Unit21

8 Step AML Compliance Checklist

A 65-Point Framework for Success

Compliance teams are the key to identifying financial crimes such as money laundering. Financial intelligence units (FIUs) have issued a record number of fines in the millions and tens of millions of dollars against organizations for not having an effective anti-money laundering compliance program.

Even as fines have been issued, Financial institutions see regulatory expectations changing.

To protect them from high-risk transactions and customers, financial institutions must put processes including training and risk compliance, in addition to tools such as sanctions list screening, risk scoring, regulatory reporting, and transaction monitoring.

Although not containing everything needed for a perfect AML compliance program, the following eight-step checklist covers the main areas where a financial institution will need to have policies and practices in place.

How to Implement an Effective AML Compliance Program

The Identity Verification process, or Know your Customer (KYC) / Business (KYB), is the first step in determining a customer's identity. It starts the risk and AML process because no further steps can be taken until the customer's identity is confirmed. The KYC process involves customer due diligence, i.e., assessing the risk of doing business with the customer during both onboarding and on an ongoing basis after that. This process demands a balancing act of protecting the business and genuine customers, while maintaining a seamless user experience.

The right solution in place allows organizations to differentiate between good customers and fraudsters and, in doing so, build trust, prevent fraud, and maintain compliance with regulatory obligations. On average, in a year, a financial organization can lose up to $15 million for the consequences of non-compliance.

Step 1: Appointing a Chief Compliance Officer

To have a successful compliance program, a financial institution must have strong senior management to set the institution's standards. In addition, compliance teams must have an in-depth understanding of their institution and the possible areas of risk where regulatory breaches can happen.

The first step to best understanding and assessing possible areas of risk in your company is to establish a Chief Compliance Officer (CCO). They must also communicate the institution's fundamental principles and compliance regulations to the rest of the institution's employees.

Compliance officers must take responsibility for the daily enforcement of the compliance.

Compliance officers are responsible for frequent enforcement of the program and must clearly explain it to all employees. That culture of compliance should be seen in all corporate departments and will help promote all employees to engage in good conduct.

The Chief Compliance Officer is often the head of the compliance department, and under that position, there are multiple levels of management depending on the institution's size.

The compliance teams also include specific AML compliance officers with the crucial skills, support, and authority to manage the AML compliance program across the entire institution.

The compliance team must have strong connections with other groups in the institution, for example, the fraud and legal departments.

Also, the Chief Compliance Officer should connect with the Board of Directors who oversee the institution's Bank Secrecy Act / Anti-Money Laundering compliance program. The board must receive reports from the compliance team regarding the company's financial risks.

8 TRAITS OF A HIGHLY EFFECTIVE CCO: WHAT TO LOOK FOR

Strong Leadership Skills

Public Speaking Savvy

Business Acumen

Collaboration Skills

Detail Oriented

Courage

Analytical Mindset

Integrity

□ **Strong Leadership Skills:** The CCO must be perceived as both a leader and a peer by others within the C-Suite. It would be detrimental to have someone who is not able to stand up for themselves handling compliance. This person must be capable of leading by example. Since the CCO will be responsible for setting the tone for internal compliance, they must understand the goals of the company's business leaders and gain their confidence so they can have transparent and impactful conversations.

□ **Public Speaking Savvy:** The CCO cannot be uncomfortable presenting to the board of directors. They must be able to point out any issues with compliance that they uncover, and be willing to offer solutions to fix those issues on the spot.

□ **Business Acumen:** A good CCO will help to grow the business while remaining in full compliance with all regulations. This requires a solid grasp of how the business operates.

□ **Collaboration Skills:** a CCO must be willing to work with everyone in the company to ensure they are in full compliance with all regulations. They do not work in a vacuum and this is not a one-person job — it takes a cooperative team to remain fully compliant.

□ **Detail Oriented:** A CCO must be able to tackle details (regardless of size) as they pertain to regulations.

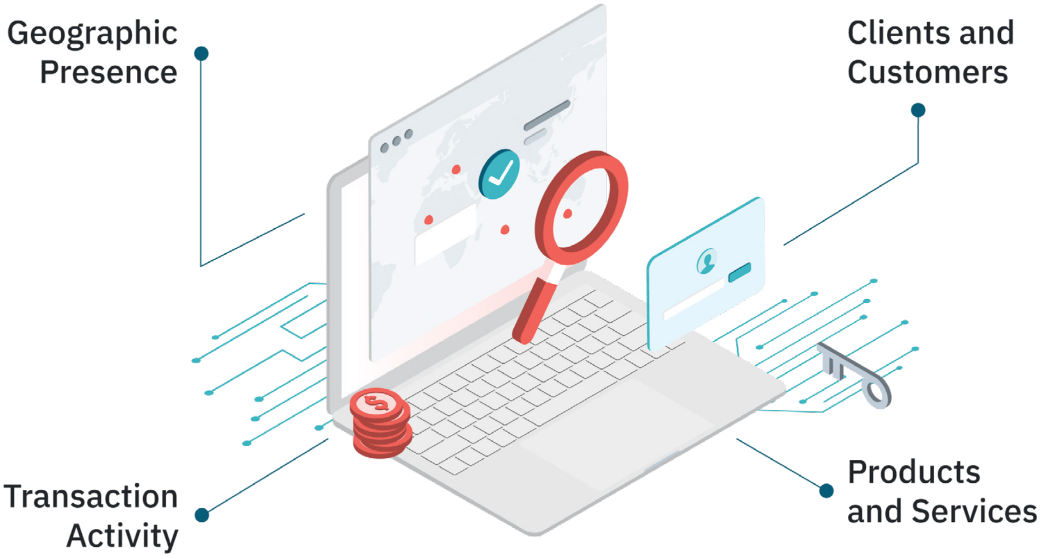
□ **Courage:** Compliance Officers must be comfortable speaking up and calling attention to potential problems. It is imperative that someone in this role can let management know immediately when something is amiss.

□ **Analytical Mindset:** A good CCO will be able to figure out what a new regulation means and what impact (if any) it will have on the organization.

□ **Integrity:** One of the most important traits of an excellent CCO is their integrity. Someone in this role must understand the rules and the implications for not following them, and be able to do the right thing by sticking to the rules in the event that breaking them might seem like an enticing option.

Step 2: Performing Risk Assessments

One of the first steps in an AML compliance program is **risk assessment** and the documentation of potential risks your company may face.



During this step, it is essential to consider:

- □ How your institution handles its clients.
- □ What your institution's overall risk tolerance is.
- □ What regions your institution operates in.
- □ What type of products your institution offers and what their potential risks are.
- □ If your institution is willing to take more significant risks in some areas, and if so, which areas and how much risk.

The primary AML risk areas that your institution should evaluate are:

- □ Clients/customers and their relationships with the institution.
- □ Your institution's products and services.
- □ The transaction activity of your institution.
- □ Your institution's geographic presence.

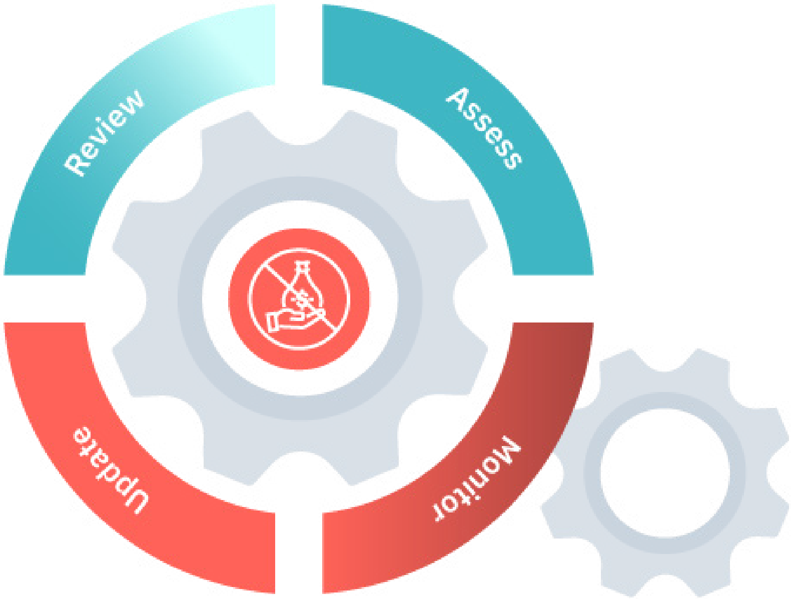
In addition to doing an initial risk assessment, your institution should re-examine them quarterly or semi-annually, depending on the institution.

Step 3: Writing AML Policies and Procedures

Your institution must document its AML policies and procedures in detail. When planning AML processes, remember to:

- □ Ensure your institution has procedures in place for onboarding new customers, monitoring transactions, and investigating suspicious activity.
- □ Implement procedures so your institution can operate within acceptable standards in the locations where you do business.
- □ Make sure what you are doing is auditable and thoroughly documented.
- □ Have procedures for reporting and investigating suspicious activities within the company.
- □ Make sure your institution has monitoring and controls in place to report to financial authorities, such as Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs).
- □ Frequently inspect processes to ensure that your institution is doing what it promised to do and adequately addresses new potential risks.
- □ Make sure new products or lines of business follow your compliance program’s guidelines and risk tolerance.

Step 4: Maintaining an AML Program

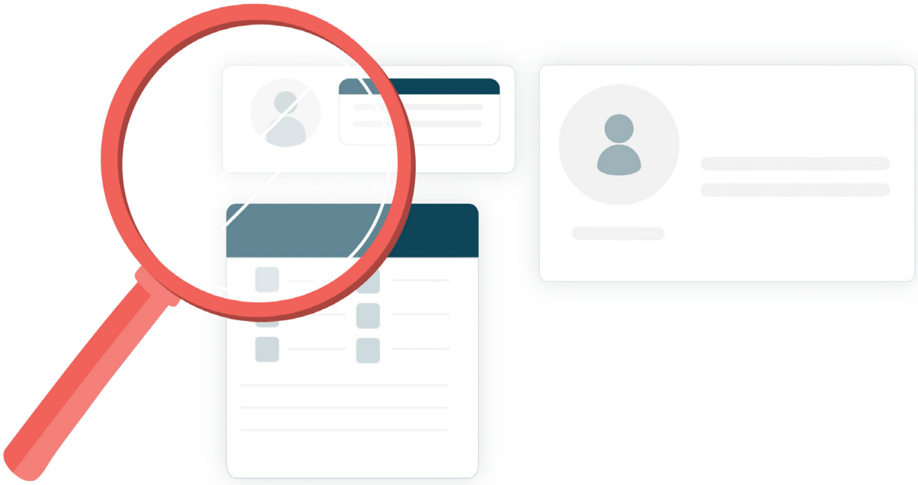


Whether implementing a new AML program or upgrading an existing program, it's essential to:

- □ Periodically review your company's policies to make sure they align with the regulations of its jurisdiction, and research or discuss with your institution's legal team regarding new state, provincial or federal regulations.
- □ Frequently carry out risk assessments to flag new and emerging risk areas so your institution can implement preventive or corrective strategies to fix compliance issues.
- □ Ensure that programs put in place to vet employees or customers are adequate for your company's size, complexity, and geographic reach. Needs can change as your institution grows or adds new products/services.
- □ Continuously monitor operations and procedures of the different areas of your institution to ensure complete compliance.
- □ Regularly monitor client activities to ensure they comply with bank policies and are legal. What your institution must monitor and how they should go about doing so could evolve with the introduction of new products, new regulations, or changes in technology.
- □ Create and update your procedures for the handling and resolution of policy infractions.
- □ Work with senior managers to properly implement new policies and ensure compliance with existing ones.

- □ Work with other departments, including the risk management or internal audit unit, to forward compliance issues for investigation.
- □ Educate and train everyone on your institution’s current or future compliance policies, procedures, and requirements and participate in seminars, conferences, and workshops to improve knowledge.
- □ Record any changes in policies and procedures and ensure that everyone in the organization is trained on these changes.
- □ Perform intermittent independent testing of the effectiveness of your AML program.
- □ Ensure that the outside organizations interacting with your institution meet your compliance requirements.
- □ Administer internal audits before external audits to ensure that policies and operations are up to standard.
- □ Regularly update senior management on the progress of compliance operations.

Step 5: Applying Due Diligence



Knowing your customers is an essential part of an AML program. Therefore, it is crucial to understand the difference between Customer Identification Program (CIP), **Customer Due Diligence (CDD)**, and **Enhanced Due Diligence (EDD)** programs.

A financial institution’s KYC process must include all three.

To have a successful KYC process, your program should have both a Customer Identification Process (CIP), a Customer Due Diligence Process (CDD), and an Enhanced Due Diligence Process (EDD).

CUSTOMER IDENTIFICATION PROGRAMS

Customer identification programs (CIPs) collect a customer's information, including their name, date of birth, home address, and ID number, to know that they are not falsely identifying themselves.

CUSTOMER DUE DILIGENCE

A successful CDD process should do these things:

- □ Completely identify the customer and business entities, including the source of funds and beneficial ownership if necessary.
- □ Create transactional activity profiles of each customer's expected future activity.
- □ Define and accept how the customer can use certain products and services.
- □ Assess and grade the potential risk that a customer or an account has.
- □ Monitor a customer's account and transactions based on that risk.
- □ Investigate and analyze unusual activity.
- □ Document findings.

CDD processes should also include periodic risk-based monitoring of the customer relationship to determine whether there are substantial changes to the original CDD information (for example, change in employment or business operations).

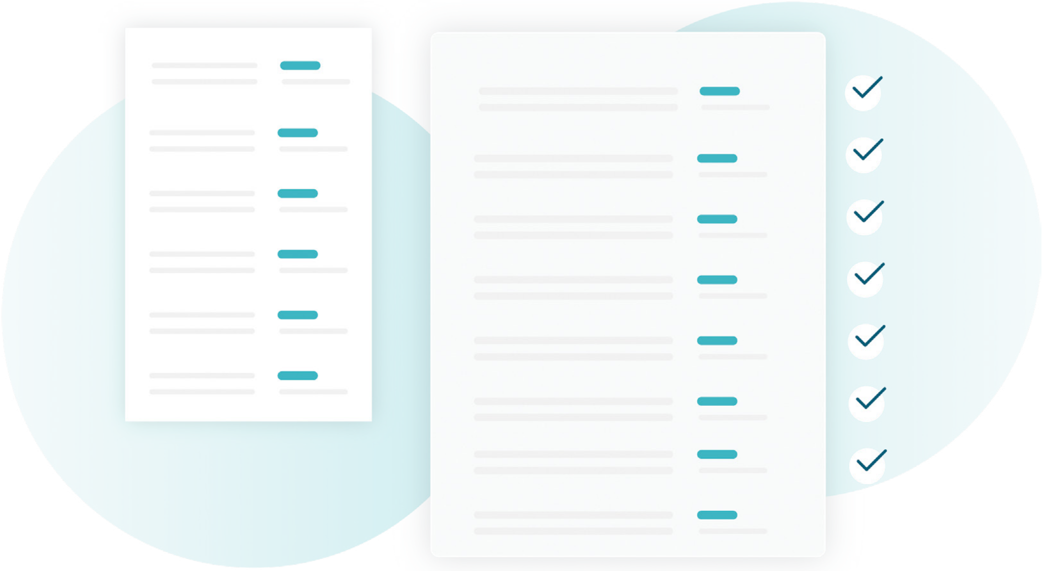
ENHANCED DUE DILIGENCE

Enhanced due diligence (EDD) is along the same lines as CDD, except it requires added measures to find and minimize the potential risk of high-risk customers.

It also requires developing a more profound knowledge of the customer's behavior, the customer's business, the types of business activities, and what level of risk they present.

Step 6: Screening Against Watch and Sanctions Lists

Companies are required to screen new customers as well as transaction records against lists of known high-risk individuals, including suspected terrorists or narcotics traffickers, or against sanction lists to make sure customers are not on either. If a financial institution comes across a possible “sanction hit” or “sanction match,” the institution must conduct further investigation to decide whether or not they have had an actual sanctions exposure.



Despite sounding simple, the process of successfully filtering out individuals that could potentially be on sanctions or on watch lists is more challenging.

Therefore, your sanction screening program should consider:

- □ The risk reference data that your institution is using. The size and jurisdiction of your institution can cause your risk profile to vary greatly, meaning that your institution could have a different sanctions list that it has to comply with.

- □ Narrative sanctions. Narrative sanctions are sanctions where, instead of an individual being listed, there is only a list of criteria that cause them to be included on the list. This poses a challenge to financial institutions because there is no specific sanctions list to follow, yet they must not make transactions with them if they meet the criteria.

- □ The use of law enforcement and adverse media data. You should make sure that you are screening records against lists from local, national, and international law enforcement agencies, including the FBI, Interpol, Europol, in order to determine if there are FATF predicate offenses. Institutions can also use adverse media from news sources to screen for involvement in FATF predicate offenses.

- □ The management of **Politically Exposed Persons (PEPs)** and State-Owned Entities. Some institutions get PEPs data from risk reference data, whereas others get it from actual sources. However, in both situations, your institution should have policies on how to handle entities marked as PEPs as well as processes for identifying and controlling state-owned entities.

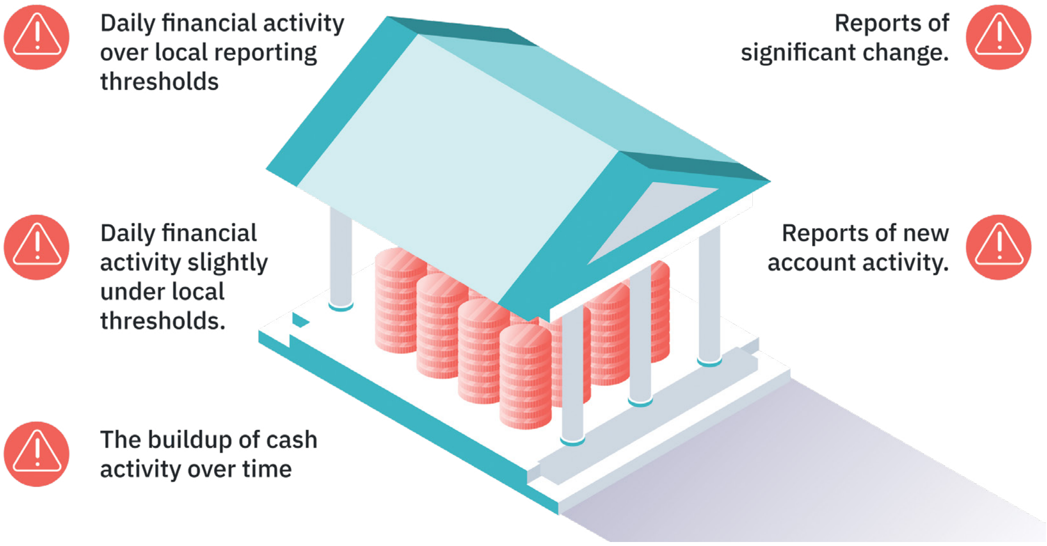
- □ Whether or not your institution has taken a risk-based approach to screening. There are a lot of determinants when trying to identify possible sanction matches, so it is crucial to ensure your software can catch these high-risk individuals.

- □ Potential name variations. Institutions should ensure that they can handle possible name variations, nicknames, and aliases.

- □ Whether or not your system effectively handles transliteration and translation. It is challenging for programs to screen for names with accents, names not in Latin-native characters, or names with other language-specific characters. Your institution should ensure that their screening program is able to handle the transliteration and translation when screening names of individuals.

Step 7: Monitoring and Screening Transactions

Analyzing transactional data and identifying suspicious activities that could indicate money laundering or other financial crimes are both integral parts of **transaction monitoring** processes.



Daily financial activity over local reporting thresholds

Daily financial activity slightly under local thresholds.

The buildup of cash activity over time

Reports of significant change.

Reports of new account activity.

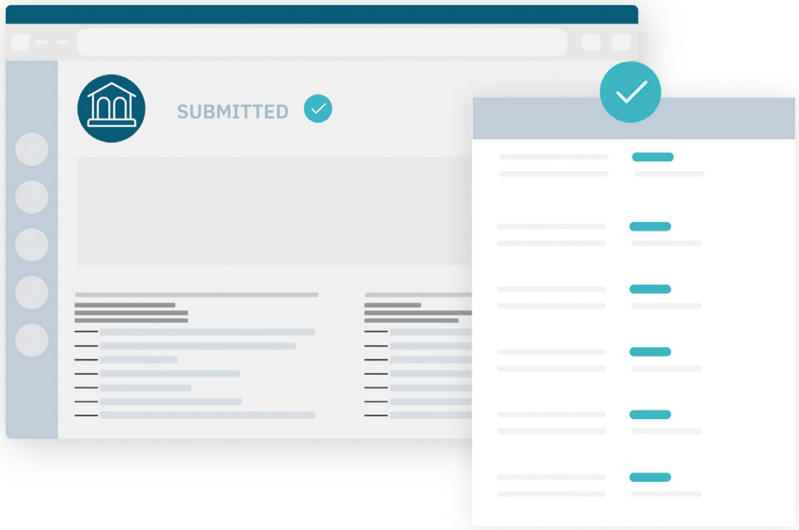
According to ACAMS (Association of Certified Anti-Money Laundering Specialists), some indicators of financial crime or money laundering are:

- □ Daily financial activity over local reporting thresholds.
- □ Daily financial activity slightly under local thresholds.
- □ The buildup of cash activity over time; several individual transactions of a specific amount add up to a more considerable amount of money.
- □ Reports of significant change.
- □ Reports of new account activity.

According to ACAMS, in a financial institution, a typical suspicious transaction reporting progress constitutes of:

- □ Suspicious transaction or activity identification using various methods such as observations or identifications by employees, an examination from law enforcement, or alerts from transaction monitoring systems.
- □ A complete evaluation of each case of suspicious activity or transaction.
- □ Documentation of reporting decisions regarding suspicious transactions.
- □ Programs to notify senior management or board of directors regarding suspicious transaction filings.
- □ Training for employees to detect suspicious activity or transactions.

Step 8: Reporting Suspicious Activities to Regulators



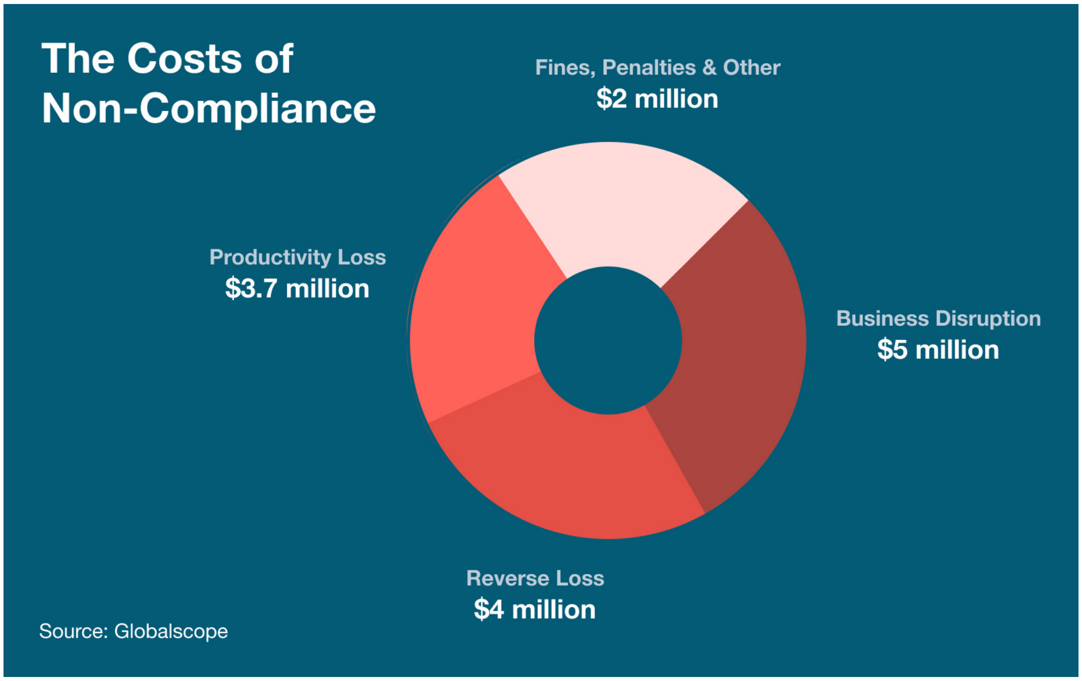
Under most jurisdictions, Financial Intelligence Units (FIUs) require all financial institutions to report suspicious activity signifying financial crimes such as terrorist financing and money laundering, and will therefore require that institutions:

- □ Determine and confirm the identity of individuals/organizations involved.
- □ Gather transaction information and give reasons for the transaction(s) being marked as suspicious.
- □ Do not inform clients of suspicious activity filings.
- □ Give all information necessary to FIUs.

These processes and requirements vary by location, so institutions must check what obligations apply to them by checking with FIUs or their legal team.

How Unit21 Helps With AML Compliance

Unit21 was built to empower Risk and Compliance Operations teams and has helped hundreds of organizations avoid the deep costs of non-compliance through the use of no-code transaction monitoring, AML case management, and identity verification tools.


The Costs of Non-Compliance

Source: Globalscope

Here are three ways that Unit21 is driving impact for customers.

1. Highly Visible

Look Beyond Transactions

Unit21 does more than just transaction monitoring. The solution encompasses more data and activities by bringing in actions, instruments, entities to monitor. Test and tune rules with both historical and future data to assess what works best for more accurate anomaly detection and investigations.

An End-to-End Solution

Unit21 provides an all-in-one solution from identity verification and transaction monitoring to case management in one system. It works with consistent datasets in one consolidated end-to-end view to track users for anomaly detection and investigations. Increase visibility and provide operators with a more seamless experience to provide more accurate assessments.

Elevate Your Team

Unit21 provides management-level reporting and analytics to help assess risk and compliance operations and team performance. Disentangle operators from the weeds so they can focus on high-risk cases.

2. Self-Managed and Streamlined

Focus on Risk and Compliance, Not Engineering

Unit21 provides an easy drag-and-drop, no-code interface that can easily be used by risk and compliance teams — reducing reliance on engineering. Teams can tweak rules on-the-fly, and test immediately.

One-Click Filing

Unit21 is intelligently automated with workflow orchestration and e-filing to regulators with integrations into FinCEN and GoAML directly from the dashboard — saving time and resources.

Day 1 Ready

Unit21 has 1,000+ tried and true, pre-built rules, models, and integrations to get started on Day 1 to meet compliance standards for your industry.

3. Scales With You as You Grow

Purpose-Built for Your Team; By Your Team

Easily customize rules and workflows to adapt to unique changes in company and regulations. Your compliance team who are closest to the action can define their operations. Create custom permissions and bring in your custom data with webhooks to control your risk and compliance approach.

Combining the Best of Customization + Automation

Unit21 provides a balance between automation and control. We provide the right rules, workflows, and automation to give teams the baseline they need to get started. Build and customize upon pre-built and automated features to continually adapt to evolving threats.

Adapt and Grow

Unit21 offers ID verification, Transaction Monitoring, and Case Management on an all-in or modular basis. Unit21 enables you to seamlessly connect to its other solutions as you scale and grow – making you adaptable to your changing environment.

Customer Story:

intuit®

Intuit has a diversified business model with a focus on innovation and providing exceptional experiences to their 50 million clients. Intuit's risk vectors have become increasingly complex as their transactions grow.

Challenges

- Transaction monitoring and case management to capture complex patterns that are more specific to Intuit's business
- Need for a high degree of automation and configurability so that teams would spend less time on manual tasks such as data aggregation and report generation, and more time on the actual investigation
- Customization would involve costly professional services hours or own internal software

Use Case

- Transaction Monitoring
- Case Management

Why Unit21?

- The ability to easily create, test, and deploy complex logic for identifying suspicious activity, without having to write any code
- The flexibility and automation of the Unit21 platform to solve large-scale problems

Impact

- 65% reduction in alert investigation times
- Used data monitoring engine to combine intelligence in anomaly detection and explainability for reporting

> *"We looked at a lot of software vendors. There isn't another product that competes with Unit21. The flexibility and automation of the Unit21 platform renders completely new ways for solving problems at scale."*
>
> — Rob DeCampos,
> Head of BSA/AML
> at Intuit

Customer Story:

bakkt™

> *"Unit21 is solving our biggest problem by monitoring hundreds of thousands of customer accounts. And the best thing is that we have been able to achieve a steady 15% false positive rate. That is a huge deal in an industry where 90-95% is the norm."*
>
> — Kailey Klein,
> Compliance and AML
> Officer at Bakkt

Bakkt is a digital asset platform that combines many different transactions with the vision to bring trust and transparency to digital assets. Bakkt unlocks the 1.20+ trillion digital assets that are currently held in cryptocurrencies, rewards and loyalty points, gaming assets and merchant- stored value. Consumers can now liquidate digital assets to trade, transfer and pay in any way using Bakkt.

Challenges

- Looking for a Fraud and AML solution to accommodate the scale of their growth from 500K to 9M customers
- Spending too much time manually filing SARs; 90 minutes on each case

Use Case

- Transaction Monitoring
- Case Management

Why Unit21?

- Ease of one system and pulling reports for auditors
- Automation capabilities
- Proactive and knowledgeable customer service

Impact

- Automatic transaction monitoring with a baseline of 15% false positive rate, versus industry averages of 95%+
- Reduced SARs management time by 66% to 20 minutes

80%+

Reduction in False Positives

Unit21 customers see a significant decrease in false positive rates. Teams become more effective since they can focus on what matters.

$100B+

Activity Monitored

Unit21 has monitored over $100B+ in transactions. We protect customers against hundreds of millions of dollars of fraud loss and money laundering.

50%+

Reduction in Fraud Losses

The enhanced detection and operational efficiency afforded by Unit21 enables customers to achieve more accuracy and cut fraud losses in half.

Backed by Google, Tiger Global Management, and other leading investors, Unit21 is redefining how risk and compliance teams fight financial crime. Unit21's fully customizable no-code platform provides a simple API and dashboard for detecting, investigating, and reporting on fraud, money laundering, and other sophisticated risks across multiple industries. ***Schedule a demo*** *today to see our platform in action.*

343 Sansome Street, Suite 1600
San Francisco, CA 94104