A crypto company can have written anti-money-laundering (AML) policies and still have serious control failures. The more useful question is whether its controls work in practice: Do they identify risky activity, prompt timely investigation, and lead to appropriate action?

For covered businesses, the Bank Secrecy Act (BSA) requires systems designed to detect and report certain suspicious activity. A company's duties depend on what it does and how it is classified. Many businesses that exchange or transmit convertible virtual currency may be treated as money services businesses and subject to BSA obligations, including registration, an AML program, recordkeeping, and suspicious activity reporting.

Red flags are not proof of a violation by themselves. They are reasons to look more closely at a company's risk assessment, transaction monitoring systems, alert decisions, and suspicious activity reports (SARs) filing. They may surface through regulators' examinations—or through people inside the company using formal reporting channels.

How BSA enforcement has changed

Historically, many BSA failures came to light through examiner-driven discovery. Bank and money-services-business examinations, law-enforcement investigations, and follow-up reviews could expose weak controls: missing procedures, inadequate monitoring, or suspicious activity that went unreported. In crypto, those same basic failures can sit alongside rapid growth, complex products, and activity spread across blockchain networks and jurisdictions.

The agency that administers the BSA's financial-crime reporting framework is the Financial Crimes Enforcement Network (FinCEN), part of the U.S. Department of the Treasury. FinCEN receives SARs and administers key BSA requirements. The Department of Justice (DOJ), by contrast, prosecutes federal crimes. Other regulators have distinct roles: the Securities and Exchange Commission (SEC) oversees securities markets, while the Commodity Futures Trading Commission (CFTC) oversees derivatives markets and certain commodity-related activity. Their enforcement roles should not be treated as interchangeable.

Enforcement is only one way problems come to light. The Anti-Money Laundering Act of 2020 (AMLA), followed by amendments enacted in 2022, strengthened the federal whistleblower framework for certain money-laundering and BSA-related reports. That shift creates a more formal route for people with relevant information to raise concerns. It does not mean every complaint qualifies for an award, or that every allegation is substantiated.

Common operational red flags

1. Wallet screening gaps

A company's controls may focus on customer identity while overlooking the wallets and counterparties involved in transactions. That can leave a gap between knowing who opened an account and understanding where funds came from, where they are going, or whether they are linked to a higher-risk service or sanctioned party.

Potential warning signs include:

- No documented process for screening wallet addresses or assessing exposure to higher-risk counterparties.

- Screening performed only at onboarding, with no meaningful ongoing review.
- Wallet risk indicators are collected but do not feed into transaction monitoring or case review.
- Controls cannot explain how they handle indirect exposure, such as funds that pass through several addresses.
- Material changes in blockchain analytics coverage, vendor performance, or supported networks are not assessed.

Wallet analytics can produce uncertain or incomplete results. The red flag is not that a system fails to label every address perfectly; it is that the company has no reasonable process for evaluating limitations, investigating relevant exposure, and documenting decisions.. It's not always that simple, though

2. High-risk geo exposure without a clear response

Geographic risk can arise through customer location, transaction counterparties, access patterns, or business relationships. A company may also face risk when customers use tools or intermediaries that make location difficult to establish. The issue is whether the company has assessed those risks and built controls that match them.

Warning signs include a risk assessment that ignores cross-border activity, inconsistent location checks, or a policy that lists higher-risk jurisdictions without explaining what the company does when exposure appears. Another concern is a sharp increase in activity connected to a region or corridor without additional review, escalation, or documented risk-based decisions.

Geographic indicators should not be treated as automatic evidence of wrongdoing. They should prompt the company to apply its stated controls, consider relevant transaction context, and document the outcome.

3. Override of compliance alerts

Transaction monitoring systems generate alerts; people and processes determine what happens next. An alert override can be appropriate when an investigator documents a sound reason. Repeated overrides without clear support are a different matter.



Look for patterns such as:

- Alerts closed with generic notes, such as “customer reviewed,” without analysis of the activity.
- Business or sales staff routinely pressing compliance to clear alerts or keep accounts open.
- High-risk alerts downgraded without an independent reviewer or recorded rationale.
- Overrides concentrated in a particular team, customer segment, product, or revenue channel.
- Managers evaluated on growth or retention without meaningful accountability for control decisions.

Management reporting should make override patterns visible. A single defensible decision may be ordinary. A recurring pattern that suppresses escalation, especially when linked to commercial pressure, deserves closer review.

4. Monitoring rules that do not reflect the business

A monitoring system is not effective just because it produces alerts. Its scenarios, thresholds, and data inputs should reflect the company’s products, customers, transaction types, and risk assessment. A system built for one business model can miss risks in a new product or a changed transaction flow.

Think about it: red flags include unexplained gaps in data, rules that have not been tested after a product launch, thresholds set so high that meaningful activity rarely alerts, or a large backlog that prevents timely investigation. A company should be able to explain how it tests monitoring coverage and updates it when risks change.

5. Weak SAR decisions and filing practices

A covered business may need to file a SAR when it knows, suspects, or has reason to suspect qualifying suspicious activity under the applicable rules. A filing decision should follow investigation and analysis—not an automatic rule that every alert becomes a report, or that no report is filed unless a specific dollar threshold is reached.

Possible red flags include repeated late filings, missing case records, unclear escalation criteria, or a small compliance team unable to handle the volume of alerts. Another warning sign is a process in which business personnel effectively control whether compliance may file. SARs are confidential; companies must not disclose a SAR’s existence to the person involved, subject to applicable legal rules. Poor confidentiality controls can create a separate problem.

Examiners and investigators may compare the company’s risk profile, monitoring output, case files, and filing decisions. A mismatch—for example, many high-risk alerts but almost no documented investigations—can invite questions about whether the controls work as described.

6. Paper policies without resources or oversight

An AML program can fail because it lacks trained staff, independent testing, usable procedures, or access to necessary data. Red flags include compliance reporting that bypasses meaningful senior oversight, audit findings left unresolved, and repeated reliance on vendors without testing whether their tools meet the company’s needs.

Outsourcing a screening or monitoring tool does not, by itself, transfer the company’s responsibility for its own program. The company should understand the tool’s limits, review performance, and retain records showing how decisions were made.

What whistleblower pathways add

Under the AMLA framework, certain individuals who voluntarily provide original information to the Treasury Department or DOJ may qualify for a monetary award if the information leads to a successful enforcement action and the statutory requirements are met. The Treasury Department administers this BSA and money-laundering whistleblower framework through FinCEN.



The award structure provides for an award generally ranging from 10% to 30% of monetary sanctions collected in qualifying actions, subject to statutory rules and available funds. The $1 million threshold matters: the award framework applies to qualifying actions in which monetary sanctions exceed $1 million. That is a threshold for the award program, not a rule that every suspected BSA violation must involve at least $1 million.

These awards are not automatic. Eligibility depends on factors such as whether the information is original, whether it meaningfully contributes to a successful action, and whether statutory exclusions apply. The framework is also distinct from programs administered by the SEC or CFTC, which have separate laws and eligibility rules.

Anti-retaliation protections and emerging case law

The AMLA also provides anti-retaliation protections for amla whistleblower improvement act 2022 certain employees who report suspected violations or participate in protected processes. Depending on the facts, a worker may have remedies such as reinstatement, back pay, and attorney fees. Statutory procedures and deadlines matter; a person considering a claim should promptly consult qualified counsel rather than assume that an internal complaint alone preserves every right.

Case law in this area is still developing. Courts may need to address how statutory protections apply to particular reports, what counts as protected activity, and how retaliation claims interact with other whistleblower laws. Decisions under securities or commodities statutes can offer context, but they do not automatically determine the outcome of an AMLA claim. The governing statute and the facts of the specific case remain central.

What this means in practice

For a crypto company, a credible AML review should test how controls operate—not just whether policies exist. A focused review can ask:

1. Does the risk assessment cover the company's actual products, customers, geographies, and transaction flows?
2. Are wallet screening and transaction monitoring connected to documented investigation procedures?
3. Can the company explain alert closures, overrides, and escalation decisions?
4. Are SAR decisions timely, consistent, confidential, and supported by case records?
5. Do compliance staff have adequate independence, staffing, data, and senior-management access?
6. Are audit findings and system limitations tracked through to resolution?

Red flag Practical question Wallet screening gaps How does the company identify and investigate relevant wallet exposure over time? High-risk geo exposure Do controls respond to geographic risk in a documented, risk-based way? Override of compliance alerts Are overrides supported, independently reviewable, and monitored for patterns? Weak SAR filing Can the company show timely, reasoned decisions and appropriate confidentiality?

The clearest warning is often not one suspicious transaction. It is a repeated disconnect between what a company's systems flag, what investigators document, what management allows, and what the company ultimately reports. That disconnect can be visible to examiners, investigators, or employees with access to the underlying records.

This article is general information, not legal advice. AML obligations and whistleblower rights depend on the company's activities, applicable law, and specific facts.