Yes—in many circumstances, a former employee of a crypto exchange can submit information about possible Bank Secrecy Act violations and may qualify for a whistleblower award. But eligibility is not automatic. It depends on the information provided, the enforcement action that follows, the sanctions collected, and the rules in effect when a claim is considered.

The Bank Secrecy Act (BSA) requires covered financial institutions to maintain anti-money-laundering programs and report certain suspicious activity. The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, administers key BSA requirements and receives tips about possible violations. The Department of Justice (DOJ) may bring criminal cases, while other regulators may pursue matters within their own authority.

For former employees, the practical question is not simply whether they worked in compliance. It is whether they have original, useful information about a potential violation—and whether they can report it lawfully without mishandling confidential records.

What the BSA Covers at a Crypto Exchange

The BSA is the federal framework for recordkeeping, customer due diligence, anti-money-laundering controls, and reporting suspicious transactions. It applies to specified financial institutions and businesses. Depending on what an exchange does and how it operates, a crypto exchange may be treated as a money services business (MSB), including as a money transmitter, and may have BSA duties.

That does not mean every company using crypto is automatically a BSA-covered entity. Business activities, customer relationships, and the company's role in transferring or exchanging value matter. Coverage is a legal determination, not a label an employee or company can settle just by calling itself a technology platform.

Where BSA duties apply, a compliance program may include written policies, a designated compliance officer, employee training, independent testing, and systems for monitoring transactions. Transaction monitoring systems can flag patterns such as unusual transaction volumes, activity inconsistent with a customer profile, or movement through high-risk addresses. Those alerts require review; an alert alone does not prove a violation.

What a SAR Is—and Is Not

A suspicious activity report, or SAR, is a confidential report that a covered institution files with FinCEN when the applicable reporting requirements are met. A SAR filing is the institution's responsibility. A former employee does not file a SAR on the exchange's behalf by submitting a whistleblower tip.



Instead, a former employee may report suspected BSA violations to the appropriate government channel. That report might describe failures to investigate alerts, weak controls, inaccurate records, or a pattern of suspicious activity that was not escalated. Whether those facts show a legal violation depends on the full circumstances, including the institution's obligations and what its decision-makers knew or did.

From Examiner-Driven Discovery to Whistleblower Pathways

Historically, BSA enforcement often began with examination findings, regulatory reviews, audits, or law-enforcement investigations. Examiners could identify gaps in an institution's controls—for example, a monitoring system that generated alerts no one reviewed, or SAR procedures that did not work as written. Those findings could lead to supervisory actions, civil penalties, or referrals for further investigation.

Examinations remain important. But they are periodic and may not reveal everything happening inside a business. Employees and former employees can have a different view: they may know how transaction monitoring systems were configured, whether alerts were routinely closed without adequate analysis, or whether managers discouraged SAR escalation.

The AMLA, enacted in 2020, strengthened the BSA whistleblower framework. It created a route for people with qualifying information to provide it to the government and, in certain successful enforcement actions, receive an award. The shift is meaningful: potential violations can reach authorities not only through examinations and institutional reports, but also through people with first-hand knowledge.

The 2022 AMLA Award Structure and the $1 Million Threshold

Under the BSA whistleblower statute, an eligible person may receive an award when original information leads to a successful enforcement action resulting in monetary sanctions exceeding $1 million. The statutory award range is generally between 10% and 30% of the monetary sanctions collected, subject to the law and the program's rules.

The threshold concerns sanctions collected in qualifying actions—not simply a company's market value, the size of a suspected transaction, or a penalty that has been announced but not collected. A tip can be valuable even if it does not ultimately result in an award. The government decides whether to investigate and what action, if any, to bring.

Issue What it means for a former employee Original information The tip generally needs to provide information not already known to the government and that materially assists an investigation or action. Successful enforcement action An award depends on a qualifying government action, not merely on submitting a report. Sanctions threshold The relevant monetary sanctions must exceed $1 million under the statutory framework. Award amount The general statutory range is 10% to 30% of qualifying monetary sanctions collected, subject to applicable rules and determinations.

FinCEN is the Treasury bureau responsible for the BSA whistleblower program. The DOJ may also pursue related criminal or civil matters, but it is important not to treat every agency as having the same role. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) handle matters within their securities and commodities jurisdiction; a crypto-related tip to one of them is not automatically a BSA whistleblower claim.

Can a Former Employee Qualify?

Being a former employee does not, by itself, disqualify someone. In fact, former employees may be well placed to explain how a control worked in practice, what management was told, and whether the company's written procedures matched its day-to-day operations.

Potentially useful information may include:



- Transaction monitoring alerts that were repeatedly closed without meaningful review.
- Known gaps in customer identification, escalation, or suspicious activity procedures.
- Internal warnings about possible money laundering that were ignored or suppressed.
- Records showing a mismatch between written controls and actual practices.
- Evidence that an exchange's leadership was informed of a serious weakness but failed to respond.

The law and implementing rules also contain eligibility limits and procedures. A person's role in obtaining information, prior access to it, and any involvement in the alleged misconduct can matter. Information already public or already known to the government may be less useful. A prospective whistleblower should get legal advice before assuming that an award is available or that a particular reporting method is protected.

Anti-Retaliation Protections

The BSA whistleblower provisions include anti-retaliation protections for qualifying reporting. They are intended to protect people who lawfully provide information to the government or participate in covered proceedings from adverse employment action because of that activity. Depending on the circumstances and lexinter.net applicable rules, protections may also relate to internal reporting.

These protections do not make every workplace dispute a whistleblower case. A former employee may not have a current job to lose, but could still face issues involving references, blacklisting, confidentiality disputes, or other alleged retaliation. Whether a particular action is unlawful depends on the facts and the legal route available.

Whistleblower law is also developing. Courts have addressed retaliation and whistleblower coverage under other statutes, including securities laws, but those decisions do not automatically determine the scope of BSA protections. BSA claims have their own statutory language and procedures. A former employee considering a retaliation claim should promptly consult an attorney about deadlines, the proper forum, and what evidence to preserve.

What This Means in Practice

A former employee should focus on a factual account, not a dramatic conclusion. Explain what happened, when it happened, who was involved, what controls were supposed to do, and what the employee personally observed. Exactly.. Distinguish direct knowledge from assumptions or second-hand accounts.

1. **Make a timeline.** Record relevant dates, job responsibilities, alert-handling practices, internal escalations, and management responses.
2. **Identify the control failure.** Describe the specific process or system at issue rather than simply saying the exchange had “bad AML.”
3. **Preserve evidence lawfully.** Do not access company systems after authorization ends, remove customer data, or take confidential files without legal advice. SARs and information that would reveal their existence are subject to strict confidentiality rules.
4. **Use an appropriate reporting channel.** A lawyer can help assess how and where to report, and whether the information supports a BSA whistleblower submission.
5. **Keep expectations realistic.** A report does not guarantee an investigation, an enforcement action, an award, or protection from every form of workplace conflict.

Common Misunderstandings

“If I saw a suspicious transaction, the exchange violated the BSA.”

Not necessarily. Suspicious activity can require review and, in some cases, a SAR, but an unusual transaction alone does not establish that the institution violated the law. The institution’s obligations, investigation, and response matter.

“I can take SARs to prove my point.”

Do not assume that. SAR confidentiality restrictions are serious. A whistleblower should not disclose SARs or information that reveals a SAR’s existence without obtaining legal advice about the permitted process.

“A tip guarantees 10% to 30% of a penalty.”

No. That range describes the statutory award framework for qualifying cases. An award depends on eligibility, the usefulness and originality of the information, a successful enforcement action, sanctions collected above the threshold, and the program’s determinations.

Conclusion

A former employee can potentially bring forward information about crypto exchange compliance and BSA violations. The 2020 AMLA framework offers a formal reporting and award pathway, with the possibility of an award when original information contributes to a qualifying action and monetary sanctions collected exceed $1 million. Last month, I was working with a client who was shocked by the final bill.. Anti-retaliation provisions may also apply.

The strongest reports are specific, supported by first-hand knowledge, and submitted through a lawful channel. Because BSA coverage, award eligibility, SAR confidentiality, and retaliation protections can turn on fine details, a former employee should speak with a whistleblower attorney before sharing company records or making public allegations. This article is general information, not legal advice.