Short answer: An employer may not lawfully retaliate against you for certain protected whistleblowing, but raising a concern about suspicious activity reports (SARs) or a transaction monitoring system does not automatically make every complaint legally protected. The details matter: what you reported, to whom, how you reported it, and whether the conduct falls within a law that protects your disclosure.



This is a developing area of law. The Anti-Money Laundering Act of 2020 (AMLA) expanded protections and created financial incentives for certain whistleblowers, but important questions—including how protections apply to particular employees and complaints—continue to be tested. If you face discipline or termination after reporting a problem, speak with an employment or whistleblower attorney promptly. Filing deadlines can be short.

What SAR and monitoring concerns can look like

A SAR is a report that a covered financial institution files with the Financial Crimes Enforcement Network (FinCEN), the U.S. Treasury bureau that administers the Bank Secrecy Act (BSA) and receives SARs. A SAR is not a criminal accusation or a finding that a customer committed a crime. It is a confidential report of activity that may warrant review by law enforcement or regulators.

Employees may raise concerns about issues such as:

- Transaction monitoring rules that appear to miss suspicious patterns or generate alerts that are routinely ignored.
- Pressure to close alerts without adequate investigation or documentation.
- Backlogs, staffing gaps, or model changes that could undermine alert review.
- Decisions not to file a SAR despite facts that appear to require escalation under the institution's procedures.
- Possible SAR confidentiality breaches or improper disclosure that a SAR was filed.
- False records, misleading statements, or efforts to conceal a compliance weakness from examiners or law enforcement.

Not every disagreement about a model, threshold, or filing decision is evidence of a violation. A good-faith concern may still be worth escalating, but the legal analysis depends on the facts and the reporting pathway.

How BSA enforcement developed

The BSA requires covered financial institutions to maintain anti-money-laundering controls, including procedures for identifying and reporting suspicious activity. The Department of the Treasury's Office of the Comptroller of the Currency (OCC), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and other regulators examine institutions they supervise. The Department of Justice (DOJ), which investigates and prosecutes federal crimes, may also pursue criminal cases. These agencies have different roles; an examiner's finding is not the same thing as a criminal prosecution.

For many years, significant BSA and AML weaknesses often came to light through regulatory examinations, internal audits, law-enforcement investigations, or enforcement actions after problems had persisted. Examiners could identify gaps in controls, documentation, staffing, or alert handling. Institutions could face remediation requirements, civil money penalties, or—in serious cases—criminal exposure.

That history matters to employees. A transaction monitoring complaint may concern a technical issue, such as a poorly calibrated rule, or a broader control failure, such as management directing staff to disregard alerts. Examiners assess an institution's overall program, but an employee's potential protection depends on the applicable whistleblower law—not simply on whether an examiner later agrees there was a weakness.

The shift toward formal whistleblower pathways

AMLA, enacted in 2021, expanded the BSA whistleblower framework. It provides a process for eligible individuals to submit information to the Treasury Secretary about possible BSA violations or violations of certain related laws. The framework also allows for awards in qualifying cases and includes anti-retaliation provisions.

The change reflects a broader enforcement approach: regulators and law-enforcement agencies may benefit from timely, specific information from people who understand how a compliance program works day to day. Formal reporting pathways can give a whistleblower a way to provide information outside the employer's internal chain of command. They do not guarantee that an agency will lexinter investigate, bring an enforcement action, or award money.

For clarity, the Securities and Exchange Commission (SEC) handles whistleblower awards and retaliation claims under certain securities laws, while the Commodity Futures Trading Commission (CFTC) has its own whistleblower program for violations within its jurisdiction. Neither agency administers the BSA program simply because a complaint involves a bank or AML controls. FinCEN and the Treasury framework are central to BSA reporting; DOJ and regulators may become involved in investigations or enforcement under their respective authorities.

What the AMLA award structure says

Under the AMLA framework, an eligible whistleblower may receive an award when the person voluntarily provides original information that leads to a successful enforcement action resulting in monetary sanctions above the statutory threshold. The potential award is generally between 10% and 30% of collected monetary sanctions, subject to the law and applicable rules.

The key threshold is **more than $1 million in monetary sanctions** in a covered action. That threshold is not a promise of a payout. An award depends on factors such as the quality and usefulness of the information, the whistleblower's role, whether the information was already known, and the amount of money actually collected. The award program has also undergone rulemaking and implementation, so potential claimants should check current Treasury requirements rather than rely on older summaries.

There is a separate question: whether you are protected from retaliation. A person does not necessarily have to qualify for an award to have a retaliation claim. Conversely, making a report that could be considered for an award does not mean every employment action that follows is automatically unlawful. The award and anti-retaliation analyses are related but distinct.

Anti-retaliation protection: what is protected?

AMLA's anti-retaliation provision generally addresses covered employers taking adverse employment action because an employee lawfully provided information about a possible BSA violation to specified recipients, including the employer or the Treasury Secretary, subject to statutory conditions. The law also provides a process for seeking relief, including reinstatement, back pay, and other remedies where available.

Whether a particular internal report is protected can turn on the law's language and the facts. For example, an employee who reports that a monitoring system is missing suspicious transactions may be raising a possible BSA issue. But a complaint about a software preference, ordinary workload dispute, or policy disagreement may not qualify unless it relates to a reasonably identified legal violation and satisfies applicable requirements.

Other laws may apply, too. Depending on the facts, protections could arise under another federal statute, state whistleblower law, or employment law. Coverage varies by employer, role, subject matter, and reporting method. A contract, compliance policy, or professional obligation may also matter, but those are not substitutes for statutory protection.

Retaliation after SAR concerns: what can count?

Retaliation is not limited to firing. It can include a demotion, pay cut, suspension, undesirable reassignment, threats, exclusion from key work, or other materially adverse treatment. A negative performance review or increased scrutiny may be relevant, especially if it begins soon after a report, but timing alone does not prove unlawful retaliation.

Employers may argue that a personnel decision was based on performance, restructuring, or misconduct unrelated to the disclosure. The evidence often matters more than the label each side uses. Relevant facts can include:

- When you raised the concern and when the adverse action began.
- Whether decision-makers knew about your report.
- How the employer treated similarly situated employees.
- Whether the stated reason changed over time or conflicts with records.
- Whether you followed the reporting process and kept a clear, factual record.

Courts and agencies are still working through the reach of AMLA's protections and how they interact with other whistleblower laws. The emerging case law is fact-specific; there is no universal rule that every

employee who flags a SAR or monitoring issue is protected, or that every subsequent termination is retaliation.

What this means in practice

1. Make the concern specific

Describe the control, process, or decision that concerns you. For example, identify the monitoring rule or alert queue, the dates involved, the relevant procedure, and what you observed. Distinguish firsthand facts from assumptions. A specific report is easier to assess than a broad claim that the AML program is "broken."

2. Use a suitable reporting channel

Depending on the situation, that might be a manager, compliance officer, internal hotline, legal department, board committee, regulator, or the appropriate government whistleblower channel. Internal reporting can create a record and prompt remediation, but it may not be appropriate in every case—particularly if senior personnel are implicated or evidence may be at risk. An attorney can help identify a lawful and safe route.

3. Protect confidential information

SARs and information revealing whether a SAR was filed are subject to strict confidentiality rules. Do not copy or send SARs, customer records, or other sensitive material to a personal account unless a lawyer advises that a specific, lawful process permits it. Avoid discussing SAR status with the customer or unauthorized people. Whistleblower rights do not create a general license to disclose protected information.

4. Keep a lawful record

Write down dates, participants, what you reported, and the response. Preserve relevant communications only in ways permitted by law and company policy. Do not alter records, access files outside your authorization, or take confidential data you are not entitled to possess. If you are unsure what you may retain, ask counsel before doing so.

5. Get advice before a deadline passes

Some whistleblower statutes require a complaint to be filed within a defined period and through a particular process. AMLA claims may have specific administrative steps and timing rules. Deadlines can differ from those under other laws, and an internal investigation may not pause them. An attorney can evaluate the applicable route, whether the disclosure was protected, and what remedies may be available.

Frequently asked questions

Can I be fired for saying a SAR should have been filed?

Not necessarily. If you raised a good-faith concern about a possible BSA violation through a protected channel, firing you because of that report may violate applicable anti-retaliation law. But a disagreement about a filing decision is not automatically protected, and the facts and legal framework matter.

Do I have to report outside the company?

Not always. AMLA's framework can cover certain disclosures to an employer as well as reports to the Treasury Secretary, subject to the statute's requirements. Other laws may set different rules. Do not assume that an internal report, an external report, or both are required without checking the law that applies to your situation.

Does a weak monitoring system prove the employer violated the law?

No. A weakness may warrant review, but whether it amounts to a legal violation depends on the institution's obligations and the facts. Examiners and enforcement agencies assess evidence, controls, and remediation; an employee's concern is a signal to examine, not a final determination.

Bottom line

Retaliation after SAR concerns can raise serious legal issues, but protection is not automatic. AMLA created a formal BSA whistleblower framework, potential awards tied to successful actions exceeding the **$1 million sanctions threshold**, and anti-retaliation protections. The precise coverage of a transaction monitoring complaint depends on what you disclosed, how you disclosed it, and the circumstances of any employment action.



Be factual, protect SAR confidentiality, document events lawfully, and get prompt legal advice if you are threatened, disciplined, or fired after raising a concern. This article is general information, not legal advice for a specific case.