Lesson 7.1: Why Regulation Exists — AML, KYC, and Financial Crime

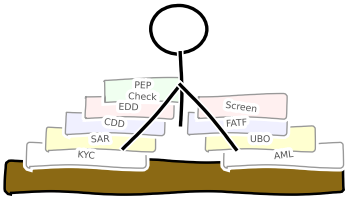
Module 7: The Compliance Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

The Compliance Maze

"I just want to send $50 to my friend..."



Meanwhile, in Compliance...

"False positive #4,827 this week..."

The $274 billion question: are we catching criminals or just generating paperwork?

Learning Objectives

After completing this lesson, you will be able to:

1. **Explain** why financial regulation exists and what market failures it addresses [Understand]
2. **Describe** the AML framework including CDD, EDD, and SAR filing [Understand]
3. **Apply** a risk-based approach to classify customer risk levels [Apply]
4. **Trace** a suspicious transaction through the SAR reporting pipeline [Apply]
5. **Analyze** the trade-offs between compliance cost and financial crime prevention effectiveness [Analyze]
6. **Evaluate** whether current AML/KYC frameworks are proportionate to the threats they address [Evaluate]

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.

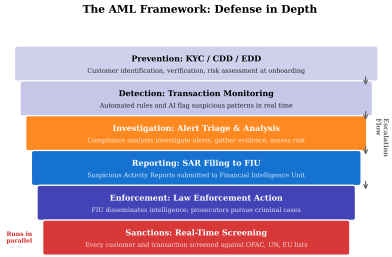
From Building Systems to Governing Them

Modules 1–6 covered how finance works:

- Payments, access, trust, risk, automation, infrastructure
- FinTech innovations that transform each layer
- Algorithms, blockchains, and platforms that move money

Module 7 asks: what rules govern all of this?

- Why can't you just **send money to anyone, anywhere**, without questions?
- What stops the financial system from becoming a **laundry service** for criminals?
- Who decides what is **suspicious** — and what happens when it is?
- How much does compliance **cost**, and is it worth it?



The AML framework: layers of defense that underpin trust in the financial system.

We have built and measured financial systems (M1–M6). Now: what rules govern them?

Core Rationale

Financial regulation exists because **unregulated financial systems** produce predictable failures: fraud, systemic collapse, exclusion of vulnerable populations, and exploitation of information asymmetries.

Four pillars of financial regulation:

Pillar	What It Addresses
Financial stability	Preventing systemic collapse (bank runs, contagion, too-big-to-fail)
Consumer protection	Ensuring fair treatment, disclosure, suitability of products
Market integrity	Preventing manipulation, insider trading, fraud
Financial crime prevention	Stopping money laundering, terrorist financing, sanctions evasion

This lesson focuses on the fourth pillar: financial crime prevention — AML, KYC, and sanctions.

Regulation is the price of trust: without it, the financial system cannot function.

Market Failures That Justify Regulation

Without regulation, financial markets suffer from:

1. **Information asymmetry:** Sellers know more than buyers (e.g., loan quality, product risk)
   - Leads to adverse selection and moral hazard
2. **Negative externalities:** One institution's failure imposes costs on others
   - A bank collapse can trigger a chain reaction across the system
3. **Public goods problem:** Financial stability benefits everyone, but no single firm has incentive to provide it
   - Each firm free-rides on others' prudence
4. **Bounded rationality:** Consumers cannot evaluate complex financial products
   - Payday loans, structured products, crypto tokens exploit this

Key insight: Financial crime *amplifies* all four failures — laundered money distorts markets, funds further crime, and erodes trust.

Regulation corrects market failures that the market itself cannot fix.

The Scale of Financial Crime

Financial crime is not a marginal problem — it is an industry:

Crime Type	Estimated Annual Scale	Source
Global money laundering	$800B – $2T	UNODC estimate (2–5% of global GDP)
Fraud losses (US alone)	$8.8B	FTC, 2022 consumer reports
Ransomware payments	$1.1B	Chainalysis, 2023
Sanctions evasion	Hundreds of billions	US Treasury estimates
Tax evasion (offshore)	$600B+	Tax Justice Network

Yet: Estimated **less than 1%** of illicit financial flows are intercepted and frozen.

The paradox: The compliance system costs $274B+ annually worldwide — but catches a tiny fraction of criminal money. Is the system effective, or is it security theater?

The scale of financial crime dwarfs the resources allocated to fighting it.

Definition: Money Laundering

Money laundering is the process of making **illegally obtained money** appear to come from a **legitimate source**. It disguises the origins, ownership, or destination of criminal proceeds so they can enter the legal financial system.

The three stages of money laundering:

Stage	Name	What Happens
1	**Placement**	Criminal cash enters the financial system (e.g., deposited in small amounts below reporting thresholds — "structuring")
2	**Layering**	Multiple transactions obscure the trail (e.g., wire transfers, shell companies, currency conversion)
3	**Integration**	"Clean" money re-enters the economy (e.g., real estate purchase, business investment)

Each stage is a potential detection point — and each stage has different red flags.

AML frameworks are designed to detect and disrupt laundering at every stage.

FATF: The Global AML Standard Setter

The Financial Action Task Force (FATF):

- Intergovernmental body founded in 1989 by the G7
- Sets the **40 Recommendations** — the global AML/CFT standards
- 39 member jurisdictions + 2 regional organizations
- Conducts **mutual evaluations** of member countries' compliance
- Maintains the "grey list" and "black list" of non-compliant jurisdictions

FATF is not a law-making body:

- It issues **recommendations**, not legally binding rules
- But: being grey-listed has severe economic consequences (reduced correspondent banking access, higher transaction costs)

FATF 40 Recommendations — key areas:

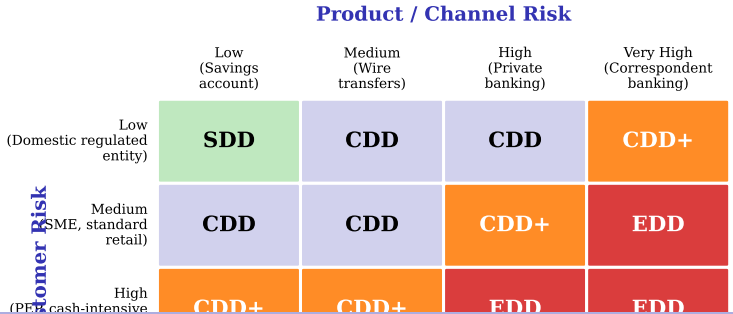
1–2	Risk assessment, national coordination
3–8	ML/TF offenses, confiscation
9–23	Preventive measures (CDD, record-keeping, STR)
24–25	Transparency of legal persons/arrangements
26–35	Institutional framework
36–40	International cooperation

FATF sets the global standard — every country's AML laws trace back to the 40 Recommendations.

Definition: Risk-Based Approach

The **risk-based approach** requires institutions to identify, assess, and understand their money laundering and terrorist financing risks, and then **allocate resources proportionally**: higher-risk customers and products receive more scrutiny; lower-risk ones receive less.

Risk-Based Approach: Due Diligence Matrix



Risk Factors in AML Assessment

Institutions assess risk across four dimensions:

Risk Dimension	Examples of Higher-Risk Indicators
Customer risk	Politically Exposed Persons (PEPs), cash-intensive businesses, non-resident customers, complex ownership structures
Geographic risk	FATF grey/black-listed jurisdictions, countries with weak AML regimes, conflict zones, tax havens
Product/service risk	Private banking, correspondent banking, anonymous instruments, crypto assets
Channel risk	Non-face-to-face relationships, third-party introductions, high-value wire transfers

Risk scoring: Each factor contributes to a **composite risk score** that determines the level of due diligence required (SDD, CDD, or EDD).

Risk factors are cumulative: a PEP in a high-risk jurisdiction using private banking triggers maximum scrutiny.

KYC: Know Your Customer

Definition: KYC

Know Your Customer (KYC) is the mandatory process by which financial institutions verify the **identity** of their clients, understand the **nature and purpose** of the business relationship, and assess the **risk** the customer poses for money laundering or terrorist financing.

KYC is not a one-time check — it is a continuous obligation:

1. **Customer identification** at onboarding
2. **Customer verification** against reliable sources
3. **Understanding the business relationship** (purpose, expected activity)
4. **Ongoing monitoring** throughout the relationship
5. **Periodic reviews** based on risk level

Why KYC matters: If you do not know who your customer is, you cannot detect suspicious behavior — because you have no baseline for "normal."

KYC is the foundation of the entire AML framework — without it, nothing else works.

KYC Onboarding: The Process

KYC Onboarding Flow: From Application to Account

Key principle: No account is opened, no transaction is processed, and no relationship is established until KYC is satisfactorily completed.

KYC onboarding is the first line of defense — it determines who is allowed into the financial system.

CDD vs. EDD: Levels of Due Diligence

Customer Due Diligence (CDD):

- Standard level for all customers
- Verify identity using reliable documents
- Identify beneficial owners (25%+ ownership threshold in most jurisdictions)
- Understand purpose of the relationship
- Ongoing monitoring of transactions

Applies to: Typical retail and commercial customers.

Enhanced Due Diligence (EDD):

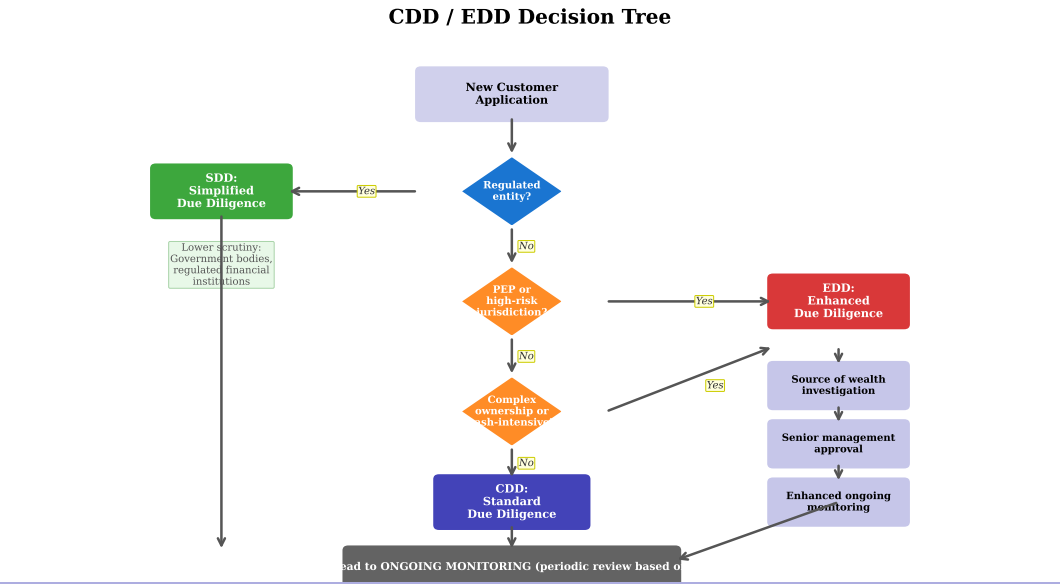
- Deeper scrutiny for higher-risk customers
- **Additional** identity verification steps
- Source of wealth and source of funds investigation
- Senior management approval required
- More frequent ongoing monitoring
- Detailed record of rationale for proceeding

Applies to: PEPs, high-risk jurisdictions, complex structures, correspondent banking.

Simplified Due Diligence (SDD) may apply to *low-risk* customers (e.g., regulated entities, government bodies) — but only where risk assessment justifies it.

The level of due diligence must be proportionate to the assessed risk — more risk means more scrutiny.

CDD/EDD Decision Tree



Beneficial Ownership: Who Really Controls the Money?

Definition: Beneficial Owner

A **beneficial owner** is the natural person who **ultimately owns or controls** a legal entity, or on whose behalf a transaction is conducted. Typically defined as any person holding $\geq$25% ownership or exercising significant control.

Why beneficial ownership matters:

- Shell companies and layered structures are the **primary tool** for hiding criminal wealth
- A company can have multiple legal layers, each in a different jurisdiction
- Without transparency, the **true controller** of assets remains invisible

Global developments:

- EU Anti-Money Laundering Directives require **public beneficial ownership registers**
- US Corporate Transparency Act (2024): requires companies to report beneficial owners to Financial Crimes Enforcement Network (FinCEN)
- FATF Recommendation 24: all countries must ensure transparency of legal persons

If you cannot see through the corporate structure to the human being behind it, AML is defeated.

Suspicious Activity Reports (SARs)

Definition: SAR

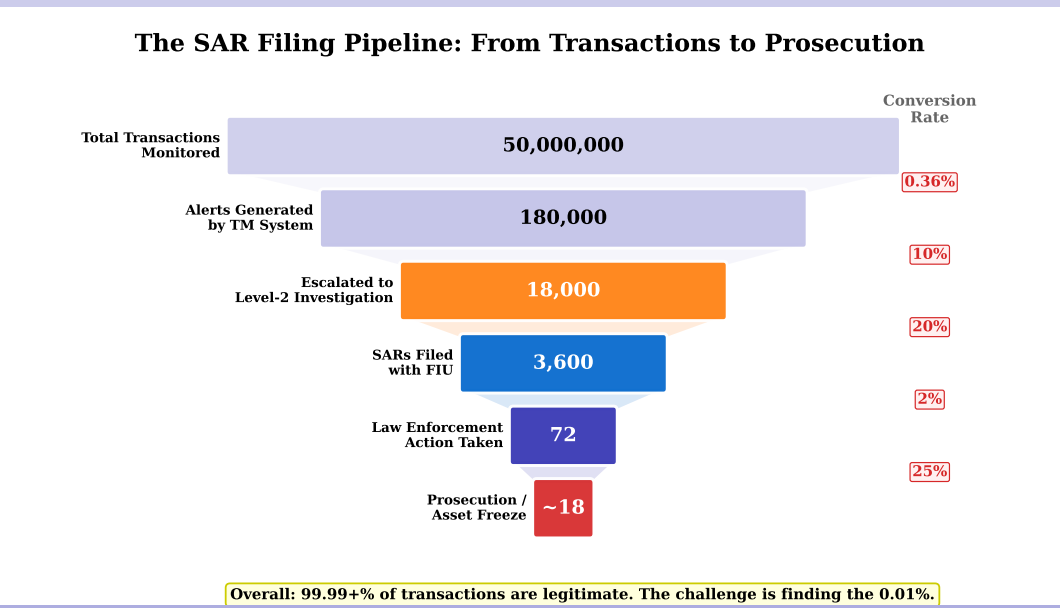
A **Suspicious Activity Report (SAR)** is a filing made by a financial institution to its Financial Intelligence Unit (FIU) when it **knows, suspects, or has reasonable grounds to suspect** that a transaction involves proceeds of crime, terrorist financing, or other illicit activity.

Key SAR principles:

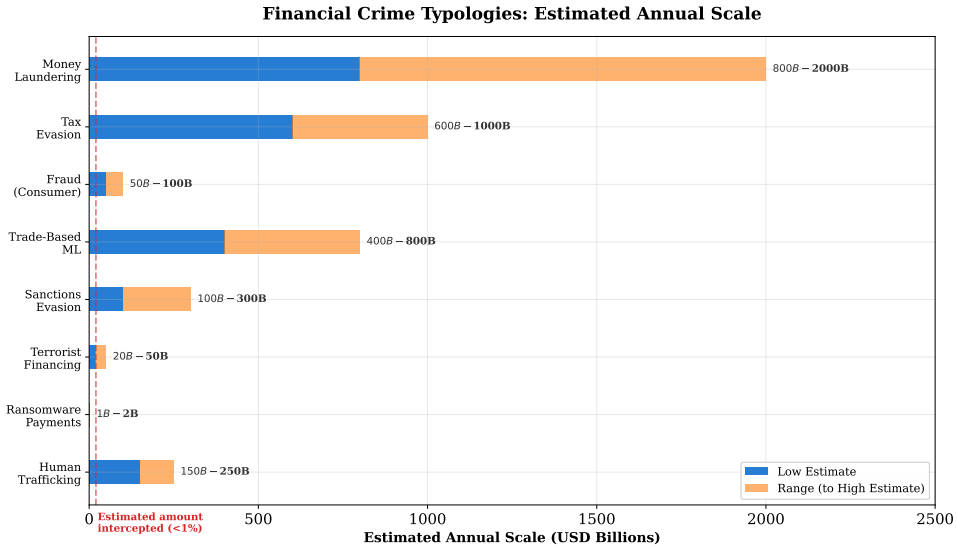
- **Mandatory:** Filing is a legal obligation, not optional
- **Confidential:** Institutions must **not** inform the customer that a SAR has been filed ("tipping off" is a criminal offense in most jurisdictions)
- **Defensive:** SARs protect the institution from prosecution for handling criminal funds
- **Low threshold:** "Suspicion" does not require proof — reasonable grounds are sufficient

Volume problem: US institutions filed **4.6 million SARs in 2023**. FIUs cannot analyze them all — leading to the "needle in a haystack" problem.

SARs are the primary intelligence feed from the private sector to law enforcement.



Financial Crime Typologies



Understanding typologies helps compliance teams recognize patterns — each crime type has characteristic red flags.

Red Flags: Detecting Suspicious Activity

Common red flags that trigger further investigation:

Transaction-based:

- Transactions just below reporting thresholds ("structuring")
- Rapid movement of funds through multiple accounts
- Large cash deposits inconsistent with the customer's business
- Frequent wire transfers to/from high-risk jurisdictions
- Round-number transactions with no apparent commercial rationale

Behavior-based:

- Customer is evasive about source of funds
- Use of third parties to conduct transactions
- Reluctance to provide KYC documentation
- Account activity inconsistent with stated occupation
- Sudden changes in transaction patterns
- Customer shows unusual knowledge of reporting thresholds

Key principle: No single red flag is proof of crime. Multiple red flags *in combination* raise the suspicion to the point of requiring a SAR.

Red flags are indicators, not proof — but ignoring them can make the institution criminally liable.

Definition: Sanctions

Sanctions are restrictions imposed by governments or international bodies (UN, EU, Office of Foreign Assets Control (OFAC)) that prohibit or restrict financial dealings with specific **persons, entities, or countries**. Violating sanctions can result in criminal prosecution and massive fines.

Types of sanctions:

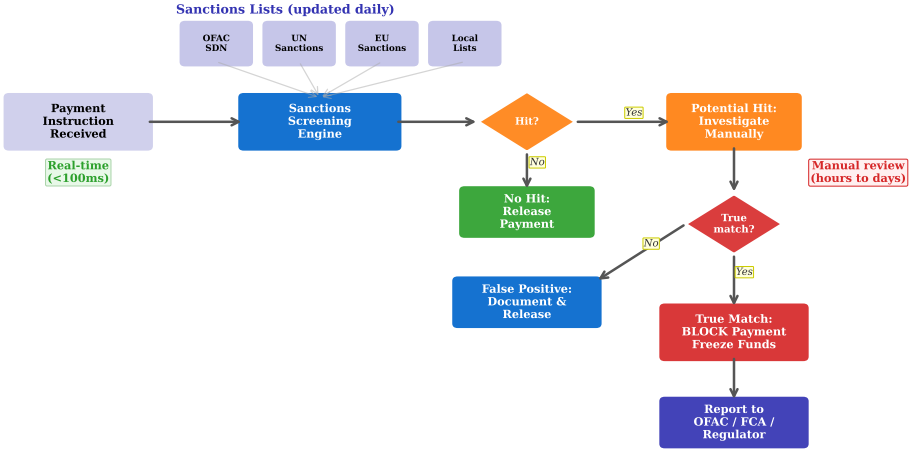
Type	Description
Targeted / "smart"	Specific individuals or entities (Specially Designated Nationals (SDN) list)
Sectoral	Restrictions on specific sectors (e.g., energy, defense) in a country
Comprehensive	Near-total embargo on a country (e.g., North Korea, Iran)

Strict liability: In many jurisdictions, sanctions violations are **strict liability** offenses — intent is not required. Even an accidental payment to a sanctioned party can result in prosecution.

Sanctions compliance is non-negotiable: a single violation can cost billions in fines and destroy a bank's reputation.

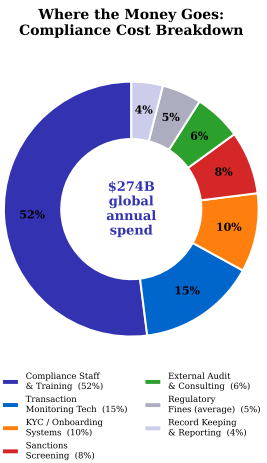
Sanctions Screening: How It Works

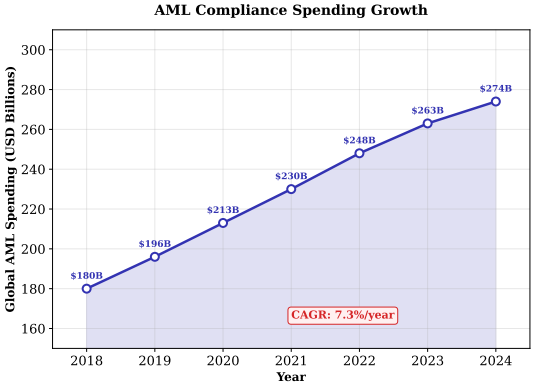
Sanctions Screening Flow: From Payment to Resolution



Screening happens at multiple points:

The Cost of Compliance





Global AML compliance spending: Estimated **$274 billion** per year (LexisNexis Risk Solutions, 2023).

Major cost drivers:

- Staff (compliance analysts, investigators, MLRO) — typically 50–60% of total cost

The False Positive Problem

Transaction monitoring systems generate massive volumes of alerts — most of which are false positives:

Metric	Typical Range	Implication
Alerts generated per day	500–5,000	For a mid-sized bank
False positive rate	95–99%	Only 1–5% lead to SARs
Analyst time per alert	30–60 minutes	Manual investigation required
Cost per alert	\$20–\$50	Including analyst salary
SAR-to-prosecution rate	$<1\%$	Most SARs are never acted upon

The compliance trap:

- Reducing thresholds $\rightarrow$ more alerts $\rightarrow$ more false positives $\rightarrow$ analyst fatigue $\rightarrow$ *real* suspicious activity gets lost
- Raising thresholds $\rightarrow$ fewer alerts $\rightarrow$ missed true positives $\rightarrow$ regulatory penalties

This is where AI/ML enters: Machine learning can improve the signal-to-noise ratio (covered in Module 5).

A 95% false positive rate means 19 out of 20 investigations are wasted effort — but the 1 in 20 could be real crime.

Terrorist financing differs from money laundering in a critical way:

	Money Laundering	**Terrorist Financing**
Source of funds	Illegal (proceeds of crime)	Often *legal* (salaries, donations, businesses)
Amounts	Typically large	Often very small ($500–$5,000)
Goal	Disguise origin	Fund an act or organization
Detection challenge	Follow the money trail	Small, legitimate-looking amounts

The detection paradox: The 9/11 attacks cost approximately $400,000–$500,000 to execute. Individual transactions were well below reporting thresholds. This makes detection through traditional transaction monitoring extremely difficult.

CFT is harder than AML because the funds are small, often legal in origin, and indistinguishable from normal activity.

De-risking: When Compliance Causes Exclusion

Definition: De-risking

De-risking is the practice of financial institutions **terminating or restricting** business relationships with entire categories of clients or regions to avoid the perceived risk of money laundering or sanctions violations — rather than managing the risk.

Consequences of de-risking:

- **Correspondent banking withdrawal:** Major banks have exited relationships with banks in the Caribbean, Pacific Islands, Africa, and the Middle East
- **Money transfer operators (MTOs):** Remittance companies lose banking access, pushing flows underground (including informal value transfer systems like hawala)
- **Non-profit organizations:** Charities operating in conflict zones are denied accounts
- **Entire countries:** Some nations lose access to the global financial system

The irony: De-risking is meant to reduce financial crime risk, but it **pushes transactions into unmonitored channels** (cash, informal networks, crypto), making financial crime *harder* to detect.

De-risking is compliance failure disguised as compliance success — it shifts risk, it does not eliminate it.

AML in the Digital Age: New Challenges

Digital finance creates new AML challenges that legacy frameworks were not designed for:

Challenge	Why It Matters
Crypto assets	Pseudonymous, cross-border, no central intermediary to monitor
Neobanks / digital onboarding	Non-face-to-face verification increases identity fraud risk
Peer-to-peer payments	Instant, high-volume, often below monitoring thresholds
Decentralized finance (DeFi)	No regulated entity to impose KYC
AI-generated deepfakes	Can bypass video-based identity verification
Privacy coins / mixers	Designed to break the transaction trail

Regulatory response: FATF's "Travel Rule" (Recommendation 16) now requires virtual asset service providers (VASPs) to share sender/receiver information — mirroring the wire transfer rules that banks already follow.

AML frameworks must evolve at the speed of financial innovation — and they are struggling to keep up.

The Travel Rule: AML for Crypto

FATF Recommendation 16 — The Travel Rule

When a virtual asset transfer exceeds a specified threshold (typically \$1,000/€1,000), the originating VASP must send the beneficiary VASP the **sender's name, account number, and address** (or equivalent). The beneficiary VASP must obtain the **receiver's name and account number**.

Implementation challenges:

- No universal messaging protocol between VASPs (unlike SWIFT for banks)
- **Unhosted wallets** (self-custody) have no VASP on one side of the transaction
- Jurisdictional differences: some countries implemented the Travel Rule; others have not
- Privacy vs. surveillance tension: blockchain transparency vs. data protection (GDPR)

Emerging solutions: TRISA, OpenVASP, and Notabene are building interoperable messaging layers for VASP-to-VASP Travel Rule compliance.

The Travel Rule extends traditional AML principles to crypto — but technical implementation remains fragmented.

Enforcement: What Happens When Compliance Fails

Major AML enforcement actions (selected):

Institution	Year	Fine	Violation
HSBC	2012	$1.9B	Mexican drug cartel laundering
BNP Paribas	2014	$8.9B	Sanctions violations (Sudan, Iran, Cuba)
Danske Bank	2022	$2.0B	€200B suspicious flows through Estonia branch
Binance	2023	$4.3B	AML/sanctions violations, unlicensed operation
TD Bank	2024	$3.1B	Systemic AML failures across US operations

Beyond fines:

- **Criminal prosecution** of individuals (compliance officers, executives)
- **Deferred prosecution agreements** (DPAs) with multi-year monitoring
- **Loss of banking license** (ultimate sanction)
- **Reputational damage** that outlasts the fine itself

AML fines have grown from millions to billions — and personal criminal liability for compliance officers is increasing.

The Money Laundering Reporting Officer (MLRO)

Definition: MLRO

The **Money Laundering Reporting Officer (MLRO)** is the designated individual within a financial institution who is responsible for overseeing AML compliance, receiving internal suspicious activity reports, and deciding whether to file SARs with the FIU.

MLRO responsibilities:

1. Receive and evaluate internal suspicious activity reports from staff
2. Decide whether to file SARs with the national FIU
3. Ensure the institution's AML policies, procedures, and controls are adequate
4. Report to the board on AML risk exposure
5. Act as the primary contact for regulators on AML matters

Personal liability: In many jurisdictions, the MLRO faces **personal criminal liability** if the institution fails to file SARs or maintain adequate controls. This makes the MLRO one of the most legally exposed roles in banking.

The MLRO is the human gatekeeper between the institution's internal monitoring and law enforcement.

Components of an AML Program

Every regulated institution must maintain an AML program with these components:

#	Component	Description
1	Internal policies and procedures	Written AML/CFT policies approved by senior management
2	Designated compliance officer (MLRO)	Named individual with authority and resources
3	Ongoing employee training	All staff trained to recognize and report suspicious activity
4	Independent audit/testing	Regular independent review of AML controls
5	Risk assessment	Enterprise-wide ML/TF risk assessment, updated regularly
6	Customer due diligence	KYC, CDD/EDD procedures
7	Transaction monitoring	Automated systems plus manual review
8	Sanctions screening	Real-time screening against sanctions lists
9	Record keeping	All CDD records and transaction data retained for 5+ years

An AML program is only as strong as its weakest component — regulators test all nine.

Is AML Working? The Effectiveness Debate

Arguments that current AML is effective:

- Without AML, the financial system would be **completely unmonitored**
- SARs have led to major law enforcement successes (e.g., FinCEN Files)
- AML frameworks create a **deterrent effect** even if detection is imperfect
- International cooperation (FATF, Egmont Group — a global network of Financial Intelligence Units) is improving

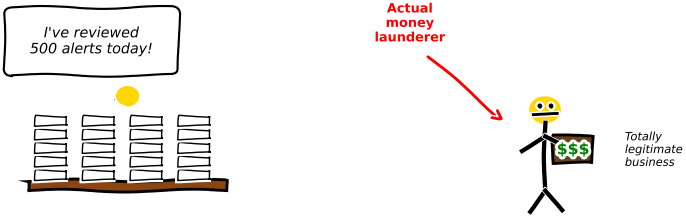
Arguments that current AML is failing:

- **Less than 1%** of criminal money is intercepted
- $274B annual cost for a system that catches a "tiny fraction" of illicit flows
- False positive rates above 95% waste analyst time
- De-risking excludes legitimate customers and pushes crime underground
- Rules-based monitoring is **easily circumvented** by sophisticated launderers

The reform question: Should we make the system more efficient (better technology, shared data) or fundamentally rethink the approach?

AML may deter more crime than it detects — but measuring deterrence is inherently difficult.

One Last Thought...



Sometimes we're so busy checking boxes, we miss the obvious red flags.

Sometimes the best way to remember a concept is to laugh about it.

Key Takeaways

1. **Financial regulation** exists to correct market failures: information asymmetry, externalities, public goods, and bounded rationality
2. **AML frameworks** target the three stages of money laundering: placement, layering, and integration
3. **FATF** sets the global standard through 40 Recommendations; non-compliance has severe economic consequences
4. The **risk-based approach** allocates scrutiny proportionally: higher risk $\rightarrow$ more due diligence
5. **KYC** is the foundation: identify, verify, understand, and continuously monitor every customer
6. **SARs** are the intelligence pipeline from banks to law enforcement — but volume overwhelms analysis
7. **Sanctions screening** is strict liability: even accidental violations can result in billion-dollar fines
8. **De-risking** is an unintended consequence that pushes activity into unmonitored channels
9. Current AML catches **less than 1%** of illicit flows at a cost of \$274B/year — the effectiveness debate is unresolved

---

Compliance is not optional, not cheap, and not easy — but it is the price of a financial system people can trust.

Key Vocabulary

- Anti-Money Laundering (AML)
- Know Your Customer (KYC)
- Countering Financing of Terrorism (CFT)
- Financial Action Task Force (FATF)
- Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD)
- Simplified Due Diligence (SDD)
- Suspicious Activity Report (SAR)
- Financial Intelligence Unit (FIU)
- Money Laundering Reporting Officer (MLRO)
- Risk-Based Approach (RBA)
- Politically Exposed Person (PEP)
- Beneficial ownership
- Placement / Layering / Integration
- Sanctions screening (OFAC, SDN list)
- De-risking
- Travel Rule (FATF Rec. 16)
- Structuring ("smurfing")

These terms form the foundation for understanding financial crime compliance.

Summary / Next Lesson Preview

This lesson: We explored why financial regulation exists, how AML/KYC frameworks work, the mechanics of suspicious activity detection, sanctions screening, and the uncomfortable reality that compliance is expensive, imperfect, and yet indispensable.

Central insight: The AML system is a risk-based filter applied to the entire financial system. It cannot catch all crime, but it creates a framework of accountability, deterrence, and intelligence-sharing that makes the financial system inhospitable to criminals — most of the time.

Next lesson (M7L2): *RegTech and Supervisory Technology* — We will examine how technology is transforming compliance: AI-powered transaction monitoring, automated regulatory reporting, and the emerging field of SupTech (supervisory technology used by regulators themselves).

Review: Can you trace a suspicious transaction from detection through SAR filing to law enforcement action?