MODERN TREASURY

How to Build a BSA / AML Compliance Program

INTRODUCTION

Who Is This Guide For?

Companies building embedded financial products need to have a compliance program because money movement is highly regulated. Whether you're building a platform for payments, lending, investing, or any other product, federal and state laws require safeguards to prevent money laundering, identify illicit financing (like drug trafficking, terrorism, and sanctioned entities), and detect fraud.

You also need to partner with a bank to be able to move money over ACH, wire transfers, RTP, and other payment methods, since these networks only permit regulated banks and financial institutions to send and receive payments. Your bank partner will review your compliance program before allowing you to launch the product, since they are ultimately held responsible by regulators for adhering to compliance laws.

How you set up your compliance program ultimately depends on your **bank partnership model**:

1. **Indirect**

   Using a **Third Party Sender** or **Banking-as-a-Service** provider means you don't get to work directly with a bank. These providers manage the relationship on your behalf, handling compliance requirements in the process.

2. **Direct**

   Using a **Payment Operations** platform like Modern Treasury lets you work directly with a bank, allowing you to set up and manage your own compliance program.

Working directly with a bank may require a larger upfront investment but has a number of long-term advantages, such as faster payment settlement, better visibility, and more control over your funds.

Modern Treasury was founded with the goal of abstracting the complexity of bank integration and payment reconciliation at scale to reduce the technical component of this upfront investment. Our platform does not sit in the flow of funds, instead providing modern APIs and an easy-to-use web app to automate payments directly through your bank account.

However, we realized that many customers initially find building a compliance program difficult, even though this process is a critical requirement to launching their product.

With this guide, our goal is to help companies seeking to work directly with a bank launch products faster. To this end, we're providing an actionable framework to understand the regulations, terminology, and concepts required to build and operate a compliance program.

Disclaimer: *This guide does not constitute legal advice. Please consult a qualified legal counsel to ensure your compliance program adheres to relevant regulatory requirements.*

CHAPTER 1

The Basics of Compliance

What is a Compliance Program?

A compliance program is a set of rules, protocols, and procedures an organization puts in place to comply with government regulations on money movement.

A compliance program should be designed to:

- Guarantee adherence to legal requirements and regulations governing financial transactions, such as BSA/AML laws.
- Protect businesses from becoming victims of money laundering, fraud, terrorism, and other illegal or malicious behavior.
- Empower and prepare business teams to deter, detect, and report bad actors to law enforcement, if necessary.
- Enable organizations to test, document, report, and analyze their compliance in an ongoing manner.
- Evolve as requirements and regulations change.

There are three major pieces of legislation governing money movement in the US that specify these compliance requirements: The Bank Secrecy Act (BSA), the USA PATRIOT Act, and the Anti-Money Laundering Act of 2020.

FinCEN, or the Financial Crimes Enforcement Network, is a bureau within the Department of Justice that is primarily responsible for upholding these laws. Predominantly an intelligence organization, FinCEN shares information with law enforcement and other regulatory agencies like the Office of the Comptroller of the Currency, or OCC.

Compliance Dictionary

Passed in 1970, the BSA was the first significant piece of legislation to kickstart the current regulatory compliance regime in the US. To learn more about changes to these laws across the years, here's a helpful breakdown from FinCEN.

Since then, an entire set of terminology has emerged in the banking and payments industry to describe the compliance requirements of the BSA and subsequent pieces of legislation. Familiarizing yourself with these terms and acronyms is a critical first step to understanding how to set up your compliance program.

AML: Anti-Money Laundering

AML is the most frequently used acronym in this space, and when broadly defined refers to the checks and safeguards financial institutions are required to implement to prevent cash acquired by illegal means from entering the banking system.

CIP: Customer Identification Program

CIP refers to the process a company and its bank partner are required to follow for customer due diligence. It entails the collection of sufficient information to reasonably verify the true identity of each customer.

CDD/EDD: Customer Due Diligence / Enhanced Due Diligence

In addition to a CIP, companies may also need to document:

- Why customers are using their product
- What fund flows they are likely to have

This additional information is important for determining when transactions are suspicious.

EDD goes further, and mandates that companies maintain a risk-based approach to verifying their customers, with defined protocols for handling each level of potential risk.

KYC/KYB: Know Your Customer/Know Your Business

KYC/KYB are the most frequently used acronyms in this space after AML. As the terms suggest, these processes involve acquiring the necessary information to reasonably identify the customer or business entity using your product. KYC/KYB is usually part of an organization's CIP.

CTR: Currency Transaction Report

A bank must submit a CTR for each transaction of more than $10,000 made by, through, or to the bank. Banks pass this requirement on to their corporate partners, requiring that partners monitor transaction amounts on an ongoing basis.

SAR: Suspicious Activity Report

A bank must file an SAR with FinCEN whenever they detect a suspected case of money laundering or fraud. Banks pass this requirement on to their corporate partners who must set up on-going transaction monitoring to flag suspicious activity.

OFAC: Office of Foreign Assets Control

The Office of Foreign Assets Control of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals by identifying prohibited countries, individuals, and business entities.

SDN: Specially Designated National

OFAC publishes a list of individuals and companies owned or controlled by targeted countries and individuals, groups, or entities—such as terrorists and narcotics traffickers—identified under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and US businesses are generally prohibited from dealing with them.

PEP: Politically Exposed Persons

A PEP is someone that holds a prominent public office and is therefore at risk of abusing their influence to facilitate money laundering or other offenses like bribery or corruption. Banks are required by regulators to check customers against PEP lists and generally pass that requirement on to their corporate partners.

Operationalizing a Compliance Program

Regulators evaluate the AML compliance programs of banks and their corporate partners according to five criteria, commonly referred to as the 'The Five Pillars of AML Compliance.' As defined by FinCEN[1], this list consists of:

- A system of internal controls to ensure ongoing compliance
- Independent testing of BSA/AML compliance programs
- The designation of an individual responsible for day-to-day compliance
- Training for appropriate personnel
- Risk-based procedures for conducting ongoing customer due diligence

Your bank partner will require a written document called a BSA/AML policy that describes your plan to meet these requirements. They also require you to commit to upholding this policy to the best of your ability before permitting your product to launch.

Implementing a compliance program that meets these criteria can be a challenging proposition, especially for companies doing so for the first time. In

[1] https://www.ncua.gov/newsroom/ncua-report/2017/fincen-adds-fifth-bsa-compliance-pillar

the rest of this guide, we'll outline an operational framework to help you get started that consists of three core components:

1. **Processes**

   From KYC, KYB, and suspicious activity reporting to periodic audits, your compliance program should have well-defined processes to support approval by a bank.

2. **Software**

   Implementing a reliable and scalable compliance program requires investing in the right software with features ranging from upfront verification of users to ongoing transaction monitoring and reporting.

3. **People**

   Whether it's a small team or an entire organization, you'll need a designated group of employees or outside consultants to own these processes and serve as the primary point of contact with your bank partner.

CHAPTER 2

Processes

Building and operating a compliance program involves setting up well-defined processes for implementing regulatory requirements. We've outlined the six most important processes your BSA/AML policy should include below.

1. Customer Identification Program

The most effective way to prevent money laundering or fraud is to conduct KYC/KYB checks to properly identify new customers when they sign up for your product.

At a minimum, your Customer Identification Program should include the following steps:

1. **Collect** the name, email, address, date of birth, and identification number (SSN/TIN) of the user at sign up. B2B products should collect this information for each beneficial owner of the business—typically anyone that directly or indirectly owns 25% or more of the company.
2. **Verify** this information, either by checking it against reputable data sources or by verifying documents like the user's passport or driver's license.
3. **Screen** this information against OFAC sanctions and PEP lists.
4. **Decide** whether to approve or deny the user based on these checks.

Your CIP can also go a step further, with additional steps for Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD):

- For CDD, you can document how the user intends to move money through your product and collect additional information like bank account details and phone numbers.
- For EDD, you can set up a risk-based framework for assessing new users, sorting them into low-, medium-, and high-risk categories with a different protocol for each. For example, low-risk users can be approved

right away, medium-risk users will require additional due diligence, and high-risk users can be automatically rejected.

2. On-going Transaction Monitoring

The risk profile of users you've already approved can change over time. For example, a customer could get added to a sanctions list or terrorism watchlist. Your users could also get targeted by fraudsters and initiate fraudulent transactions through your product. For example, a bad actor could take over their account or use social engineering to get them to initiate a fraudulent payment.

Monitoring transactions in an on-going manner is critical for warding off these threats. Your BSA/AML policy should describe the mechanisms for detecting these events and the protocol you have in place to address issues when they arise.

3. Regulatory Reporting

Your BSA/AML policy should also include processes for supporting your bank partner in complying with their regulatory reporting obligations. There are three processes that banks most frequently require:

- **Suspicious Activity Reports (SAR):** If your CIP or transaction monitoring processes detect suspicious activity (i.e., transaction patterns used by money launderers or payments to a sanctioned entity), you should have processes in place to flag these events to your bank partner. Their compliance team will then decide whether to file an SAR with FinCEN.
- **Currency Transaction Reports (CTR):** You will need to provide a report of all transactions greater than $10,000 to your bank so that they can file a CTR form with FinCEN to comply with BSA regulations.
- **314(a) and 314(b) Requests:** You will need to support your bank partner in complying with information requests from law enforcement agencies related to an active terrorist financing or money laundering investigation. These requests, mediated by FinCEN, require banks to conduct a one-time search of their records on your accounts to identify accounts or

transactions that could be associated with the suspects of the investigation.

Depending on your use case, your bank may also require other types of regulatory reporting.

4. Internal Testing and Updates

Most banks will also require the establishment of an internal, on-going risk assessment process that can proactively identify changes to your company's risk profile. Examples of such changes could include:

- Introducing new products or services
- Changing existing products or services
- Company expansion through mergers and acquisitions

Your BSA/AML Policy should outline the details of this process and the frequency with which you will perform risk assessment.

5. Annual Independent Audits

Your bank will require a periodic, independent assessment of your compliance program from external auditors (typically every 12-18 months). Results of this assessment should be made available to the bank's compliance team.

While the specific requirements will vary based on your bank, they typically include:

- An assessment of the overall adequacy and effectiveness of the processes in your compliance program
- Transaction testing to verify your adherence to recordkeeping and reporting requirements
- An evaluation of your efforts to resolve violations and deficiencies noted in previous audits
- A review of staff training for adequacy, accuracy, and completeness

6. Record Retention

Finally, your BSA/AML Policy should retain all records generated as part of your CIP, transaction monitoring, SAR filing, and other processes, such as:

- User identifying information, like names, emails, and dates of birth.
- The methods used for verifying this information, for example digital copies of passports or driver licenses.

The retention period for these records will depend on the requirements of your partner bank.

CHAPTER 3

Software

The role of great software tools in operating a compliance program cannot be understated, especially in embedded payments products which, at a minimum, require completely automating the following workflows:

1. **Onboarding**: Recording and verifying a user's personal and bank account details so they can move money using your product.
2. **Payments:** Initiating, tracking, and reconciling payments to and from users.
3. **Controls:** Creating payment approval rules and alerts to ensure full control over automated money movement.

Each payments workflow has an associated compliance workflow that needs to be automated as well:

Payments Workflow	Compliance Workflow
Onboarding	Customer onboarding (KYC/KYB)
Payments	Transaction monitoring
Controls	Case management

Additionally, since operating a compliance program requires collecting and retaining sensitive personal information like SSNs and bank account numbers, as well as responding to regulator requests for user or transaction information, your software should also provide secure data storage and reporting tools.

In this chapter, we'll outline four key features you should look for when evaluating compliance software.

Customer Onboarding

Embedded payments and fintech products are designed for complete self-service. Users can download an app or visit a website, create an account, and start using the product. Given the importance of Customer Identification Programs in BSA/AML compliance, automating KYC and KYB checks at sign up is critical.

Key capabilities to look out for here include:

1. **Embeddable UIs:** Pre-built forms for collecting personal and business information plus bank account details provide a fast and secure way to automate data collection. These forms should also be customizable, so that you can request additional information more relevant to your use case.
2. **Real-time identity verification:** This tool should support real-time KYC and KYB by either checking user information against reputable data sources or verifying documents like passports and driver's licenses.
3. **A rules engine:** Your solution should provide a rules engine to sort users into different risk levels based on criteria custom to your business and risk tolerance. You should also be able to configure different business logic for each category.
4. **Sanctions screening**: On top of identity verification, the software should also screen information against OFAC, SDN, and PEP watchlists.
5. **User behavior biometrics:** Certain usage patterns, like copy/pasting personal information, are typically associated with fraudulent activity. Being able to intelligently detect these patterns at sign up can give your compliance program a leg up.

Transaction Monitoring

Manually checking every transaction isn't feasible for a fintech product handling hundreds of transactions a day. Since continuous monitoring is a critical regulatory requirement, your compliance tool should support automated transaction monitoring on all payments.

Key capabilities to look for here include:

1. **Ease of integration:** Transaction monitoring should be easy to integrate with your payment provider so that every single payment can be automatically checked for suspicious or fraudulent behavior.
2. **A rules engine:** Your solution should also include a rules engine to enable risk-based assessment of transactions, similar to Customer Onboarding. It should be configurable, allowing you to set up and fine tune your own criteria for different risk thresholds.
3. **Customer information checks:** On top of screening transactions, your compliance tool should also support screening the customer that initiated the transaction to detect changes in their risk profile. For example, if a user gets added to an SDN list, your compliance team should be notified.

Case Management

Combining automation with human oversight is key to building a robust BSA/AML compliance program. Case management workflows equip your compliance team to quickly investigate high-risk transactions and users in order to determine the best course of action. A "case" is any user or transaction that might require manual review.

Key features to look for include:

1. **Support for users and transactions:** Your workflow should create cases for suspicious users and transactions, since they're both likely to trigger manual reviews.
2. **Collaboration tools:** Your compliance tool should support assigning cases to different team members, adding comments, uploading documents, attaching proof of resolution, and other tasks required to resolve a case.
3. **Decision feedback:** Your team should be able to give feedback to the rules engine or algorithm about the final decision. This will help fine tune risk thresholds over time, especially in the event of a false positive or false negative.

4. **Audit logs:** Key actions for every case—such as comments and the final decision—should all be recorded in an immutable audit log. This data helps your team with internal assessments of your compliance program and can also be useful for external audits.

Record Retention

As outlined in chapter 1, retaining all records related to your compliance program is mandatory. You also need to be able to assist your bank partner in responding to 314(a) and 314(b) requests from FinCEN.

Key features to look for include:

1. **Secure storage:** Typically, compliance data includes highly sensitive PII (or personally identifiable information). You'll want to ensure your compliance software is storing it securely.
2. **Reporting tools:** Your software should include user-friendly reporting, so you can quickly respond to requests from your bank partner.
3. **Adequate access controls:** Your tool should include role-based access controls to securely manage employee access to PII.

CHAPTER 4

People

A BSA/AML policy should describe the structure, roles, and responsibilities of each member on your compliance team. It should give your bank partner a clear understanding of how the processes outlined in the policy will be executed, evaluated, and updated on an ongoing basis.

While some banks might require more details, the policy at a minimum should describe how the following groups and individuals will be involved.

Board of Directors

Your company's board should approve the BSA/AML policy. Their approval should be noted in the minutes of the board meeting. Any substantial revisions or updates to the policy may also need to be approved by the board.

Designated Compliance Officer

Your board of directors should appoint a Designated Compliance Officer (DCO) as the owner of the BSA/AML policy. This person will also serve as the primary point of contact with your bank's compliance team and may delegate some of their responsibilities to your internal compliance team. The DCO is responsible for monitoring compliance processes on a regular basis and surfacing issues and violations to the board and your bank partner.

The DCO is also in charge of internal testing and updates to the compliance program, as well as coordinating annual audits of the compliance program with independent consultants.

All Employees

It's important for all employees to be aware of your company's compliance obligations because building an internal "culture of compliance" is essential to running a robust compliance program. Your BSA/AML policy should outline the following responsibilities for your employees to:

- Understand the laws and regulations behind the policy
- Complete compliance training
- Report suspected violations to your compliance team

Third-parties

Depending on the nature of your use case with the bank, they may also require you to describe the role third-party service providers, vendors, and contractors (for example) will play in your compliance program.

CONCLUSION

Getting Started

Our hope is this eBook makes it easier for you to understand how to start setting up your compliance program. In addition to helping you draft your BSA/AML policy, assemble a compliance team, and train your employees, we hope it streamlines the due diligence process with your partner bank and helps drive a productive long-term partnership with them.

If you're looking for compliance software to streamline and automate the processes in your BSA/AML policy, you might want to explore our Compliance product. Compliance is pre-integrated with our Payments product, enabling you to launch faster with AML compliance and fraud prevention enabled on all payments from day one.

Compliance has three core features:

User Onboarding

- Save time with embeddable onboarding flows to collect personal information.
- Screen users against OFAC, SDN, PEP watchlists and adverse media databases to manage your CIP / CDD / EDD requirements.

Transaction Monitoring:

- Enable transaction monitoring on all payments to stay on top of evolving fraud patterns.
- Detect fraud and money laundering behavior with advanced machine learning algorithms.
- Fine tune detection criteria for your product over time with a no-code rules engine.

Case Management:

- Configure manual case reviews and automated judgments based on risk levels.
- Investigate cases with a unified view of user and transaction data in the Modern Treasury app.
- Collaborate easily with case assignments and notifications.

To learn more about Compliance, or explore how Modern Treasury can help power money movement for your products, please visit our website or reach out to us at sales@moderntreasury.com.