failure to maintain an effective BSA/AML program, a failure to file required SARs, or another violation—not simply whether the institution's system produced an imperfect result.

Several factors can increase enforcement risk:

- **Scale:** The gap affects many customers, transactions, business lines, or locations.
- **Duration:** The problem persists across multiple review cycles or examination periods.
- **Foreseeability:** Known risks, prior findings, or obvious data problems were not addressed.
- **Management awareness:** Reports identified backlogs or control weaknesses, but leaders did not provide resources or corrective action.
- **SAR consequences:** The weakness caused the institution to miss or delay reports it was required to file.

- **Remediation:** The institution did—or did not—identify the issue, assess its effects, and fix the underlying cause.

These factors are not a substitute for the applicable legal standard. They help explain why an agency may view systemic alert failures differently from a limited, promptly corrected defect.

Whistleblower Incentives and Formal Reporting Pathways

Internal and external reporting can bring a monitoring problem to government attention before an examination does. Employees may use internal compliance channels, report concerns to a regulator, or provide information through an authorized whistleblower process. A report is not itself proof of a violation, and it does not guarantee an investigation or award.

The Anti-Money Laundering Act of 2020 (AMLA) established a whistleblower program for certain original information about BSA violations and related money laundering. Congress later strengthened the framework through amendments enacted in 2022. FinCEN administers the program; it is the Treasury bureau that receives SARs and oversees the BSA whistleblower process.



The $1 million sanctions threshold and award range

The award framework is tied to successful enforcement, not simply to the seriousness of an allegation. In general, a qualifying whistleblower may be eligible for an award when original information leads to a successful enforcement action resulting in monetary sanctions exceeding $1 million. The award may be 10% to 30% of the monetary sanctions collected, subject to the statute and program rules.

The threshold is important. A report that helps an agency identify a real weakness does not automatically produce an award. The statutory conditions must be met, including the required enforcement result and sanctions. The award percentage also depends on the circumstances; it is not automatically 30%.

Issue Practical point Qualifying information Generally, the information must be original and lead to a successful covered enforcement action. Sanctions threshold Monetary sanctions must exceed $1 million for the award framework to apply. Potential award The statutory range is generally 10% to 30% of monetary sanctions collected. Administrator FinCEN administers the BSA whistleblower program.

Employees should not assume that taking or disclosing confidential records is protected simply because they believe they have uncovered misconduct. The rules governing submissions, confidentiality, and eligibility are technical. Anyone considering a report may want independent legal advice about lawful ways to preserve and provide information.

Anti-Retaliation Protections and Emerging Case Law

AMLA also provides anti-retaliation protections for covered whistleblowers. The protections address employment actions taken because a person provided information to the government or participated in a covered proceeding. Remedies may include reinstatement, back pay, and other relief allowed by law, subject to statutory requirements and procedures.

Coverage is not a blanket shield for every workplace dispute. The facts matter: what the employee reported, to whom, whether the report falls within the law, and whether the employer's action was connected to protected activity. Timing can be evidence, but timing alone does not establish retaliation.

What the developing case law means

The AMLA whistleblower framework is newer than established programs such as the SEC whistleblower system, so its published case law remains comparatively limited. Courts may have to address questions about the scope of protected activity, procedural requirements, causation, and the remedies available. Decisions under other whistleblower laws may offer context, but they do not automatically control AMLA claims.

For employers, that uncertainty is a reason to handle complaints carefully—not a reason to assume the law is irrelevant. A sound response includes documenting the complaint, preserving relevant records, limiting access to information on a need-to-know basis, and ensuring that employment decisions are supported by legitimate, consistently applied reasons. Retaliation against an employee who raised a compliance concern can create a separate legal problem even if the underlying allegation is ultimately not substantiated.

What This Means in Practice

For financial institutions, the central issue is not whether a transaction monitoring system is flawless. It is whether the institution can show that its controls are risk-based, tested, and responsive to problems—and that it took SAR filing obligations seriously.

When an institution finds a material monitoring gap, a disciplined response generally includes:

1. **Contain the issue.** Identify affected products, systems, time periods, and transaction populations.
2. **Preserve evidence.** Retain relevant alert data, model and rule versions, change records, case files, and governance materials.
3. **Assess reporting impact.** Determine whether prior activity requires investigation or SAR filing, using qualified compliance and legal personnel.
4. **Fix the cause.** Address data, scenario design, staffing, workflow, or oversight problems—not just the visible symptom.
5. **Document decisions.** Record the scope of the review, conclusions, remediation, and any unresolved issues.
6. **Protect reporting channels.** Handle employee concerns without retaliation and preserve the integrity of internal and external reporting processes.

A rushed response can create a second problem: fixing alerts while leaving the underlying data, governance, or SAR decision process untouched. Conversely, a well-documented investigation and prompt remediation can help demonstrate that the institution treated the issue as a control failure requiring attention rather than as an inconvenience.

Bottom Line

Monitoring system gaps can support a BSA enforcement action when they reveal a meaningful failure in the institution's AML program or contribute to missed SAR obligations. Examiners remain a major source of discovery, but AMLA's whistleblower framework gives qualifying insiders another formal reporting path and, in eligible cases, a potential award when monetary sanctions exceed $1 million.

For institutions, the practical test is whether they can detect weaknesses, understand their scope, file required SARs, and correct the underlying controls. For employees, the key is that whistleblower protections and awards have specific legal requirements. Neither a system defect nor a report alone decides the outcome; the surrounding facts do.