For years, many Bank Secrecy Act (BSA) problems came to light through a familiar channel: a financial institution's own controls—or an examiner's review of those controls. Examiners might find gaps in transaction monitoring, question the handling of suspicious activity reports (SARs), or identify failures that later led to enforcement. That model still matters. But https://www.lexinter.net/the-rise-of-bsa-whistleblower-lawsuits it does not depend on the people closest to a problem deciding to speak up.

"Lowering the informational barrier to disclosure" means making it easier for people with relevant knowledge to recognize potential misconduct, find a reporting route, and understand the risks and protections involved. It does not mean every employee has a winning claim or that every tip leads to an award. It means formal whistleblower pathways can help move useful information beyond the institution's internal controls and into the hands of authorities.

In practice, the change involves more publicized awards, clearer anti-retaliation rules, and greater awareness of the program. It may also make it easier to find counsel who understands the rules. Those changes can matter especially in AML compliance, where key facts may sit in alerts, escalation records, SAR decision-making, and communications about whether to fix a known control weakness.



How BSA enforcement traditionally surfaced problems

The BSA requires financial institutions to maintain programs designed to detect and report certain suspicious activity. Those programs can include customer due diligence, transaction monitoring systems, internal escalation procedures, and SAR filing. The law and its implementing rules are enforced through several channels, not a single agency.

The Financial Crimes Enforcement Network, or FinCEN, is the Treasury bureau that administers the BSA and receives SARs. Federal banking regulators examine the institutions they supervise and may identify compliance deficiencies. The Department of Justice (DOJ) investigates and prosecutes federal crimes. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have separate roles when conduct falls within their markets and jurisdiction.

Historically, BSA enforcement often grew out of examiner-driven discovery. An examiner could review a bank's written program, test sample transactions, assess how alerts were investigated, and evaluate whether SAR decisions were timely and adequately documented. A regulator might then require remediation or refer a matter for further action. Law enforcement could also develop a case through its own investigation.

This system can uncover serious failures. But it has a built-in limit: reviewers can only test what they can see and what the institution's records reveal. A person inside the organization may know that managers ignored repeated warnings, altered escalation practices, discouraged SAR filing, or treated monitoring gaps as a cost of doing business. That information may not be obvious from a sample of files or a written policy.

From examiner discovery to formal reporting pathways

Whistleblower programs add another source of information. They give people with first-hand knowledge a route to report possible violations to government authorities, sometimes with the possibility of an award if their information contributes to a qualifying enforcement action.

That is a meaningful shift in emphasis. The goal is not to replace examination or internal compliance. It is to give individuals a reason—and a defined process—to report information that might otherwise remain inside an organization. A whistleblower could, for example, provide evidence about how a transaction monitoring system was configured, how alerts were handled, or whether senior staff knew that a control was failing.

"Lowering the informational barrier" is partly about practical access. A person needs to know that a program exists, understand what information may qualify, and be able to find a reporting channel. If the process is unfamiliar, people may assume that only executives or compliance officers can report, or that they must first prove a complete legal violation. A formal program can make clear that a person may submit relevant information even if the government—not the whistleblower—ultimately decides whether to investigate or bring a case.

Awareness of the program matters

Rules do little if potential whistleblowers do not know about them. More publicized awards can increase awareness of the program and show that reporting can have real consequences. Publicity can also help employees recognize that AML information may matter even when it looks like an internal control issue rather than a headline-grabbing crime.

But awareness should not be confused with an automatic payout. An award depends on statutory requirements, the quality and usefulness of the information, the outcome of the government action, and the amount of qualifying sanctions collected. A tip that is vague, already known to authorities, or unrelated to a covered action may not qualify.

The AML whistleblower award structure

The Anti-Money Laundering Act of 2020 (AMLA) created an award framework for eligible whistleblowers who provide original information leading to successful enforcement of covered violations. Congress later addressed important implementation and protection issues in legislation enacted in 2022 as part of the National Defense Authorization Act for Fiscal Year 2023.



The central award structure allows an eligible whistleblower to receive between 10% and 30% of monetary sanctions collected in a qualifying covered action, including certain related actions, when the sanctions exceed $1 million. The $1 million figure is a threshold for the qualifying action; it is not a promise that a whistleblower will receive $1 million. The award is a percentage of sanctions collected, and the final amount depends on the law and the facts of the case.

Program feature What it means Potential award Generally 10% to 30% of qualifying monetary sanctions collected, subject to statutory rules and agency determinations. Sanctions threshold The covered action must involve more than $1 million in monetary sanctions for the award framework to apply. Information The information must meet program requirements, including rules concerning originality, usefulness, and the whistleblower's role. Outcome An award is tied to a qualifying successful enforcement action and sanctions collected—not simply to submitting a tip.

The 2022 legislation also addressed the practical problem of funding awards and strengthened the statutory framework, including anti-retaliation protections. These changes helped make the program more operational. They did not remove the need to satisfy eligibility rules or guarantee a particular result.

What this means in practice

For someone working in AML, relevant information may be more specific than "the bank has a bad compliance program." It might include dated escalation emails, evidence that known monitoring gaps were left unresolved, internal instructions about how to handle certain alerts, or records showing that suspicious activity was repeatedly reviewed but not reported.

Transaction monitoring systems can generate large volumes of alerts, and an alert by itself does not establish a violation. The details matter: what the system was designed to detect, what the institution knew about its limitations, how investigators handled alerts, and whether management responded to documented risks. Similarly, a SAR filing decision involves sensitive information and legal obligations. A whistleblower should distinguish reporting underlying facts from disclosing a SAR itself.

SARs are confidential under federal law. A person should not assume that the existence or contents of a SAR may be freely shared, even when trying to report wrongdoing. The safer course is to get advice on how to describe relevant conduct without unlawfully disclosing a SAR or other protected information. A

whistleblower submission to an authority does not automatically make every underlying document appropriate to disclose.

FinCEN administers the BSA and receives SARs; it is not the same agency as DOJ, which prosecutes federal crimes. Depending on the facts, information may be relevant to FinCEN, a federal regulator, DOJ, or another authority. A person should not assume that submitting information to one agency automatically submits it to every agency that may have jurisdiction.

Anti-retaliation protections and emerging case law

The AML whistleblower framework prohibits certain forms of retaliation against individuals who make protected disclosures. The 2022 amendments strengthened the statutory protections and provided a route for eligible whistleblowers to bring retaliation claims. Potential remedies can include reinstatement, back pay, special damages, and attorneys' fees, subject to the statute and the circumstances of the claim.

Protection is not the same as immunity from every workplace consequence. The details matter: what was reported, to whom, whether the disclosure was protected, the timing of an employer's actions, and whether the person followed applicable procedures. A worker may also have obligations concerning confidential information, trade secrets, privileged material, or SAR confidentiality. Legal advice before disclosure can help identify those boundaries.

Case law and agency practice in this area continue to develop. Courts may be asked to interpret who is covered, what counts as a protected disclosure, what procedures apply, and what remedies are available. That makes it risky to rely on a general internet summary for a specific situation. It also makes contemporaneous documentation important: dates, recipients, the substance of internal reports, and any later changes in job duties or treatment.

Why it may be easier to find counsel

As the program becomes more visible, it may be easier for potential whistleblowers to find counsel familiar with AML reporting and retaliation issues. That does not mean every lawyer handles these cases, or that a lawyer can guarantee an award. It means public discussion of the program can help people identify the right questions before they submit information or confront an employer.

Before contacting counsel, a person can write down a factual timeline and identify the records they can lawfully access. They should not remove documents, access systems without authorization, or send sensitive materials to personal accounts. Counsel can help assess the reporting route, preserve evidence appropriately, and avoid disclosures that could compromise a case or violate confidentiality rules.

The bottom line

Lowering the informational barrier to disclosure means making it more realistic for people with first-hand knowledge to understand and use formal reporting pathways. In AML matters, that can bring information about transaction monitoring failures, escalation practices, and SAR filing decisions to the attention of authorities—not only examiners.

The award framework, the more publicized awards, and anti-retaliation provisions can encourage reporting. They do not make every tip a qualifying claim or every case an award. The practical questions remain: Is the information original and useful? Does it concern a covered violation? Does the action meet the $1 million

sanctions threshold? And can the person report safely, without improperly disclosing a SAR or other protected material?

For a potential whistleblower, the first step is informed, careful advice—not an assumption of a payout. For institutions, the lesson is equally direct: effective controls depend not only on what examiners can find, but also on whether employees believe they can raise serious concerns without being punished for doing so.