Customer due diligence, usually shortened to CDD, is the process a bank uses to understand who a customer is, what the customer's account is for, and whether account activity fits the bank's understanding of that customer. CDD is a core part of a bank's anti-money laundering program—not just a form collected when an account opens.



For customers, employees, and potential whistleblowers, the practical question is often: what should the bank have documented, and what does it mean if those records are missing or ignored? The answer depends on the customer, the product, the risk, and the legal duty involved. A missing document is not automatically evidence of fraud or a reportable violation. But records can help show whether a bank followed its obligations under the Bank Secrecy Act (BSA) and related rules.

What CDD means in a bank's AML program

CDD is a risk-based process. A bank gathers information to identify and understand its customers, develops a customer risk profile, and monitors activity over time. "Risk-based" does not mean every customer receives identical scrutiny. It means procedures should be reasonably designed to address the risks presented by the bank's customers, products, services, and locations.

CDD is often described as having four practical parts:

- **Identify the customer:** Collect and verify identity information under applicable customer identification requirements.
- **Understand the relationship:** Learn the purpose and intended nature of the account or service.
- **Identify beneficial owners when required:** For covered legal entity customers, obtain information about certain individuals who own or control the entity, subject to applicable rules and exemptions.
- **Monitor and update:** Review activity for consistency with the customer's profile and refresh information when risk or circumstances warrant.

For covered legal entity customers, the CDD rule generally calls for identifying each individual who owns 25% or more of the entity, if any, and one individual with significant responsibility to control, manage, or

direct it. The rule has exceptions, and the details can depend on the type of entity and account. In practice, this is why **beneficial owner info** is an important category of customer due diligence records.

CDD, SARs, CTRs, and the bank's wider duties

CDD is connected to, but not the same as, a suspicious activity report (SAR) or a currency transaction report (CTR). The bank's records and procedures help it decide whether a report is required; the reports themselves are separate BSA duties.

- **SAR:** A bank must file a SAR when applicable rules require it to report suspicious transactions. Suspicion may involve possible illegal activity, attempts to evade BSA requirements, or activity lacking an apparent lawful purpose after review. A SAR is not a finding that a customer committed a crime.
- **CTR:** Banks generally report currency transactions exceeding $10,000 in one business day, applying the relevant aggregation rules. CTR reporting concerns cash transactions; it is not a general report of every large wire or check.
- **AML program:** Banks must maintain an AML program that meets applicable requirements, including internal controls, independent testing, a designated compliance officer, and employee training. CDD and monitoring should work within that program rather than exist as isolated paperwork.

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, administers key BSA regulations and receives many BSA reports. Banks also have duties under other laws and regulations, and their exact obligations depend on their activities and circumstances.

What customer due diligence records should a bank keep?

There is no single file that proves a bank complied with every https://usattorneys.com/how-to-file-a-bsa-whistleblower-lawsuit/ CDD obligation. A bank's records may be spread across account-opening systems, customer profiles, transaction-monitoring tools, case-management platforms, and reporting systems. Relevant **customer due diligence records** may include the following:

Record category Examples Why it may matter Identity and account opening Customer name, date of birth or formation, address, identification details, verification results, account purpose, and opening date Shows what the bank collected and how it established the customer relationship Beneficial ownership Names, dates of birth, addresses, identification numbers, ownership percentages when collected, and control-person information Documents the bank's understanding of the people who own or control a covered legal entity Risk assessment Customer risk rating, relevant risk factors, rationale for a rating, and changes over time Helps explain how the bank applied its risk-based procedures Monitoring and review Alerts, case notes, transaction analysis, customer outreach, escalation decisions, and account reviews Shows how activity was assessed against the customer's profile and what action followed BSA reports and supporting material CTR records, SAR filing records, and documentation supporting a SAR Helps establish whether reporting and retention duties were handled appropriately

Retention periods vary by record type and rule. Many BSA records must be kept for five years, but the starting point and exact requirement can differ. For example, SAR supporting documentation generally must be retained for five years from the date the SAR is filed. Other account and transaction records may have their own retention triggers. A bank should consult the applicable regulation and its record-retention procedures rather than assume that one five-year period applies to everything.

SARs and information revealing that a SAR was filed are subject to strict confidentiality rules. A bank generally cannot tell the subject of a SAR that one was filed. That does not mean every underlying record is automatically secret for every purpose; access and disclosure questions are fact-specific and should be handled through proper legal channels.

What could qualify as a reportable BSA/AML violation?

A compliance concern becomes more significant when facts suggest a bank failed to meet a legal duty, not merely when an employee disagrees with a business decision. Potential concerns might include repeated failures to investigate meaningful alerts, knowingly inaccurate reporting, deliberate circumvention of controls, or an AML program that is ineffective in practice despite being documented on paper.

Context matters. A single late review, a mistaken risk rating, or an alert that closes without a SAR does not automatically establish a violation. Banks make judgment calls, and the BSA does not require a SAR for every unusual transaction. A credible concern is stronger when it identifies the duty, the conduct, the people or systems involved, and facts suggesting the problem was serious, repeated, concealed, or left uncorrected.

Useful questions include:

- What BSA or AML obligation may have applied?
- What facts did the bank know, and when did it know them?
- Was the issue isolated, or did it appear across customers, branches, products, or time periods?
- Were alerts, audit findings, or regulator concerns escalated and addressed?
- Is there evidence of intentional evasion, concealment, or inaccurate records?

Do not rely on “everyone knows” as evidence. Identify what you personally observed, what records support it, and what remains uncertain. A careful distinction between facts and conclusions can make a report more useful.

Whistleblower basics: original information and eligibility

FinCEN has a whistleblower process for information about certain BSA violations. The agency’s whistleblower materials and the **FinCEN whistleblower submission form** describe how to submit information. Eligibility for a potential award is governed by law and agency rules; submitting a tip does not guarantee an award, an investigation, or a particular outcome.

In general, a whistleblower should focus on specific, credible information that is not already known to the government or otherwise publicly available in the relevant way. “Original information” has legal meaning and can involve information derived from independent knowledge or analysis, subject to exceptions. A person’s eligibility may depend on the source of the information, the person’s role, the nature of the conduct, and other legal requirements. Employees involved in the conduct, people who obtained information through certain restricted roles, and people who are legally barred from disclosure may face special rules or exclusions.

Before sharing sensitive information, consider speaking with a whistleblower attorney. An attorney can help assess eligibility, confidentiality options, whether the information is protected, and how to submit it without disclosing unrelated customer data. A lawyer can also explain whether a reward may be available and what must happen for one to be paid. No attorney can promise that an agency will open a case or that a reward will result.

Internal reporting and safe documentation

Internal compliance channels may include a supervisor, compliance department, ethics hotline, or designated reporting portal. Internal reporting can give an institution a chance to investigate and correct a problem, but it may not be appropriate or safe in every situation. Consider whether the people implicated control the channel, whether there is a retaliation concern, and whether a legal deadline or external reporting option matters.

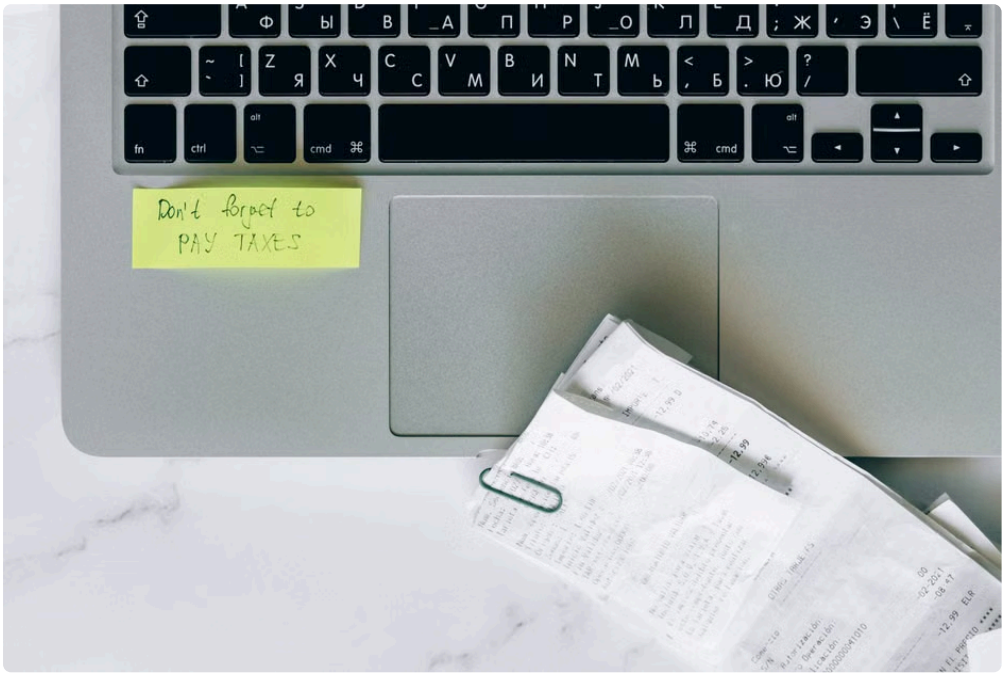
Keep a factual record for yourself, but do not take or copy customer files, SARs, or other restricted work materials without authorization. Do not email yourself bank documents or move them to a personal device or cloud account. Confidentiality, privacy, employment, and trade-secret laws may apply. An attorney can advise how to describe what you know and whether lawful access to particular records is possible.

Write down a timeline the same day something happens. Include dates, approximate times, who was present, what you observed directly, what was said, and how you learned it. Label documents you are authorized to retain, preserve relevant communications lawfully, and separate firsthand facts from assumptions. A contemporaneous timeline can help you recall details accurately without collecting records you are not allowed to possess.

Working with a whistleblower attorney

An attorney experienced in whistleblower matters can help organize the facts, identify the potential legal duty, evaluate reporting routes, and protect the client's interests. Firms and directories such as USAttorneys.com may help people locate lawyers, but a listing is not a recommendation or a guarantee of a particular lawyer's experience. Ask about the attorney's work with BSA matters, confidentiality, conflicts, and how communications will be handled.

Some whistleblower lawyers work on a contingency-fee basis, meaning the fee is tied to a recovery or award under a written agreement. Terms vary. Ask whether you could owe costs if there is no recovery, how expenses are handled, what percentage applies, and whether the fee arrangement complies with the applicable rules. Do not assume that "contingency" means there can never be any out-of-pocket obligation.



A practical checklist

1. Write a same-day timeline of the events you personally observed.
2. Identify the possible duty involved—CDD, monitoring, SAR, CTR, or AML program controls—without labeling conduct “fraud” before the facts support that conclusion.
3. Separate direct knowledge from what someone else told you, and note what you do not know.
4. Use authorized internal compliance channels if appropriate, while considering confidentiality and retaliation risks.
5. Do not remove or email yourself restricted bank records.
6. Consult a qualified whistleblower attorney before submitting sensitive information, and review FinCEN’s current instructions and eligibility rules.

CDD records help show how a bank understood its customers and responded to risk. The most useful account of a possible violation connects those records—or an apparent gap in them—to a specific BSA duty and a clear timeline. Careful documentation, lawful handling of information, and realistic expectations are safer than assumptions about what a bank “must have known” or how quickly an agency will act.