Yes—many crypto exchanges are covered by the Bank Secrecy Act (BSA), but coverage depends on what the business does, where it operates, and which customers or transactions it serves. In the United States, an exchange that accepts and transmits convertible virtual currency may be treated as a money services business and required to maintain an anti-money laundering (AML) program. That can mean customer identification, transaction monitoring, recordkeeping, and filing suspicious activity reports (SARs).

The practical question is not simply whether a company calls itself an "exchange." Regulators look at the activities it performs. A trading platform, wallet provider, or other virtual asset service provider may face different obligations depending on its role in moving or safeguarding funds.

This guide explains how the BSA applies, how enforcement has developed, and what the newer whistleblower framework means for digital asset compliance.

What the BSA requires of covered crypto businesses

The BSA is the federal framework for financial institutions' recordkeeping, reporting, and AML obligations. The Financial Crimes Enforcement Network (FinCEN), the U.S. Treasury bureau that administers the BSA and receives certain financial reports, sets rules and guidance for covered businesses. FinCEN's role is different from that of the Department of Justice (DOJ), which prosecutes criminal cases, or the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC), which regulate securities and derivatives markets.

FinCEN has said that certain businesses exchanging or transmitting convertible virtual currency can qualify as money services businesses, including money transmitters. The analysis is activity-based. A company that merely develops software or provides a platform without accepting or transmitting funds may be treated differently from one that takes custody of customer assets or executes transfers.

A covered business generally must register with FinCEN as a money services business when required, establish an AML program, and meet applicable reporting and recordkeeping obligations. State money-transmitter laws may apply separately. A business can also face other federal or state requirements depending on its products, customers, and operations.

Core AML program elements

A BSA-compliant AML program is not just a policy document. It needs to work in practice and be tailored to the risks of the business. Typical elements include:

- **Internal controls:** Written procedures for identifying customers, assessing risk, reviewing activity, and escalating concerns.
- **A designated compliance officer:** Someone with authority, access to resources, and responsibility for administering the program.
- **Training:** Role-appropriate instruction for employees and relevant contractors.
- **Independent testing:** Periodic review of whether controls operate as intended and whether deficiencies are corrected.
- **Transaction monitoring:** Rules and investigations designed to identify activity that may be inconsistent with a customer's profile or otherwise suspicious.
- **Reporting and records:** Timely SAR filing when required, along with retention of specified records and supporting documentation.

Transaction monitoring systems can help identify patterns such as rapid movement of assets, unusual transaction volume, activity involving high-risk services, or behavior that differs from a customer's expected use. But a system is only as useful as its data, scenarios, thresholds, investigations, and escalation process. Automated alerts do not replace judgment or a documented review.

When must a crypto exchange file a SAR?

A covered money services business generally must file a SAR when it knows, suspects, or has reason to suspect that a transaction meets applicable reporting criteria—for example, that it involves funds from illegal activity, is designed to evade BSA requirements, or has no apparent lawful purpose and lacks a reasonable explanation after review. The precise rules depend on the institution and transaction.

A SAR is a confidential regulatory report. It is not a public accusation, and filing one does not prove that a customer committed a crime. Businesses generally must not disclose the existence of a SAR to the person involved. They should preserve the supporting analysis and follow applicable rules for filing, confidentiality, and record retention.

For a crypto exchange, the work can be complicated by pseudonymous blockchain addresses, off-platform activity, rapid transfers, and limited information about counterparties. These challenges make it important to combine on-chain indicators with customer information, transaction context, and a defensible investigation process.

What enforcement history tells exchanges

For years, BSA enforcement often surfaced through regulators' examinations and government investigations. Examiners reviewed a firm's controls, testing, staffing, and handling of suspicious activity. Investigators could then pursue civil or criminal consequences when they believed the business had failed to meet legal obligations or had engaged in other misconduct.

That history matters because a regulator may discover a weakness through routine oversight—not only after a dramatic law-enforcement case. In the crypto sector, scrutiny has included questions about whether businesses registered when required, whether their AML programs matched their business models, and whether they detected and reported suspicious activity effectively.

In practice, examiners and investigators may look beyond whether a written policy exists. They can ask whether monitoring systems generated useful alerts, whether employees escalated concerns, whether the company investigated them, and whether identified problems were fixed. A gap between policy and actual operations can be more revealing than the policy itself.

From examiner-driven discovery to whistleblower reporting

Examinations and investigations remain important. But the legal landscape now also offers formal pathways for people to report suspected violations. Congress expanded BSA whistleblower provisions through the Anti-Money Laundering Act of 2020 (AMLA), with significant changes enacted in 2022.

The AMLA framework is designed to encourage people with relevant information to report potential BSA violations or related misconduct to the government. A report may give authorities leads that are difficult to see from an examination alone—for example, information about internal warnings, management decisions, or how a control worked in practice.

That does not mean every internal concern qualifies for an award, or that every report results in enforcement. Eligibility and payment depend on statutory requirements and https://www.lexinter.net/the-rise-of-bsa-whistleblower-lawsuits the facts. Employees also need to distinguish between raising a concern through a company's internal process and making a protected report to the government.

The 2022 award structure and the $1 million threshold

Under the amended AMLA framework, eligible whistleblowers may receive an award of **10% to 30% of monetary sanctions collected** in a qualifying action, subject to the law's requirements. The award framework generally applies when the relevant monetary sanctions exceed **$1 million**. That threshold is not a promise of a payout: a person must meet the applicable eligibility rules, and authorities must obtain qualifying monetary sanctions and collect them.

The BSA framework is administered through the Treasury Department and its relevant components, including FinCEN, the bureau that administers the BSA. It is not the same as the SEC or CFTC whistleblower programs. Those agencies have their own statutes, covered conduct, procedures, and award rules. A crypto-related matter may raise issues under more than one legal regime, but the agencies' roles should not be conflated.

Issue What it means Covered conduct Potential BSA violations or related conduct within the scope of the statute and program rules. Sanctions threshold The statutory award framework generally requires monetary sanctions exceeding $1 million. Potential award Eligible whistleblowers may receive 10% to 30% of qualifying monetary sanctions collected. Outcome An award is not automatic; eligibility, cooperation, the government's action, and collections matter.

Anti-retaliation protections and emerging case law

The amended BSA whistleblower provisions include anti-retaliation protections for eligible people who make protected reports. Remedies can include reinstatement, back pay, special damages, and attorneys' fees, subject to the statute and the circumstances of the case. These protections matter because employees may fear being fired, demoted, or otherwise penalized for raising concerns.





The boundaries of those protections are still developing through regulations and litigation. Disputes may turn on questions such as whether a person made a qualifying report, whether the report was made through a protected channel, whether the employer's action was retaliatory, and what remedies are available. The answers can depend on the governing law and the specific facts; companies and employees should not assume that every workplace complaint is automatically protected by the BSA whistleblower provision.

For employers, the practical response is straightforward: maintain a documented process for receiving and investigating concerns, prohibit retaliation, and train managers not to punish employees for good-faith compliance reporting. For employees considering an external report, legal advice can help clarify reporting options, confidentiality issues, deadlines, and whether the facts fit the applicable program.

What this means in practice for digital asset compliance

A crypto exchange that may be covered should treat BSA compliance as an operating function, not a registration exercise. The program should reflect the services actually offered, the assets and transaction routes involved, the customer base, and the jurisdictions in which the business operates.

1. **Map the business model.** Identify where the company accepts, holds, exchanges, or transmits value, and assess whether those activities create money-transmission or other BSA obligations.
2. **Test monitoring against real activity.** Review alert logic, data quality, escalation paths, and whether investigations capture relevant on-chain and customer context.
3. **Make SAR decisions traceable.** Document why activity was or was not escalated and reported, while protecting SAR confidentiality.
4. **Fix known weaknesses.** Track audit, testing, and examination findings through remediation, with accountable owners and deadlines.
5. **Give employees safe reporting channels.** Make internal escalation routes clear, prohibit retaliation, and ensure staff know that internal and government reporting pathways are not identical.
6. **Prepare for more than one regulator.** Determine which agencies may have authority over particular products or conduct without assuming that one agency's role replaces another's.

The bottom line

Crypto exchanges can be covered by BSA rules when their activities make them money services businesses or otherwise bring them within applicable requirements. Coverage is not decided by branding alone. A business's role in accepting, exchanging, or transmitting value—and the details of its operations—matter.

For covered firms, effective digital asset compliance means more than having written procedures. Transaction monitoring must support meaningful investigations, SAR decisions must be handled and documented correctly, and employees need a credible way to raise concerns. Examinations remain a major source of regulatory discovery, while the AMLA whistleblower framework adds formal reporting incentives and anti-retaliation protections. The award structure can reach 10% to 30% of qualifying sanctions collected when the statutory conditions are met, including the $1 million threshold—but payment is never automatic.