The United States Department of Justice (DOJ) Bank Integrity Unit (BIU) investigates and prosecutes serious criminal misconduct involving banks and other financial institutions. Its work can include cases where an institution's anti-money laundering controls failed, where employees helped move criminal proceeds, or where a bank misled regulators about its compliance programme.

For compliance teams, the BIU matters because **financial institution enforcement** can reach beyond a failure to file paperwork. Prosecutors may examine what a firm knew, how it responded to warnings and whether individuals or the institution enabled criminal activity. For employees, the issue is different but connected: a report made inside a firm is not the same as a submission to a regulator or law enforcement agency, and the timing of a report can matter.

This guide explains the BIU's role, how it relates to suspicious activity reporting and what the amended Bank Secrecy Act (BSA) whistleblower programme may mean for people who report misconduct. It is general information, not legal advice. The facts and applicable rules matter in any particular case.

What is the DOJ Bank Integrity Unit?

The BIU is a specialised unit within the DOJ's Criminal Division. It focuses on criminal cases involving financial institutions and the systems intended to prevent them from being used for money laundering and other unlawful activity. The unit works with federal law enforcement and regulatory agencies, including the Financial Crimes Enforcement Network (FinCEN), which administers key parts of the BSA.

The BIU is a criminal enforcement unit, not a regulator and not a general complaints office. Regulators supervise institutions and can take civil or administrative action. Prosecutors investigate potential crimes and may bring criminal charges where the evidence and legal tests support doing so. These roles can overlap: the same conduct may lead to regulatory action, a criminal investigation or both.

What does the BIU investigate?

Cases may involve alleged failures to maintain or implement anti-money laundering (AML) controls, including weaknesses in customer due diligence, transaction monitoring or the escalation of suspicious activity. Prosecutors may also investigate whether an institution or its staff concealed misconduct, made misleading statements to authorities, or knowingly processed transactions connected with criminal conduct.

Not every control failure is a crime. A compliance weakness, by itself, does not establish criminal intent or prove that an institution committed an offence. Investigators may look at the full picture: the risks the firm faced, what its systems detected, what employees reported, what management knew and whether the firm took reasonable steps to address the problem.

Depending on the evidence, investigations can examine conduct by the institution, senior managers, compliance staff or other employees. Potential consequences differ by case and may include criminal charges, financial penalties, independent monitoring or other conditions. No particular outcome follows automatically from a report or an investigation.



SAR obligations and internal reporting are not the same thing

Under the BSA, certain financial institutions must file a Suspicious Activity Report (SAR) with FinCEN when applicable reporting requirements are met. A SAR is a regulated report about suspected suspicious activity. It is generally not a public document, and institutions face restrictions on revealing that a SAR has been filed.

An employee's internal compliance report is different. It may alert a manager, compliance team, legal department or designated reporting channel to a concern. That can help a firm investigate and meet its obligations, including deciding whether a SAR is required. But an internal report is not itself a SAR, and it is not automatically a submission to FinCEN, the DOJ or another authority.

Route What it is for What it does not automatically do Internal compliance channel Raises a concern within the organisation for review and possible action. It does not necessarily notify a regulator or qualify as an external whistleblower submission. SAR filing Meets a financial institution's reporting obligation to FinCEN when the legal requirements apply. It does not, by itself, establish that a crime occurred or guarantee an enforcement action. External whistleblower submission Provides information to an authorised government body under an applicable whistleblower programme. It does not guarantee an investigation, award or protection from every form of workplace harm.

Employees should not assume that reporting internally satisfies every external reporting requirement, or that filing externally removes an real estate cash purchase reporting institution's separate SAR duties. Nor should staff copy or disclose confidential or restricted information without considering the law, company policies and the relevant reporting process. A lawyer with experience in whistleblower and financial regulation matters can help assess lawful options.

The BSA whistleblower programme: what changed in 2022?

Congress strengthened the BSA whistleblower programme through the Anti-Money Laundering Whistleblower Improvement Act, enacted in December 2022. The overhaul addressed longstanding concerns about whether the programme offered a sufficiently clear and meaningful incentive for people to provide useful information about violations.

The programme is administered by the US Treasury Department, through FinCEN. It is not a DOJ-only scheme. Qualifying information may support enforcement actions brought by the DOJ or by other covered authorities, subject to the statutory requirements. The programme is separate from an employer's internal reporting system and from an institution's duty to file SARs.

The $1 million sanctions threshold

A potential award is tied to a successful enforcement action, or related actions, in which monetary sanctions exceed $1 million. The threshold concerns sanctions imposed in the relevant action or related actions; it is not a promise that a whistleblower will receive money whenever they report a concern. The government must pursue a qualifying action and collect sanctions, among other requirements.

The threshold also helps explain why reports of serious, well-supported misconduct may be more relevant to the programme than reports of isolated errors that do not lead to a covered enforcement result. The legal test depends on the statute and the facts, not simply on how serious a report sounds to the person making it.

Mandatory awards and the 10 to 30 per cent range

For a whistleblower who meets the statutory conditions, the amended law provides for a mandatory award of between 10 and 30 per cent of the monetary sanctions collected in the qualifying action or related actions. "Mandatory" does not mean that every person who submits information receives an award. It means that, when the legal eligibility conditions are met, the award framework is not simply an optional reward decided without statutory criteria.

The percentage is not fixed at 30 per cent. The amount within the range depends on factors set out in the law and implementing rules, including the significance of the information, the degree of assistance provided and the programme's law-enforcement interests. The precise calculation and eligibility can be complex. An award is linked to sanctions collected, not merely to an announced penalty or a company's settlement headline.

In practical terms, the range is an incentive, not a forecast. A person cannot reliably estimate an award from the size of a suspected loss or a potential penalty. There may be no qualifying enforcement action, the information may not meet the required standard, or statutory exclusions and other rules may apply.

Anti-retaliation protections and a federal cause of action

The BSA whistleblower provisions prohibit an employer from retaliating against a whistleblower for qualifying lawful acts, such as providing information to the relevant government authorities or assisting with an investigation or proceeding. Prohibited conduct may include termination, demotion, suspension, threats, harassment or other discrimination connected to protected activity.

The law also provides a federal cause of action: a whistleblower who believes they suffered prohibited retaliation may bring a claim in federal district court. The statute provides for remedies that can include reinstatement, double back pay with interest, compensation for certain special damages, and costs and reasonable legal fees. Claims are subject to statutory deadlines and procedural requirements; the law generally sets a two-year period for bringing a retaliation action. Anyone facing retaliation should obtain prompt legal advice rather than rely on a general summary of the rules.

Protection is not the same as immunity from every workplace consequence. A dispute about performance, for example, may be different from retaliation for protected reporting, and the facts can be contested. Keeping a careful, lawful record of relevant events and getting advice early may help a person understand their position. Do not remove or retain documents you are not entitled to access or keep.



Internal channels or an external submission?

Internal reporting can be valuable. It may let a firm stop misconduct, preserve evidence, correct a control weakness or make a required regulatory report. But employees should distinguish the benefits of internal escalation from the rules governing an external submission. An internal hotline report does not automatically become a submission to FinCEN or the DOJ, and it does not necessarily satisfy the criteria for a whistleblower award.

Nor should a person assume they must report internally before approaching an authorised government body. Whether internal reporting is required, useful or strategically sensible depends on the relevant law, employment arrangements, the risk of evidence being lost and the person's safety. The 2022 amendments and implementing rules should be checked against the specific route being considered.

For anyone considering a report, a measured approach is generally safer than either delay based on assumptions or an impulsive disclosure. Consider getting independent legal advice, identifying the correct government programme, and preserving information lawfully. Avoid sharing SAR-related information or other confidential material in ways that could breach legal restrictions.

What the BIU means for compliance teams

For financial institutions, BIU scrutiny reinforces that AML controls need to operate in practice, not merely appear in policies. Firms should have clear escalation routes, timely investigation processes, documented decisions and appropriate oversight of recurring or high-risk issues. A report that reaches a compliance team should be assessed on its substance, not dismissed because it is inconvenient or raised by a junior employee.

For individuals, the central point is to separate three questions: what the institution must report under SAR rules; what the employee may report internally; and whether the employee has information that could be submitted under a government whistleblower programme. The answers may overlap, but they are not interchangeable.

Key points

- The DOJ Bank Integrity Unit pursues criminal cases involving financial institutions and alleged failures or misconduct connected with financial crime controls.

- AML failures can prompt serious scrutiny, but a control weakness alone does not prove a crime.
- A SAR is a regulated filing to FinCEN; an internal report and an external whistleblower submission are different channels.
- The 2022 BSA whistleblower overhaul provides for awards of 10 to 30 per cent of sanctions collected in qualifying cases exceeding the $1 million threshold, if statutory conditions are met.
- The law prohibits certain retaliation and provides a federal route to bring a retaliation claim, but deadlines and legal requirements apply.

The BIU is one part of a broader system of financial institution enforcement. Understanding the difference between internal escalation, SAR obligations and external reporting can help firms respond responsibly—and help individuals avoid relying on assumptions about awards, confidentiality or protection.