A whistleblower award is not a fixed percentage for every person who reports a Bank Secrecy Act (BSA) problem. Under the BSA's whistleblower provisions, an eligible person may receive between 10% and 30% of monetary sanctions collected in a qualifying action, subject to the statutory requirements and the rules that apply to the claim. The percentage depends on the facts, including the **significance of the information**, the whistleblower's **assistance to the investigation** and whether the submission contains genuinely **original information**.

That makes the difference between a useful report and a strong award claim more than a matter of telling a regulator that something "looked suspicious". Investigators need specific, supportable information that helps them understand what happened, who was involved, how the conduct may have breached the law and where they can verify the evidence. A report should also distinguish an honest mistake from conduct that may have been deliberate.

This article explains the main factors that can influence an award, how to document concerns responsibly, and why timing and anonymity require careful thought. It is general information, not legal advice. Award eligibility and procedures can depend on the specific statute, implementing rules and facts.

Start with the award framework

The BSA whistleblower programme provides for awards tied to monetary sanctions collected in qualifying enforcement actions. The statutory range is generally 10% to 30% of the monetary sanctions collected, where the legal requirements are met. The amount is not calculated simply by counting documents, emails or hours spent helping. The decision-maker considers the value of the information and the whistleblower's contribution to the outcome, among other relevant factors.

"A 10% award" and "a 30% award" are therefore not guaranteed tiers that a person can select when filing. Nor does every report lead to an award. A report may be valuable for compliance purposes without producing an eligible enforcement action or collected monetary sanctions.

For current programme information, consult the relevant materials from the US Department of the Treasury and FinCEN. The Federal Financial Institutions Examination Council (FFIEC) also publishes examination materials and BSA/AML resources that can help readers understand supervisory expectations. Those materials are useful context, but an examination manual is not, by itself, a finding that a particular person or institution violated the law.

What counts as a BSA violation — and what may be a mistake?

The BSA and its implementing regulations impose obligations on covered financial institutions and other regulated entities. Depending on the institution and circumstances, those obligations can include maintaining an AML programme, conducting customer due diligence, keeping certain records and filing currency transaction reports (CTRs) or suspicious activity reports (SARs) when required.

A missed filing, a late review or an incomplete customer file can be a warning sign. But one error does not automatically prove a BSA violation, much less intentional misconduct. It may reflect a human error, unclear procedures, a system failure, insufficient training or a temporary operational problem. By contrast, evidence that someone knowingly concealed a problem, falsified records, repeatedly overrode controls or directed staff not to file required reports may support a more serious concern. Context and evidence matter.

Separate the event from your interpretation

A report is more useful when it separates what you personally observed from what you infer. For example:

- **Observed fact:** "On 14 March, I reviewed the case record for customer account ending 4821. The system showed a cash transaction of £/US$[amount] on 12 March."
- **Relevant record:** "The case log shows the alert was closed on 15 March by [role or name], with the note 'no action'."
- **Question or inference:** "I am concerned the alert may not have received the review required by our procedure because the record does not show the documented checks listed in that procedure."

That is more credible than writing, "Management is laundering money," without dates, transactions or a clear basis for the allegation. The aim is not to make a legal conclusion yourself. It is to give investigators facts they can test.

Original information and its significance

Original information is information derived from the whistleblower's independent knowledge or analysis, rather than information already known to the relevant authorities or merely repeated from public sources. The precise legal test and exclusions depend on the governing rules. Before submitting, consider whether your information is new, specific and obtained through a lawful, authorised route.

Originality is not the same as being the first person to have a suspicion. A person may add value by identifying a new transaction pattern, explaining how a control was bypassed or providing records that connect a previously known concern to particular dates, accounts or decision-makers. Conversely, forwarding a news story or repeating a general rumour may add little if it gives investigators no new lead.

The **significance of information** is about how much it helps authorities assess or prove the suspected conduct. Information may be significant when it:

- identifies specific transactions, customers, accounts, products or business units;
- shows how a suspected pattern operated over time;
- explains who made, approved or altered a decision, and when;
- points to records, systems or witnesses that can independently verify the account; or
- helps investigators understand why existing controls did not detect or address the conduct.

A short, well-supported account can be more significant than a large document dump. Avoid collecting information you are not authorised to access, altering records or taking customer data outside approved channels. Preserve what you already lawfully possess and ask a qualified lawyer about safe handling.

Assistance to the investigation

The whistleblower's **assistance to the investigation** can influence the award. A person who provides a clear account, identifies where records are kept, explains technical terminology and responds promptly to reasonable follow-up questions may be more helpful than someone who submits a report and becomes unavailable. Assistance does not mean that a whistleblower should conduct an investigation, question colleagues or access systems beyond their authority.

Investigators may need to test an account against other evidence. Being candid about gaps in your memory, uncertainty or possible explanations can strengthen credibility. If you made an earlier mistake, correct it promptly and explain the correction. Do not present a guess as a fact merely because it makes the report sound stronger.

The award decision may also consider the whistleblower's role in the conduct and other circumstances under the applicable rules. Someone who planned or directed wrongdoing should not assume that making a report erases their own responsibility. Get independent legal advice before submitting information if you may have participated in the conduct.

Evidence and documentation that holds up

Good documentation lets a reviewer follow the trail without relying on vague allegations. Make a contemporaneous note where possible, and distinguish what you saw from what someone else told you. For example, record: "On 6 June, at approximately 10.30 am, I saw when to file a SAR the SAR case status change from 'pending review' to 'closed'. I did not make the change. The system audit trail may identify the user." This is more useful than "They buried the SAR."

What to write down

- **Date and time:** when the event occurred and when you learned of it.
- **Transaction or case details:** amounts, dates, account or case references, and relevant business unit, using only information you are authorised to record.
- **People and roles:** who was present, who took an action and who may have approved it.
- **Source:** whether you saw a system entry, read an email or heard a statement directly.
- **Exact words:** where a quotation matters, note it as accurately as possible and identify whether it is verbatim or from memory.
- **Records to locate:** for example, a dated SAR log entry, alert disposition, audit trail, policy version, training record or approval email.
- **Uncertainty and alternative explanations:** note missing context, possible system issues or what you do not know.

Do not edit original records, backdate notes or move confidential material to a personal device or email account. A dated note made at the time may help establish what you knew and when, but it is not a substitute for the underlying records.

Less useful account More useful account "The bank ignored suspicious activity." "On 9 September, I reviewed alert 77531 concerning three cash deposits over two days. The case log records closure on 11 September. The log does not show the customer review listed in procedure version 4.2. The audit trail may show who closed it." "My manager told us not to report anything." "At the team meeting on 3 October, my manager said, 'Do not escalate these alerts this month.' I noted the statement immediately afterwards. Two alerts discussed were cases 88402 and 88419."

Timing pressure and limitation periods

Timing matters for two different reasons: an investigation may need prompt, accurate information, and legal deadlines may apply to an award claim or a retaliation claim. These are not necessarily the same deadline. The applicable period can depend on the claim, the relevant agency process and the date of the alleged conduct or retaliatory action. Do not rely on a general blog post to calculate it.

For instance, the BSA includes anti-retaliation protections and a time limit for bringing certain retaliation actions. The National Law Review has published an overview of filing an AML/BSA whistleblower lawsuit; see its discussion at The National Law Review and confirm the current law with a lawyer. A retaliation claim may involve a different

procedure and deadline from an award submission. Keep dated records of when you reported, to whom, what response followed and any later changes to your duties, pay, access or employment status.

Do not delay solely while trying to assemble a perfect file. At the same time, avoid rushing into a disclosure that could expose confidential information or compromise your position. A whistleblower lawyer can help assess the relevant route, deadlines, confidentiality issues and retaliation risks. If retaliation occurs, document it promptly and seek advice about available protections and reporting channels.

Anonymous versus identified submissions

Depending on the applicable process, a whistleblower may be able to submit information anonymously through an attorney. Anonymity can reduce immediate exposure, but it does not necessarily mean the agency never learns the person's identity. The rules may require identity verification or disclosure at a later stage, such as before an award can be paid. Check the current programme requirements rather than assuming that an anonymous submission guarantees permanent secrecy.

An identified submission may make follow-up easier: investigators can ask questions, clarify dates and request help locating records. But a person may reasonably fear workplace retaliation, reputational harm or pressure from colleagues. Before choosing, discuss the practical risks with independent counsel. Consider whether a protected internal channel, a regulator submission or more than one lawful route is appropriate in your circumstances; do not assume that reporting internally alone preserves an external award claim or meets every legal deadline.

What can move an award towards the higher end?

No single factor guarantees 30%, but a stronger submission will generally be specific, verifiable and useful. It will explain the suspected conduct without overstating what the evidence proves, include genuinely original information where required, and help investigators find or interpret the relevant records. Continued, truthful cooperation may also matter.

A lower award or no award may result where information is duplicative, too general to investigate, already known, unsupported or unrelated to a qualifying action. An award may also depend on whether monetary sanctions are collected and on other statutory and regulatory criteria. The percentage is ultimately a legal determination, not a negotiation based on how serious the whistleblower feels the issue is.





Practical next steps

1. Write a dated, factual chronology, separating direct observations from assumptions and second-hand information.
2. Identify the transaction, alert, SAR log, policy or system record that could verify each key point.
3. Preserve information lawfully; do not access, copy or disclose records outside your authority.
4. Record internal or external reports and any subsequent workplace changes, with dates and relevant communications.
5. Get independent legal advice promptly about eligibility, anonymity, retaliation protections and deadlines.
6. Use official Treasury or FinCEN materials for current submission requirements, and treat FFIEC examination materials as guidance rather than a finding about your case.

The most persuasive whistleblower account is neither dramatic nor vague. It is a careful, dated explanation of what happened, what records support it and what remains uncertain. That approach helps investigators assess the significance of the information, evaluate its originality and understand the whistleblower's assistance to the investigation—without confusing human error with willful misconduct.