Building an Effective AML Compliance Program: a 5-Step guide

Hummingbird

hummingbird.co

ABOUT THIS PAPER

Operating a regulated business is complex, expensive, and difficult to get right. How do you balance creating a great customer experience with lowering your risk exposure and satisfying your regulators? And with limited engineering resources, do you build your compliance toolset in house or do you outsource it to a third party? This paper provides a high-level, strategic framework for establishing an anti-money laundering (AML) compliance program, and is intended for executives of fintech startups and other non-bank financial institutions.

We'll go over five core practice areas: Risk Assessment, Know Your Customer, Monitoring, Investigations, and Reports. You'll learn which questions you should be asking about your business when approaching each of them. When it comes to building an effective AML compliance program, one size fits none.

ABOUT HUMMINGBIRD

Our mission at Hummingbird is straightforward: Fight financial crime. We do this by building tools to help financial institutions investigate suspicious behavior and communicate it to law enforcement.

Hummingbird offers Automated SAR filing, and a Case Management and Reporting platform. These innovative solutions streamline case work, and the management processes associated with anti-money laundering, anti-fraud, disputes, and testing.

hummingbird.co

Stay informed about future articles and free guides by signing up for the Hummingbird newsletter **here**.

Introduction

There's a moment of reckoning when a company determines – even though it may not be a bank – that it needs to put an anti-money laundering (AML) compliance program into place.

This situation arises when fintech startups and other non-bank financial institutions offer products and services that fall under Bank Secrecy Act / Anti-Money Laundering (BSA/AML) regulation. Or, often the case, when a regulated bank requires an AML compliance program from a fintech partner.

The costs and effort of a strong AML compliance program might seem burdensome at first, but if you weigh those against the costs of inadequate compliance – such as regulatory fines, reputational damage, and even rejection by a bank partner – the strategic decision becomes clear: you want to do this right.

FIVE CORE PRACTICE AREAS

To break this big project down into manageable chunks, here are the five core practice areas common across AML compliance programs:

1. Assess Risks
2. Know Your Customer (KYC)
3. Monitoring
4. Investigations
5. Reports

Building a robust AML program isn't a one-size-fits all endeavor, as each company will have a unique risk profile. Assess your specific vulnerabilities and risk thresholds in order to tailor the most effective approach. Take a broad view of potential scenarios for how criminals might exploit your company – not just for prototypical money-laundering, but also for possible adjacent and associated financial crime.

Look at the most basic characteristics of your company: products and services, customers, and locations. Then ask questions such as:

- ✓ How easily could criminals launder money through your products?
- ✓ Could they use your products to facilitate other kinds of crime like human trafficking?
- ✓ Could they use your company as a channel for stolen credit cards and identities?
- ✓ Could they hijack your services for scams?

Q. How easily could criminals launder money through your products?

> **"The strategic decision becomes clear: you want to do this right."**

1 Assessing Your Unique Risks

Every financial institution has unique risks when it comes to financial crime. Bad people are out there probing for weaknesses in the financial industry - the strategies and tactics they use to commit financial crime are sophisticated. So how do you formulate a defense strategy and put protections in place? You start by thinking through your institution's potential risks and defining a system of defenses that will help protect you. Your risk assessment process should look broadly at all types risks facing your company - crime, fraud, money laundering, consumer rights violations, information security, and others. For this guide, though, we'll continue our focus on AML.

To identify the risk your institution has of being used to launder money, it is useful to have a framework for your thinking. Using a framework will help you think broadly about the problem and cover different perspectives.

A commonly used framework for risk assessment is to think about your financial institution along the following lines:

- ✓ **Products & services:** what financial products & services does your institution provide?
- ✓ **Customers**: what types of customers does your institution work with?
- ✓ **Geographies:** where are your customers in terms of geography?

The goal of thinking through your unique risks along these lines is to formulate a more thorough defense strategy. Since each category can be quite broad, let's explore how to use them in your risk assessment work.

Risk Factor 1: Products and Services

What products and services does your financial institution offer? The risks involved with a debit card account are different than those of a mortgage, for example. By carefully considering each product or service that you offer, you'll be able to better understand the risks associated with each.

To get you started, here's a list of a few examples of financial products & services:

- ○ Checking / savings accounts
- ○ Debit cards
- ○ Credit cards
- ○ Prepaid cards
- ○ Checks
- ○ ACH transfers
- ○ Money orders
- ○ Correspondent banking
- ○ Loans
- ○ Brokerage/ trading accounts
- ○ Cryptocurrency
- ○ Foreign currency exchange
- ○ Remote deposit capture
- ○ Wires

Q. What products and services does your financial institution offer?

To get started, consider our list of example financial products & services. Be sure to look closely at your business and consider every interaction you have with your customers at the product or service level. Be sure to watch for secondary products / services: for example, you might be a debit card provider that enables customers to fund their accounts via ACH transfer – it is important to consider the risks of both the debit cards and the ACH transfers.

Risk Factor 2: Customers

Q. Do you provide financial products and services to people, businesses, legal entities, or some combination of all these categories?

The next risk factor to consider is the profile of your customers. Do you provide financial products and services to people, businesses, legal entities, or some combination of all these categories? Within these categories, there are many different profiles, and you'll want to know which your institution works with.

CUSTOMER PROFILE

Alaskan Bank of Commerce

- Alaska
- Small business
- Family-owned
- Incomes tend to vary seasonally
- Predominantly English speaking
- Common industries include tourism, restaurants, and outdoor gear stores

If your institution provides products and services to people, think about their characteristics. Do you cater to people in a particular industry or job? A particular demographic background? People trying to achieve something specific - an auto lender likely targets people that want to buy a car, for example.

If your institution works with businesses or other types of legal entities, consider carefully what those legal entities exist for and how they might use your service. You'll want to understand what the expected behaviors of these businesses are, which could be quite different depending on what they do.

By considering the types of customers that your institution works with, you'll get a better sense of what their expected financial behaviors are. Consider the expected financial behaviors of your customers. These expected behaviors establish a baseline for your ongoing monitoring but they also inform the decisions you make in designing your program. This will help you understand the risks of each customer profile and spot strange patterns that might indicate financial crime.

> **"Consider the expected financial behaviors of your customers."**

Risk Factor 3: Geographies

The last risk factor are the geographies involved with your financial institution.

You want to think broadly about geography as well, considering things like:

- ✓ Where are your customers based?
- ✓ Where do they use your products and services?
- ✓ Are people or legal entities that you do not work with directly involved, for example the recipients of wire transfers that you send - where are they?
- ✓ Could your products and services be used when your customers are away from home?
- ✓ Are the expected behaviors associated with your products and services likely to happen in a particular place?

As a concept, geography can be a powerful risk factor, particularly when considered in combination with the products, services, and customers that your financial institution caters to.

PUTTING IT ALL TOGETHER

While each of these risk factors can be useful individually, you will probably do your best risk assessmentwork when you consider them together. We recommend thinking of them as a matrix that can help you identify where criminals might exploit your institution.

With this framework for risk assessment in place, you'll be better equipped to design a strong AML program.

2

Know Your Customer

While each of these risk factors can be useful individually, you will probably do your best risk assessment work when you consider them together. We recommend thinking of them as a matrix that can help you identify where criminals might exploit your institution.

Let's go over the basics of the second core AML compliance area and how it may apply to your company.

What's the Point of KYC?

When you are in the money business, it's a good idea to know who you're dealing with. Companies in the financial industry need to know who their customers are -who they are processing transactions for, lending money to, or providing savings accounts to.

This is what the Know Your Customer (KYC) practice area is all about: the data and procedures used to identify your customers.

So why not just ask your customers who they are? This is certainly a good starting point, but you can't trust criminals to give an honest answer. An "ask but verify" approach is a better way to operate.

KYC touches on one of the deepest, most fascinating concepts of the modern world (in our opinion): identity. How do you know someone is who they say they are? How do you verify identity, keeping in mind that you have to do it in different settings. How do you know someone signing up for your service online is the person they claim to be? How do you know someone signing up for your service is who they claim to be?

Identity verification is a fascinating problem, particularly on the web. You won't need to solve the problem for the entire Internet, but you will need to have a compliant KYC program if you want to operate a financial institution. Luckily there are data sources and identity verification techniques that can help you put together a KYC program.

> "How do you know someone signing up for your service is who they claim to be?"

Know Your KYC Data

Getting the KYC process right from the get-go will save many headaches later on. The first step is to determine the information you need to know from new customers and ensure that your onboarding process collects it.

Common KYC information for individuals include name, address, date of birth, and some sort of ID number. Corporate KYC, sometimes called “Know Your Business” or KYB, requirements include company vitals and ownership structures, as well as individual-level data.

The full set of appropriate customer KYC data fields and the verification processes will vary significantly between companies. As an example, banks are subject to something called the “Customer Identification Program” or “CIP’; which carries a specific set of requirements. On the other hand, Money Services Businesses have a bit more flexibility.

To figure out what other information to collect, the appropriate speed of verification, and the risk level of your specific institution, consider:

- Methods of opening accounts
- Types of identifying information available
- Size of your company
- Customer base
- Geographic customer subgroups
- Product/Service use customer subgroups

These considerations can help you figure out what you need to know about your customers - it depends on the unique risks faced by your service. When setting up your KYC program, we also recommend talking to an expert.

The KYC compliance program should then check the customer-provided data against public records, vendor databases, and your company’s own research. The intent of this process is to know whether your customer has any warning signs or risk signals you should be aware of before providing them with your financial services.

KYC and Onboarding Customers

The KYC practice area has a direct impact on how customers sign up for your financial services. The customer onboarding process is generally where KYC information is collected, and it's helpful to think KYC information coming from two primary channels:

- ✓ Information that the customer provides directly to you (e.g. name, email, etc.)
- ✓ Information that you can obtain about the customer from other sources

KYC data sources commonly look at public records, court records, employment history, education, residence history, and other information about people. This information can be licensed from KYC vendors, and does not need to be collected directly from your customers.

In the digital setting, financial service providers view onboarding flows as a competitive differentiator: the easier your sign up flow, the less drop off you will have when people try to join your service. Peer-to-peer payment apps like Venmo, Square Cash, Paypal, and others have spent years optimizing these onboarding flows, and are constantly refining their KYC procedures to reduce the amount of information that users have to provide directly.

That process of optimization is beyond the scope of this article, but the key to remember is KYC information can be obtained through both of the channels mentioned previously: directly from the customer or in the background through KYC data providers.

INTEGRATING KYC

An optimal program would leverage RegTech KYC solutions that integrate well with technology for other practice areas, such as investigations and suspicious activity report filing. A common issue we see in KYC is licensing the data, but failing to integrate it into compliance workflows. With the KYC data well integrated with case management and workflows, compliance teams are forced to switch between systems and look through fairly raw data sources in order to complete investigations - it's a lot of time spent on tedious work.

This is one of our core focus areas at Hummingbird: integrating KYC directly into the case management and investigation flows. With the information pre-integrated, investigators spend a lot less time hunting around for things.

While knowing your customer marks an initial step in setting up a compliance program, it is only the first pillar.

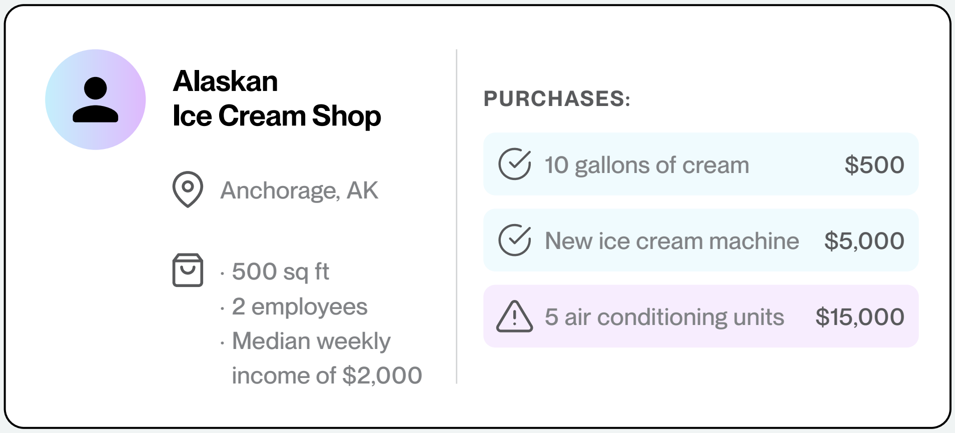
> **"The easier your sign up flow, the less drop off you will have when people try to join your service."**

3 Transaction Monitoring

When a customer opens an account, the customer onboarding process captures some initial Know Your Customer data. For example, the customer might say they're a company selling a variety of items in the southwestern United States. You have that first set of KYC information, great.

In the next step of anti-money laundering compliance, a fintech startup or financial service provider needs to ask: are the customer's transactions consistent with the given identity? Do they fit with expectations? Or does something about the account activity seem odd? Do the customer's transactions fit with expectations?

CUSTOMER PROFILE



Alaskan Ice Cream Shop

Anchorage, AK

· 500 sq ft
· 2 employees
· Median weekly income of $2,000

PURCHASES:

✓	10 gallons of cream	$500
✓	New ice cream machine	$5,000
⚠	5 air conditioning units	$15,000

An AML compliance program needs a transaction monitoring system to watch customer behavior. Monitoring systems will apply rules to flag transactions that could be suspicious, either because they match financial crime typologies or stand out as anomalies in behavior.

Monitoring systems also track high-risk customers, identified during onboarding or after a case investigation, for enhanced due diligence or ongoing customer monitoring. For example, a customer might work with a high-risk country, or they might have a dubious reputation.

Companies facing AML compliance requirements have two main choices for establishing their AML transaction monitoring systems: hire a vendor or build it in-house.

Mind the differences between anti-fraud and AML when it comes to transaction monitoring.

Anti-fraud monitoring systems can ideally make fast risk calculations and make decisions on transactions in real time – this is how you prevent loss to fraudulent activities.

In contrast, money launderers will rarely commit fraud (they don't want to be detected!), and monitoring rulesets need to identify unusual patterns of behavior over time. Further, certain AML rules are required by regulation.

When thinking through your monitoring strategy, make sure you consider both anti-fraud and AML algorithms.
You will need both, but they don't necessarily have to come from the same solution.

> **"Do the customer's transactions fit with expectations?"**

Vendor Systems

Vendor transaction monitoring systems may be sufficient if your needs aren't complicated or you're just getting started. Buying a transaction monitoring system from a vendor often provides an out-of-the-box set of protections. The main benefit of working with a monitoring vendor is the ability to get a system in place quickly. However, an out-of-the-box solution isn't going to be great at providing protection against the unique risks you face. With a bit of scale or added complexity in your business, the monitoring coverage from a vendor can start to feel inadequate. Companies that outsource their monitoring may start to feel that they need more customization and better analytics to address their unique risks.

Does a vendor have accessible APIs that easily integrate with your company's other systems?

The better monitoring systems have accessible APIs that can function smoothly and effectively with the other parts of your overall AML compliance program

(such as Hummingbird's investigation and reporting platform, which is designed to complement monitoring systems and has modern APIs).

Building In-House

Building in-house takes investment, but will likely provide better coverage for unique risks and ability to scale over time. You retain control over the decisions you make for transactions: whether to allow, review, or prevent the transaction. If you are a financial institution that handles transactions, this decision is core to your business.

Transaction monitoring is an investment like any other area of your business operations. You'll need the technical resources to build, maintain, and improve the system. It may make sense to outsource monitoring to a vendor as you are getting things started, but we recommend making continuous refinements to the algorithms and investing in the practice area over time.

Build vs. Buy

Here are a few factors that will help you form a roadmap for the monitoring practice area at your financial institution. Consider what approach will fit best with your company's current growth stage, business model, and other systems in your AML compliance program.

Buying a vendor monitoring system has its benefits:

- It requires fewer technical resources.
- You can get monitoring up and running more quickly.

... But you should also consider the drawbacks:

- Would a vendor system meet all your regulatory requirements?
- Do you have unique risks that may not be well covered by a vendor?
- Would you be outsourcing a critical decision flow of your business?
- Would the vendor system easily integrate with other systems?
- Would it scale as you grow? Would unit costs make sense as you scale?
- Would you be able to refine, adapt, and upgrade the system as you grow and learn?

4 Case Investigations

When your AML transaction monitoring system flags an activity, or another trigger prompts a review, your compliance team will need to conduct a case investigation. The customer behavior could have a perfectly legitimate explanation. Or it could be a tip that helps law enforcement crack a terrorist financing syndicate.

Case investigations are particularly critical junctures in AML, both for companies as well as regulators. Unfortunately, there tends to be a defensive impulse towards over-reporting. It's understandable, but a blunt approach can backfire in effectiveness, as well as budgets. Approaching case investigations with care, wisdom, and the appropriate technological resources will contribute to more meaningful inputs towards protecting society.

The Association of Certified Anti-money Laundering Specialists (ACAMS) developed the 360 Degree AML Investigation Model as a professional standard to guide compliance teams through case investigations. Their model advises probing the situation with the following six steps.

Politically Exposed Person (PEP): A person who holds a prominent public position. They might be susceptible to behaviors such as bribery or corruption.

Understand the Trigger

What was the cue for this review? Is it the first alert you've had for this customer? What monitoring system rule prompted this alert? Periodic monitoring, an adverse media alert, a law enforcement referral, or a regulator's response to reported activity could also be part of this sequence of events.

Understand the Customer

Take a closer look at who they are and what they do. You'll really appreciate your earlier efforts with Know Your Customer data at this point! Round out the KYC data you have with more information.

For instance, consider:

- ✓ Has your team investigated the subject before? What did they find?
- ✓ Could their cultural background help explain some behaviors?
- ✓ Are they a Politically Exposed Person?
- ✓ What products do they hold and why?
- ✓ Can you find any adverse information associated with the customer or their business, close associates, or family?

> **"Unfortunately, there tends to be a defensive impulse towards over-reporting."**

Understand the Activity

Take all the information-transactions, accounts, locations, entities with whom they interact, and their expanded identity details-and look at how a big picture fits together … or not. What story do they tell about this customer's story?

Eliminate the Norm

Pare away the information that makes sense in order to focus on the parts that don't fit a normal, legitimate pattern. The information you want to hone in on could be something like a series of in-person transactions in different states at the same time.

Decide if the Activity Is Suspicious

Evaluate the unusual behavior holistically. Transactions on their own may appear insignificant, but the context of the entire account and past behavior can help you to identify them as suspicious. A predicate offense, a recent event such as an adverse media mention or criminal charges, can be very conclusive at this step. Gut-level instincts can also contribute to your decision: ACAMS suggests considering if the behavior "raises questions or gives rise to discomfort, apprehension, or mistrust."

Report and Consider Divesting

If you've decided the activity rises to the level of "suspicious," you'll proceed on to the next practice area, filing a Suspicious Activity Report (SAR) or other related reports. But there's another question to resolve: Whether or not to keep this customer? Compare the benefits of maintaining this relationship against the risk appetite of your financial services company.

REQUEST A DEMO

Case investigations are not easy, and they demand a combination of clear data and a strong analytical process. Consider how your team will access and organize disparate pieces of information for an overall view. Regtech systems such as Hummingbird can help direct attention to the most significant details and patterns, while automating away the routine, laborious parts of investigations.

Request a demo →

> **"Evaluate unusual behavior holistically."**

5

Filing Suspicious Activity Reports (SARs)

Slight possibility you could help identify a crime ring? Okay, that does make regulatory compliance kind of exciting. Filing out long, complicated forms? Ah, not so much.

We've been going fairly light on explaining how Hummingbird's anti-money laundering regtech tools can help, but Suspicious Activity Report (SAR) filing has such a glaring need for automation that we have to be blunt here: it's time to move on from manual processes. Efficiency and cost reduction are compelling reasons for your company. Better SAR data accuracy and quality could serve your compliance performance, employee morale, and society.

2.3M
SARs filed
In 2019, a total of 2.3M SARs were filed

2-4
hours spent
Investigators can spend 2-4 hours on each SAR

28%
of costs
Financial institutions spend 28% of total compliance costs on reporting suspicious activity

What is a SAR?

SARs are the predominant channel for information in AML compliance. If a case investigation concludes a customer's activity could be suspicious, your company will then need to file a SAR (or a UAR). To recap from earlier, suspicious activity includes financial transactions that: do not make sense, are unusual for a customer, or appear to be obfuscating another transaction.

The SAR form has many fields, nebulous requirements, and is tricky to validate. Filing them is a complex process, prone to errors. Without automation, each SAR can take investigators around 2-4 hours. Financial institutions spend 28% of total compliance costs on this practice area. Incorrect or overlooked SARs can result in costly penalties and painful remediation requirements.

> **"Without automation, each SAR can take investigators 2-4 hours."**

How Hummingbird Can Help

SARs are difficult to operationalize at a financial institution and can be a huge drain on compliance resources. Technology can help make SAR information more accurate, complete, and useful.

Hummingbird can help:

- Ensure investigations follow a thorough process.
- Get more detailed information into SARs.
- Spot trends across different reports.
- Run checks to ensure that the information is valid and meets specifications.
- Use automation to eliminate the time spent filling out forms by hand.
- Increase information security through direct integration with FinCEN rather than maintaining PDF reports on employee computers.
- Deliver the information to law enforcement quickly.

As we mentioned earlier, there's also your compliance team's sense of purpose and the good of society. The information in SARs can be difficult to parse, and there are significant unmet needs for collaboration among the financial industry, regulators, and law enforcement. A recent U.S. Government Accountability Office report addresses how law enforcement "may be underutilizing these reports - to the detriment of their investigations." Meanwhile, criminals are getting increasingly sophisticated in their use of technology. Better data and broader adoption of AML regtech across institutions could enhance communication and capabilities among banks, regulators, and law enforcement.

Unusual Activity Reports (UARs)

Most financial institutions file SARs directly to a regulatory agency-overall they filed 2.3 million in 2019. But fintechs that have a compliance program in order to support a banking partnership typically file Unusual Activity Reports (UARs) to the regulated financial institution, which then holds the responsibility for determining in each case whether or not to file a SAR. Note that the word "suspicious" carries legal weight for regulated financial institutions. Fintech partners should be very careful about how and where you use it.

SARs and UARs have different requirements for formatting, timelines, and content. Filing them the right way, at the right time is important. Hummingbird makes filing either type of report easy-we know the regulations inside-out and have built the technology to automate the process. To ensure that your banking partner or regulatory agency receives accurate, timely, and correctly formatted reports, consider how a Hummingbird system could be a strategic choice for your company.

WHAT'S NEXT?

Through various sections of this guide, you've learned how to approach five core AML practice areas: Risk Assessment, Know Your Customer, Monitoring, Investigations, and Reports. With these fundamentals in mind, you can now get started building the AML compliance program that best suits the needs of your business. But how do you do that, exactly?

The key idea we've come back to time and again in this paper is this: when it comes to building an effective AML compliance program, one size fits none. That's why Hummingbird offers free 30-minute advisory sessions where you can get guidance and recommendations specific to your business. You'll speak with compliance experts, including former regulators, compliance program operators, and policy makers; and come away with clear next steps.

When it comes to case management and reporting, Hummingbird offers the most complete solution on the market. Our customers range from pre-launch fintechs to some of the largest financial institutions in the world. If you'd like to learn more about how Hummingbird can help meet your unique business needs.

Book your session →

Contact info@hummingbird.co to schedule a demo to learn more!