

AMLift

AMLIFT HANDBOOK SERIES · 2026

# AML Compliance Fundamentals Handbook

A complete guide to AML fundamentals, from the basic rules to how careers work in this field. It is written for people about to start their first AML job, and for experienced AML professionals who want to refresh their knowledge before an interview or to stay up to date.

26 modules · 7 parts · KYC · TM · SAR · Sanctions · Crypto · Built by AML practitioners



Google "[learn AML](#)" and the first page of results shows the problem. The results fall into four groups. First, course marketplaces that sell single paid courses with no link to what comes before or after. Second, corporate training companies that make required courses so employers can show the training was done, not so people learn and grow. Third, certification bodies that charge for programs lasting several weeks, built for people already set on a compliance career, not for a fresher who is just starting or an experienced AML professional who needs a quick, accurate refresher. Fourth, scattered posts from individual AML professionals: useful, but personal, informal, and out of date once the author stops updating them. None of these link the fundamentals, the refresher, the career path, and keeping up with changes. And none of them show what the job is really like on a normal workday with forty alerts waiting for review.

So we built what was missing. At every stage of an AML career, from getting a first job to refreshing skills years later, the same gap appears: most material explains the rules well, but rarely shows how to apply them to a real case or how to explain that thinking in an interview. This handbook is free, kept up to date, and puts the fundamentals, the refresher, and the career path in one place. It's also the first step toward something bigger: a real community of AML and financial-crime professionals. It is not meant to be read once and forgotten. It is a place to come back to as the field changes and your career grows.

There are twenty-six modules, in the order the work happens: basics first, then the laws and regulators, then the checks on customers, then the casework itself, then a full section on fintech and crypto, and finally how hiring and career growth really work, whether you're trying to get in or move up.



AMLIFT · [amlift.tech](https://amlift.tech)

## WHO THIS IS FOR

# Two different starting points

### Freshers

Preparing for your first AML, KYC, or transaction monitoring role? Or already in a junior role, following checklists without fully knowing why they exist? This handbook explains the reasons behind them.

### Experienced professionals

Every experienced AML/FinCrime professional reaches a point where their core knowledge needs a refresh: before an interview, before moving to another country's rules, or after months on one type of work while the rest of the field changed. This handbook is built to refresh your knowledge quickly and keep it accurate, not just to teach beginners.

## Where to start reading

- New here? Read [Part I](#) (p. 7) through [Part III](#) (p. 21) in order. Each one builds on the last.
- Refreshing? Jump straight to the regulatory timelines in [Module 03](#) (p. 9) and the crypto coverage in [Module 20](#) (p. 35). Those two areas are the most likely to have changed since you last looked.
- Treat every "red flags" box as interview prep, not just study notes.
- [Part V](#) (p. 34) covers fintech and crypto, where the field is changing quickly right now. Don't skip it.
- [Module 26](#) (p. 46) ends with how hiring managers review AML resumes, and how careers grow from there.

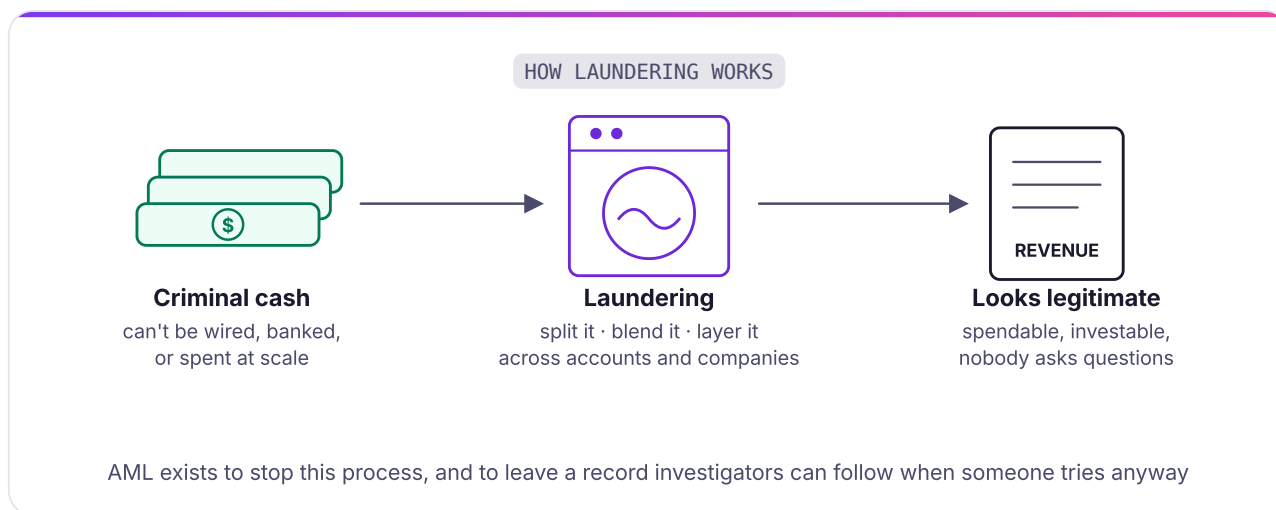
### BEFORE WE BEGIN

## What money laundering actually is

Set the acronyms aside for now. Here is the simple version.

The Financial Action Task Force, the international body that sets the global AML standard, defines **money laundering** as "the processing of criminal proceeds to disguise their illegal origin." In simple terms, the money itself is not the problem. The problem is the link between that money and where it really came from. That link is exactly what a criminal wants to erase, so they can spend it, invest it, or move it through the banking system without anyone asking where it came from.

Imagine a group that sells illegal drugs and ends up holding a large amount of cash. In that form, the cash is hard to use. It can't be wired abroad or used to buy property, and it can't sit in a bank account without someone asking where it came from. So the group launders it. It deposits the cash in small amounts, mixes it into the income of a business that normally handles a lot of cash (a restaurant or a car wash, for example), then moves it through layers of accounts and shell companies (companies that exist only on paper). At the end, the money looks like ordinary business income. In short, laundering makes criminal money look like it came from a legitimate source.



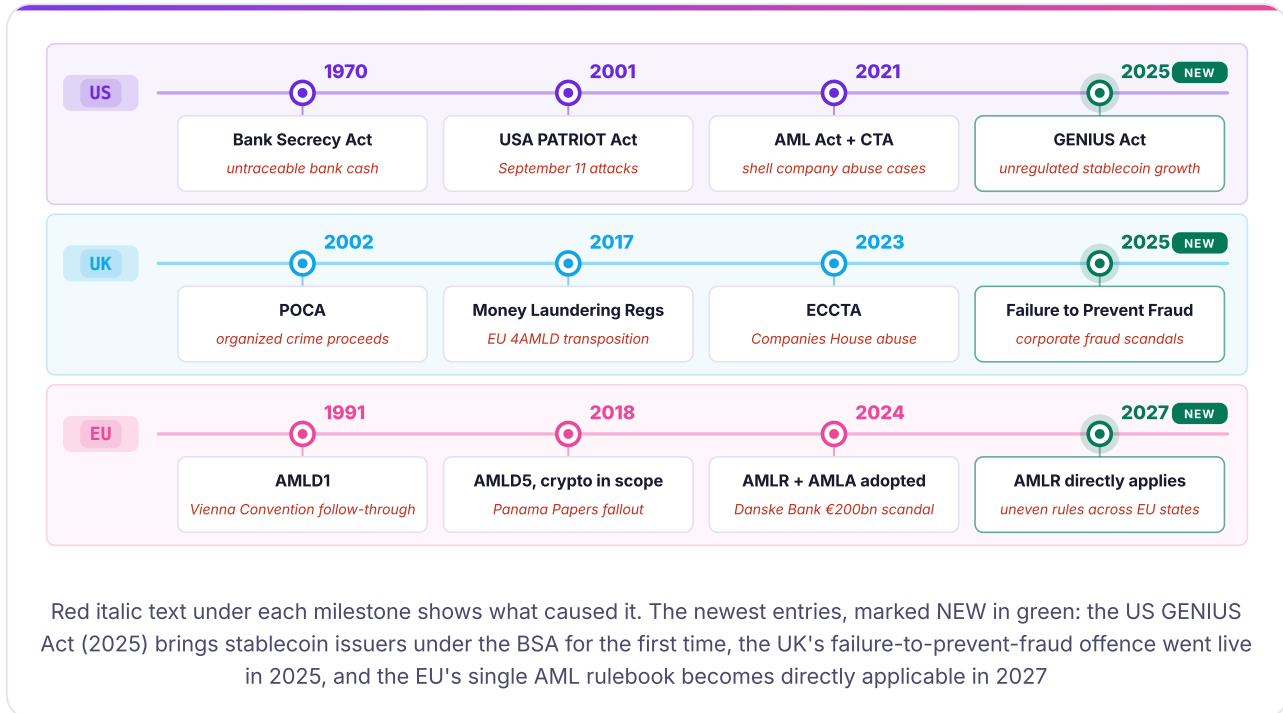
**AML (anti-money laundering)** is the whole system built to stop that process from working: laws, regulators, bank policies, KYC checks, transaction monitoring systems, SAR filings, sanctions screening, and the AML professionals in the middle of it all deciding which activity has a legitimate explanation and which doesn't. AML doesn't catch criminals directly. That's law enforcement's job. AML makes it hard to launder money through the financial system, and gives investigators a record they can follow when someone tries anyway.

One more point before the modules start, because almost every module has a "red flags" box. A **red flag** is simply a sign that activity doesn't fit the pattern you'd expect. It is not proof of a crime. From an **investigation point of view**, a red flag is where a closer review starts, not where guilt is decided: a customer suddenly wiring large sums to a country they've never dealt with is worth a look, not evidence of guilt. From an **everyday point of view**, the same idea applies in daily life: a stranger asking to route a big payment through your personal account, or a job offer that pays you to move money for someone else. Those are reasons to ask more questions, not reasons to panic or blame someone. Every red flags box in this handbook works the same way: a list of what should make you look closer, not a checklist for declaring someone guilty.



## A brief history of AML

AML law is newer than it seems: the first major law, the US Bank Secrecy Act, dates from 1970, and the rules are still being written today. The timeline shows three regulatory histories side by side: the US, the UK, and the EU.



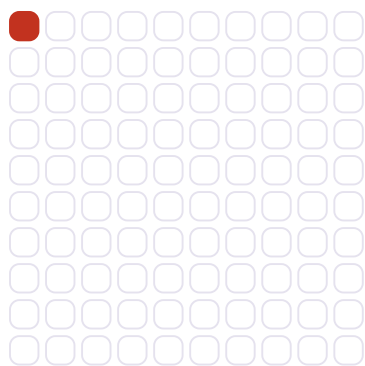
Notice the pattern: almost every major milestone in that timeline came after a scandal or a crisis, not from a policy decision planned in advance. The Bank Secrecy Act followed worries about untraceable cash moving through banks. The PATRIOT Act followed the September 11 terrorist attacks. Even the newest entries fit: the GENIUS Act followed years of unregulated stablecoin growth, and ECCTA's fraud offence followed a series of corporate scandals that regulators felt existing law could not deal with. In this field, regulation usually reacts to events. That is why keeping up with real cases and enforcement actions matters as much as knowing the rules.

## How big the problem actually is

The UN Office on Drugs and Crime has long estimated that somewhere between 2% and 5% of global GDP gets laundered every year. The range is wide because laundering is designed to stay hidden, so nobody can measure it precisely. What can be measured is what institutions report. FinCEN receives millions of SARs every year, and in September 2026 it tied nearly \$13 billion in suspected activity, drawn from more than 33,000 filings, to overseas scam centers alone.

Now a worrying number. Europol has estimated that only around 1% of criminal proceeds in the EU ever get confiscated. That gap is why AML matters. The system doesn't need to catch everything. It needs to make laundering costly, slow, and risky enough that criminals cannot

use the financial system freely.



~1%

**of criminal proceeds in the EU  
ever gets confiscated**

Europol estimate. Each square is 1% of criminal proceeds; only one is ever confiscated.

#### Q LATEST DEVELOPMENTS

- FATF's June 2026 plenary added Iraq and Bosnia and Herzegovina to the grey list and removed Algeria and Namibia, leaving 22 jurisdictions under increased monitoring. The blacklist is unchanged: North Korea, Iran, and Myanmar.
- FinCEN's September 2026 alert on overseas scam centers flagged nearly \$13 billion in suspected activity linked to pig butchering and romance-baiting fraud (scams where criminals build trust over time, then take the victim's money).
- FinCEN's October 1, 2026 alert on Russia's A7 network shows sanctions evasion using trade middlemen in other countries and a stablecoin linked to the ruble.
- The EU's single AML rulebook (AMLR) applies directly from 10 July 2027, and AMLA begins direct supervision of selected high-risk firms in 2028.

## CONTENTS

# The trail ahead

## PART I Foundations & Global Architecture

|                            |    |                               |    |
|----------------------------|----|-------------------------------|----|
| 01 AML Foundations         | 7  | 02 Money Laundering Lifecycle | 8  |
| 03 Global AML Architecture | 9  | 04 FATF & Risk-Based Thinking | 12 |
| 05 US BSA / AML Framework  | 14 | 06 EU AML Framework           | 16 |

## PART II Program, Intelligence & Sanctions

|                                   |    |                                 |    |
|-----------------------------------|----|---------------------------------|----|
| 07 The AML Program & Five Pillars | 17 | 08 Financial Intelligence Units | 18 |
| 09 Sanctions Compliance           | 20 |                                 |    |

## PART III Know Your Customer

|                         |    |                         |    |
|-------------------------|----|-------------------------|----|
| 10 KYC, CIP, CDD & EDD  | 21 | 11 Beneficial Ownership | 25 |
| 12 Customer Risk Rating | 26 | 13 High-Risk Customers  | 28 |

PART IV Products, Monitoring & Casework

|                                   |    |                                      |    |
|-----------------------------------|----|--------------------------------------|----|
| 14 Business Entities & Structures | 29 | 15 Accounts, Products & Transactions | 30 |
| 16 Transaction Monitoring         | 31 | 17 Alert Investigation               | 32 |
| 18 SAR & Narrative Writing        | 33 |                                      |    |

PART V Fintech & Crypto

|                               |    |                                    |    |
|-------------------------------|----|------------------------------------|----|
| 19 Fintech & Digital Payments | 34 | 20 Cryptocurrency & Virtual Assets | 35 |
|-------------------------------|----|------------------------------------|----|

PART VI Typologies & Predicate Crime

|                                        |    |                             |    |
|----------------------------------------|----|-----------------------------|----|
| 21 Common ML Typologies                | 37 | 22 Corruption & Trafficking | 41 |
| 23 Terrorist & Proliferation Financing | 42 | 24 Fraud & Financial Crime  | 44 |

PART VII Technology & Career

|                              |    |                       |    |
|------------------------------|----|-----------------------|----|
| 25 AML Technology, Data & AI | 45 | 26 Career Development | 46 |
|------------------------------|----|-----------------------|----|

PART I

# Foundations & Global Architecture

Why AML exists, how dirty money actually moves through the system, and how every country builds on the same FATF standards but adds its own rules on top.

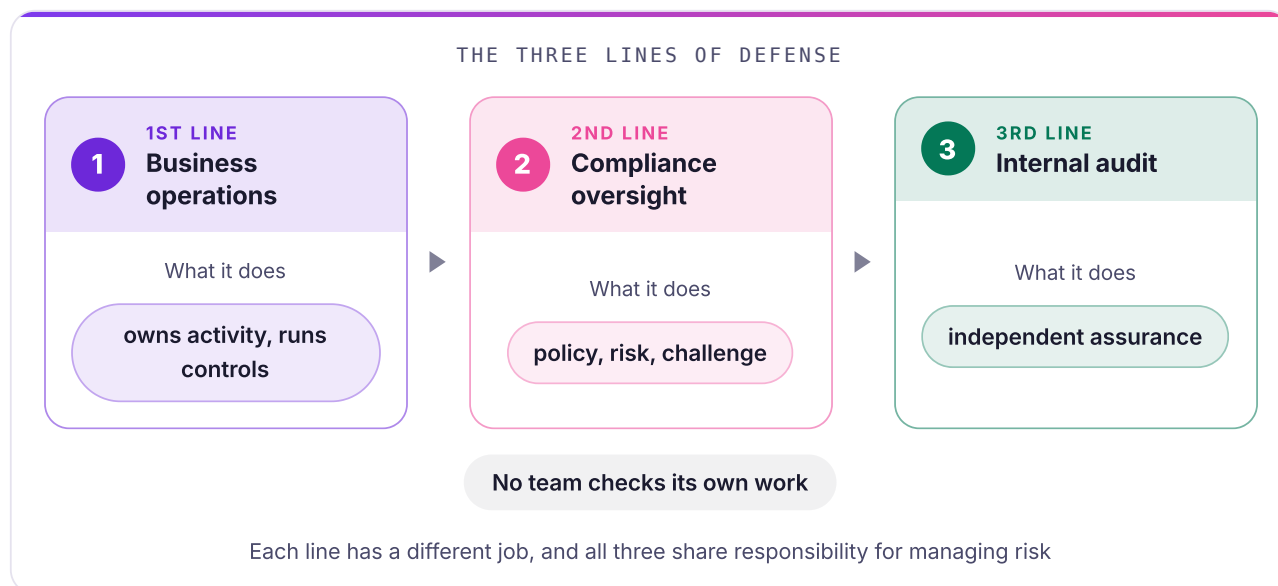
01 AML Foundations

Why does AML exist? Criminals need their money to look legal before they can spend it, invest it, or move it freely, and the financial system is where that usually happens. Many newcomers think an AML professional's job is to prove a crime happened. It is not. The job is to notice when activity does not match what is expected from a customer, and to keep clear records that still make sense when a senior person reads them later. Everything else in this handbook (KYC, monitoring, SARs) supports that one job: turning a suspicion into a written decision that can be explained and defended.

RED FLAGS

- Activity that clearly does not match the reason the customer gave for the account
- A sudden behavioral shift with no documented business or personal reason
- Multiple parties, accounts, or products all linked to the same flow of money
- Missing information that makes it hard to understand where the money came from or where it is going

Most institutions split the work into three lines of defense, so no team checks its own work:



## 02 Money Laundering Lifecycle

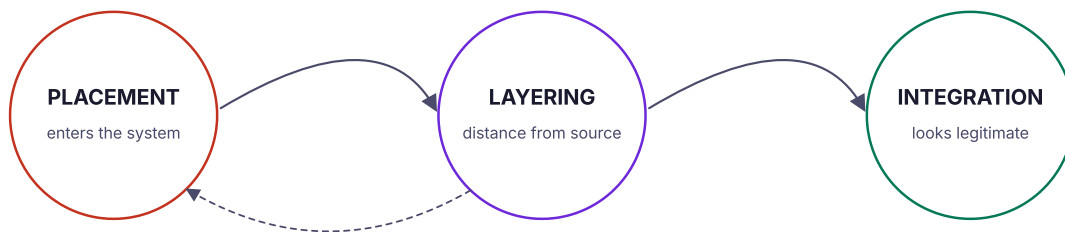
Every laundering scheme, simple or complex, has three stages. Put simply: get the money into the system, move it far from its source, then bring it back so it looks legal.

**Placement** is the moment dirty money first enters the financial system. Before placement, it is just cash or an asset that no bank can see. This is the criminal's problem: large amounts of cash cannot be wired, invested, or spent without people asking questions. Common example: someone deposits cash from drug sales in small amounts and pretends it is the daily income of a cash-heavy business they own, like a car wash or a restaurant.

**Layering** comes next: moving that money through a chain of transactions designed to hide where it really came from. Each transfer makes the source harder to trace. Common example: the deposited cash is wired to an account in another country, split across several shell companies (companies that exist only on paper), then changed into a different currency. Each step makes the paper trail longer and messier.

**Integration** is the last stage: the money, now far from its source, comes back into the legal economy as what looks like normal income or assets. Common example: the layered funds buy an apartment, a piece of art, or shares in a business. On paper, it looks like a normal purchase that is easy to explain.

Training teaches this as three steps that happen in order. Real cases often do not follow that order. Money can be placed and layered in the same transaction. Integration can start before layering is done. Use the model to ask which stage you are looking at right now, not as a checklist to follow in order.



#### 🚩 RED FLAGS

- Cash or crypto entering the system in amounts just under reporting thresholds
- Funds moved through multiple unrelated accounts with no clear business reason
- Rapid conversion between asset types, currencies, or products
- Money that ends up in what looks like normal spending, but comes from funds with an unclear source

## 03 Global AML Architecture

Every country builds its AML rules on the same FATF standards, but each one adds its own laws, regulators, and reporting requirements. Plenty of AML professionals, especially at outsourced compliance and managed-service firms, work on cases from several countries in a single shift. They must switch between rule sets without mixing up what each regulator expects. Below is the current picture, as of 2026.

### | Regulators worth knowing

First, two terms to understand. A **regulator** is the government body with legal power to supervise financial institutions, set the rules, and penalize anyone who breaks them. An **FIU (Financial Intelligence Unit)** is the government body that receives the reports institutions file (SARs, STRs, CTRs), analyzes them, and passes useful leads to law enforcement. Some countries put both jobs in one agency; others split them. Here are the ones you will see most often on international cases.

#### UNITED STATES

##### FinCEN

Part of the US Treasury. It runs the Bank Secrecy Act and sets the standards that examiners at other agencies (OCC, FDIC, Fed) use when they check banks. Its rules affect AML programs far beyond the US, because a large share of global business uses US banks and the US dollar.

[fincen.gov](https://fincen.gov) ↗

#### UNITED KINGDOM

##### FCA & NCA

The FCA supervises financial firms under the Money Laundering Regulations. The National Crime Agency runs the UK's FIU and receives SARs through its UKFIU function. These are two agencies with two different jobs, and both appear often on UK cases.

[fca.org.uk](https://fca.org.uk) ↗ · [nationalcrimeagency.gov.uk](https://nationalcrimeagency.gov.uk) ↗

#### EUROPEAN UNION

##### AMLA

The EU's new central AML authority, operational since mid-2025, headquartered in Frankfurt. From 2028 it will directly supervise about 40 of the highest-risk financial groups that work across borders. National regulators will still supervise everyone else, under a new shared rulebook.

[amla.europa.eu](https://amla.europa.eu) ↗

#### AUSTRALIA

##### AUSTRAC

Australia's combined regulator and FIU. Its reach recently grew. From 1 July 2026, lawyers, accountants, real estate agents, and trust and company service providers came under its AML/CTF rules for the first time. Crypto rules, which since 2018 covered only crypto-to-cash exchanges, now also cover custody (holding crypto for others), crypto-to-crypto exchange, and transfers.

[austrac.gov.au](https://austrac.gov.au) ↗

#### CANADA

##### FINTRAC

Canada's FIU, administering the PCMLTFA. It has a detailed set of required reports: large cash transaction reports, electronic funds transfer reports, and casino-specific duties that have no direct match in most other countries' rules.

[fintrac-canafe.canada.ca](https://fintrac-canafe.canada.ca) ↗

#### SINGAPORE

##### MAS & STRO

The Monetary Authority of Singapore regulates financial institutions directly; the Suspicious Transaction Reporting Office, under the Singapore Police Force, is the FIU. Other countries in Asia watch Singapore's rules closely, because it is a major financial center for the region.

[mas.gov.sg](https://mas.gov.sg) ↗ · [STRO](#) ↗

#### INDIA

##### FIU-IND

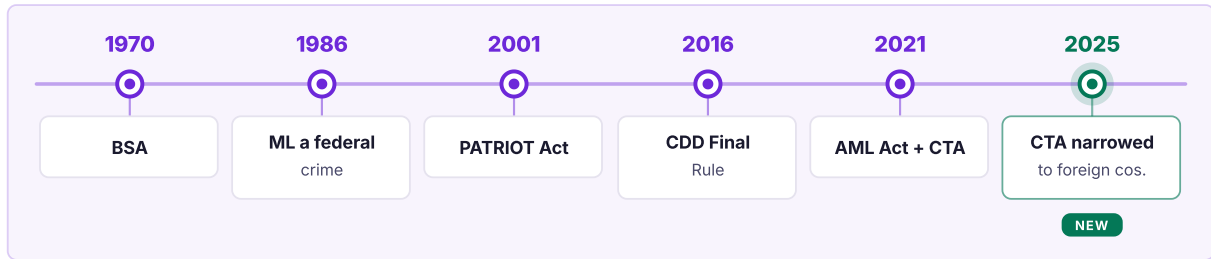
India's financial intelligence unit, part of the Department of Revenue. It receives STRs, CTRs, and NTRs (non-profit organisation transaction reports) from a growing list of reporting firms, which now clearly includes VDA (crypto) service providers.

[fiuindia.gov.in](https://fiuindia.gov.in) ↗

## | How the rules got here, and where they're headed

Three regions, each shaped by different pressures, are moving toward the same goal: rules that are risk-based, in proportion to the risk, and harder to get around.

### UNITED STATES



2025: FinCEN exempted all US-formed companies from beneficial ownership reporting. Only foreign companies registered to do business in the US still have to file.

### UNITED KINGDOM



September 2025: large organizations can now be criminally liable if they fail to prevent fraud committed for their benefit, a new type of crime for companies

### EUROPEAN UNION



The AMLR (Regulation 2024/1624) becomes one directly applicable rulebook across all 27 member states from 10 July 2027, replacing the mix of different national versions of the rules

## | The biggest AML fines in history

Learn these cases. They show how much weak controls can cost a large firm.

| # | Institution        | Fine                                                                                                       | What happened                                                                                                                                            |
|---|--------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | BNP Paribas        | <b>\$8.9B</b> (2014)<br>  | Processed transactions for Sudan, Iran, and Cuba in violation of US sanctions, still the largest AML/sanctions fine ever issued                          |
| 2 | Binance            | <b>\$4.3B</b> (2023)<br>  | BSA and sanctions violations, the largest penalty in crypto history                                                                                      |
| 3 | TD Bank            | <b>\$3.0B</b> (2024)<br>  | Let money laundering networks move over \$670M through its accounts, the largest bank in US history to plead guilty to Bank Secrecy Act program failures |
| 4 | Danske Bank        | <b>\$2.0B</b> (2022)<br>  | Roughly €200B in suspicious flows through its Estonian branch                                                                                            |
| 5 | HSBC               | <b>\$1.9B</b> (2012)<br>  | Allowed Mexican and Colombian cartel funds through its US operations                                                                                     |
| 6 | Standard Chartered | <b>\$1.1B</b> (2019)<br> | Sanctions violations involving Iran and other countries, plus AML failures, settled with US and UK authorities                                           |

### 🔍 TRUE STORY

HSBC's case is often used to explain why banks became so careful about correspondent banking (one bank providing accounts and services to another bank) afterward, and why many turned to "de-risking": cutting off whole categories of higher-risk customers instead of assessing them one by one. Study the details, not just the headline: weak CDD on correspondent relationships is what let cartel money flow through for years.

### 🚩 RED FLAGS

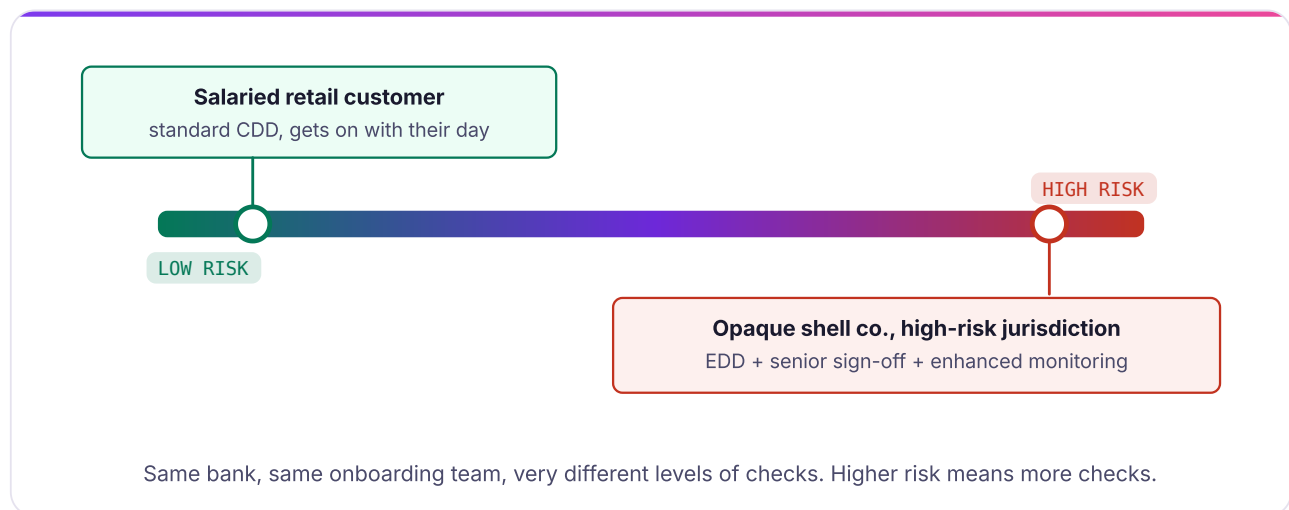
- Cross-border activity touching a jurisdiction with weak AML supervision
- Structuring (splitting money into smaller amounts) that seems planned around one country's reporting threshold
- A customer's documented home country that doesn't match where their transactions actually happen

## 04 FATF & Risk-Based Thinking

The **FATF (Financial Action Task Force)** is a group of governments, founded by the G7 in 1989. It writes the global standards that almost every country's AML law is based on. FATF does not enforce rules directly. It sets the 40 Recommendations that national

regulators build their laws around. It then runs mutual evaluations, which are reviews that publicly grade how well each country actually applies them.

The most important of those 40 is **Recommendation 1**. It requires countries and institutions to identify, assess, and understand their own money laundering and terrorist financing risks, then use their resources in proportion: more checks where risk is higher, fewer checks where it is lower. That's the **risk-based approach (RBA)**, and it is the main idea behind almost everything else in this field. For example: a retail customer with a salaried job and regular spending gets standard CDD and no extra checks. A shell company registered in a high-risk country, with no clear business purpose and unclear ownership, gets EDD, senior approval, and ongoing enhanced monitoring. Same bank, same onboarding team, very different levels of checks. Why? Because the same checks for everyone waste effort on low-risk customers and do not protect enough against high-risk ones.



FATF doesn't work alone. The [Egmont Group](#) connects FIUs so they can share information across borders. The [Wolfsberg Group](#), a coalition of major global banks, publishes practical guidance that often affects bank policy sooner than formal rules do. The [Basel Committee](#) and [IOSCO](#) publish guidance for banking supervisors and securities regulators. None of them make law on their own. Still, a strong AML professional knows their names, because much of what the industry calls "best practice" comes from their guidance.

#### 🚩 RED FLAGS

- The same control used for every customer no matter the risk, usually a sign of a weak program
- Beneficial ownership information that's incomplete, inconsistent, or unverified
- A VASP (crypto service provider) or fintech taking on customers without controls that match its own level of risk

The **Bank Secrecy Act (BSA)**, passed in 1970, is the starting point of AML law in the US. It requires banks and other financial institutions keep certain records and file certain reports, so the government has records to follow when money moves in ways that suggest crime. Almost everything else in this module is part of what the BSA requires in practice:

**CTR (Currency Transaction Report):** filed automatically when a customer's cash transactions in the same direction total more than \$10,000 in a single business day. Same direction means all deposits, or all withdrawals, never a mix of the two. A \$5,000 cash deposit and a \$6,000 cash withdrawal on the same day don't trigger a CTR. Two \$6,000 cash deposits on the same day do, and so do two \$6,000 cash withdrawals. No suspicion is needed. The rule applies automatically every time.

**SAR (Suspicious Activity Report):** filed when an institution suspects activity may involve a crime and can't find a reasonable explanation for it. Unlike a CTR, a SAR takes judgment: a person has to decide that the activity does not make sense. Filing becomes mandatory at these US thresholds, and institutions can always file voluntarily below them:

| Situation                                                                                                         | Mandatory SAR threshold |
|-------------------------------------------------------------------------------------------------------------------|-------------------------|
| Bank: suspected crime where a suspect can be identified                                                           | \$5,000 or more         |
| Bank: suspected money laundering, terrorist financing, or an attempt to evade BSA reporting (such as structuring) | \$5,000 or more         |
| Bank: suspected crime where no suspect can be identified                                                          | \$25,000 or more        |
| Bank: suspected insider abuse (an employee or director involved)                                                  | Any amount              |
| Money services business (MSB)                                                                                     | \$2,000 or more         |

### CTR automatic

**Trigger:** over \$10,000 cash in a day  
all deposits or all withdrawals, never mixed

**Judgment:** none, it's automatic

**Suspicion:** not required

### SAR a judgment call

**Trigger:** activity that doesn't add up

**Judgment:** yes, a human decides

**Amount:** \$2,000 to \$25,000, by case

**CIP (Customer Identification Program):** the steps a bank takes to actually verify who a customer is before opening an account, like checking a government ID against the name on file.

The **USA PATRIOT Act**, signed weeks after September 11, 2001, is one of the biggest expansions in the BSA's history. It did not replace the BSA. It added counter-terrorism duties to it: CIP became a formal legal requirement for the first time (Section 326), banks and the government got a dedicated legal channel for sharing information (Section 314, explained in the next paragraph), Section 312 required enhanced due diligence on foreign correspondent and private banking accounts, and Section 313 fully banned correspondent accounts for foreign shell banks (banks with no physical office anywhere). Much of what is now standard KYC traces back to this Act.

**314(a) and 314(b)**: two information-sharing channels created by the PATRIOT Act.

314(a) lets law enforcement ask banks whether they hold any accounts tied to a name under investigation. 314(b) lets banks voluntarily share information with each other about a customer they both suspect, without that sharing counting as a privacy violation.

**FinCEN**, the US Treasury bureau that administers the BSA, oversees all of it. It issues guidance and updates what examiners expect each year. So read its advisories directly, and do not rely on training slides that may be a year or two old.

FinCEN writes the rules, but it doesn't examine most institutions itself. That job belongs to each institution's primary regulator: the **OCC** for national banks, the **Federal Reserve** for state member banks, the **FDIC** for state non-member banks, the **NCUA** for credit unions, the **SEC and FINRA** for broker-dealers, and the **IRS** for money services businesses and casinos. That is why one enforcement case often comes from several agencies at once, as it did with TD Bank in 2024.

#### Q WHAT THE AML ACT OF 2020 CHANGED

- Created the Corporate Transparency Act and its beneficial ownership reporting regime
- Expanded whistleblower awards to between 10% and 30% of sanctions collected in large BSA cases
- Added "value that substitutes for currency" to the BSA, which clearly brings crypto under the law
- Brought antiquities dealers into the regime
- Required FinCEN to publish national AML/CFT priorities, which it first issued in June 2021
- Increased penalties for repeat violators
- Allowed individuals found to have committed egregious (very serious) BSA violations to be barred from serving on the board of a US financial institution for 10 years

The Act is named for 2020 but became law on 1 January 2021, which is why the timelines show it under 2021.

BSA failures are not only a company problem. Individuals can be punished too. In 2017, MoneyGram's former chief compliance officer, Thomas Haider, agreed to pay \$250,000 and accept a three-year industry ban to settle FinCEN's case against him for failing to stop fraud flowing through MoneyGram agents. In 2024, Binance founder Changpeng Zhao was sentenced to four months in prison after pleading guilty to failing to maintain an effective AML program. If you are aiming for a senior compliance role, remember this: you can be held personally responsible for the program you approve. The UK takes the

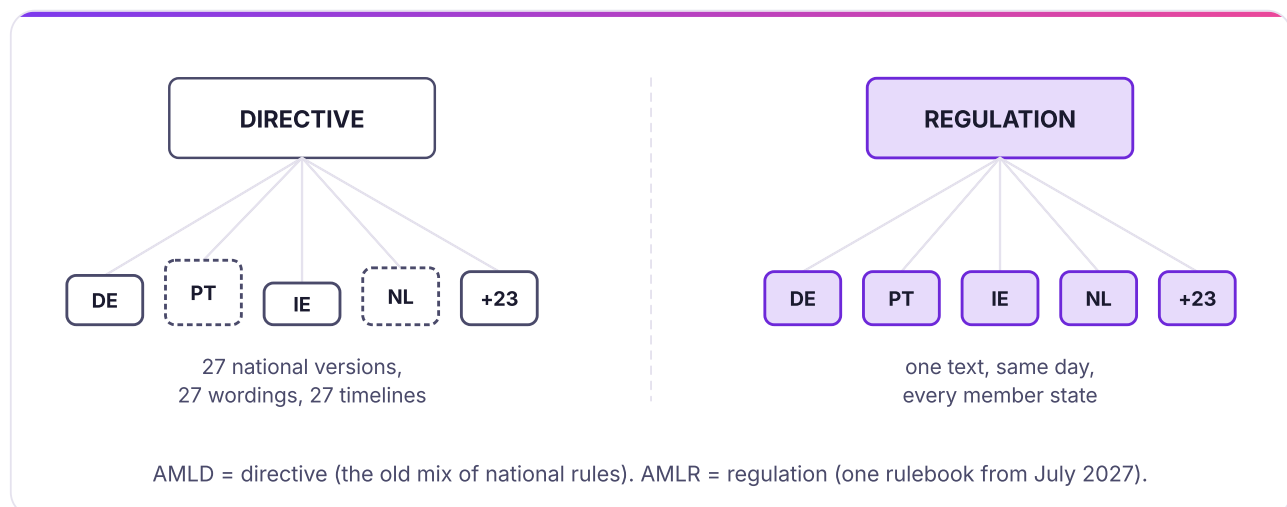
same view: under the Senior Managers and Certification Regime, the MLRO holds a named senior management function (SMF17) and can be held personally accountable by the FCA for failures in their area.

#### 🚩 RED FLAGS

- Transactions structured to stay just under the \$10,000 CTR threshold
- A SAR narrative that gives a conclusion without the timeline of events that supports it
- CIP information that was collected but never actually verified

## 06 EU AML Framework

One difference explains this whole module. A **directive** sets a goal that each EU country then writes into its own national law, in its own words, on its own timeline. This is why the same EU rule can be enforced differently in Germany and in Portugal. A **regulation** becomes law automatically in every member state on the same day. No national rewriting required.



The EU's AML rules began as a series of **AMLDs (Anti-Money Laundering Directives)**. AMLD5 brought crypto exchanges into scope; AMLD6 made the definition of predicate crimes (the crimes that produce the dirty money) the same across the EU. Because these were directives, enforcement still varied country to country. That is now changing. The **AMLR (Anti-Money Laundering Regulation)** is a regulation, not a directive: one directly applicable rulebook across all 27 member states, no national rewrite needed. Alongside it sits **AMLA**, the EU's new central AML authority, which started operating in 2025 and takes on direct supervision of the riskiest cross-border firms from 2028. This ends the mix of national rules that let companies choose the country with the weakest enforcement.

So what changes in daily work when AMLR applies in July 2027? Here are a few examples. Cash payments above **€10,000** for goods or services become prohibited across the EU, and member states can set a lower cap. The beneficial ownership threshold stays at **25%**, but the rules for finding owners behind complex ownership chains become much more detailed and strict. Crypto-asset service providers follow the

same rulebook as banks. And because it's a regulation, a compliance team operating across Germany, Ireland, and the Netherlands works to one text instead of three national versions.

#### Q WHY THE EU CENTRALIZED

Danske Bank's Estonian branch processed roughly €200 billion of suspicious, largely non-resident flows between 2007 and 2015. Danish supervisors watched the parent bank. Estonian supervisors watched the branch. Neither saw the whole picture. AMLA is built to fix this gap: one authority that can look at a cross-border group as a whole.

#### 🚩 RED FLAGS

- A corporate structure routed through a member state known for lighter beneficial-ownership enforcement
- A customer relationship that moves to another EU country right after controls get stricter in a different one

## PART II

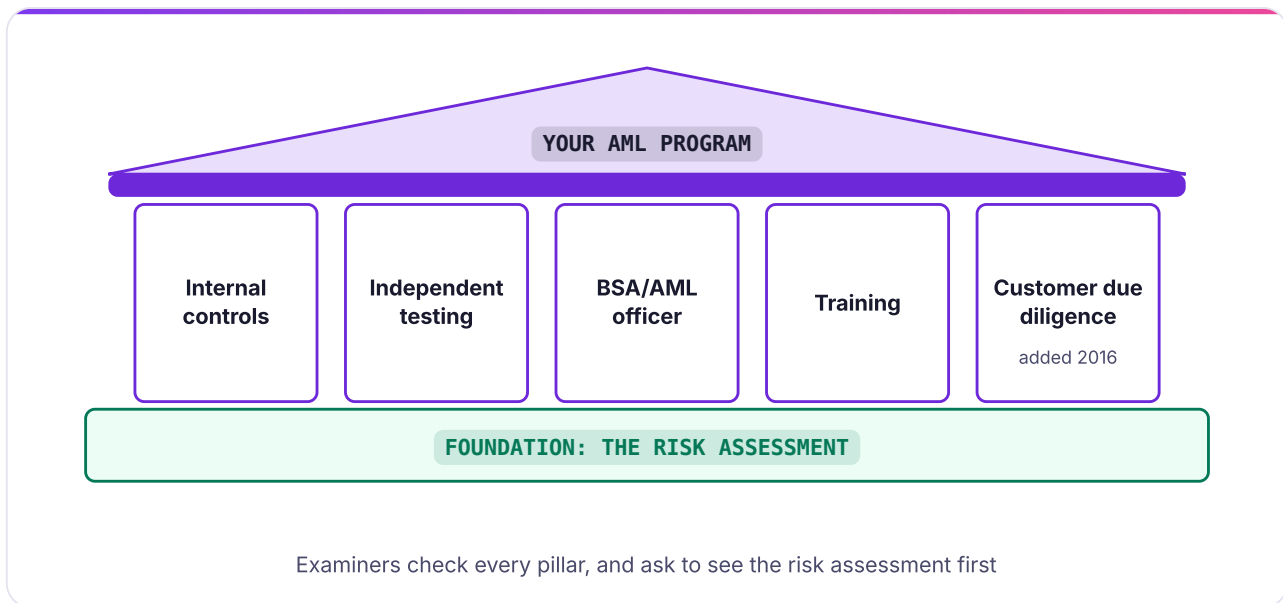
# Program, Intelligence & Sanctions

How a compliance program is built to pass a regulator's exam, where your report goes after you file it, and why sanctions screening is a separate job from AML, even though the two work closely together.

## 07 The AML Program & Five Pillars

An **AML program** is the actual set of policies, people, and processes an institution runs every day to detect and prevent money laundering: onboarding checks, alert queues, even the training new hires sit through. In the US, every program stands on five specific pillars, and examiners check all five, not just whether the institution is "doing AML" in general:

**Internal controls:** the policies, procedures, and systems (like transaction monitoring rules) that manage the institution's risk. **Independent testing:** a separate team, not the one that built the controls, checking whether those controls genuinely work. **A designated BSA/AML compliance officer:** one named person accountable for the program. **Training:** making sure staff actually know how to spot and escalate what the controls are built to catch. And **customer due diligence**, added as the fifth pillar by FinCEN's 2016 CDD Rule, covering beneficial ownership and ongoing monitoring of customer relationships.



Underneath all five sits the **risk assessment**: a documented analysis of where the institution's money laundering risk actually lives, by product, customer type, and geography. It isn't one of the five named pillars, but every pillar is set up based on it, and examiners will ask to see it first.

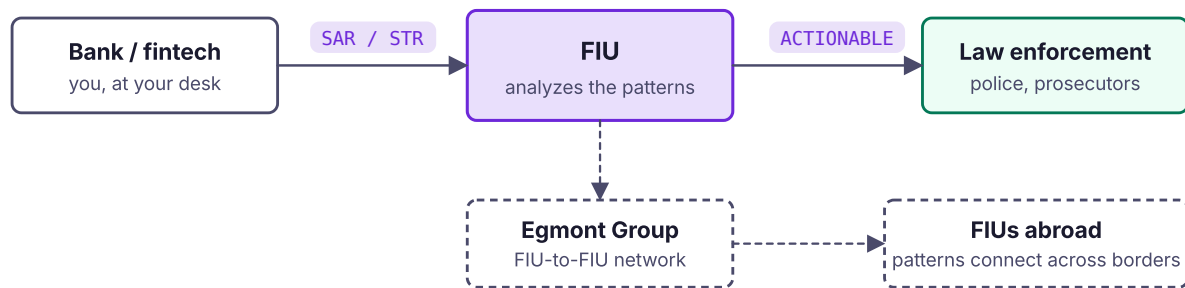
If one pillar is missing, the whole program gets flagged in an exam. A bank can have strong monitoring rules and still fail if no one independently tests whether those rules work in real life.

#### 🚩 RED FLAGS

- A risk assessment that hasn't been updated after a big change in products or customers
- Independent testing performed by the same team that built the controls
- Training that's generic rather than role-specific

## 08 Financial Intelligence Units & Reporting

A **Financial Intelligence Unit (FIU)** is the government body sitting between banks and law enforcement. It receives the SARs, STRs, and CTRs institutions file, analyzes them for patterns, and passes anything actionable to police or prosecutors. FinCEN in the US and FIU-IND in India are both FIUs. Each is the national body that receives the reports this handbook describes.



Your report's journey. Specific facts get matched to other reports and acted on; generic boilerplate gives investigators nothing to use.

An FIU can only work with the reports it receives. Many vague SARs full of generic, copy-paste text (boilerplate) do not help an investigator, even if each one technically meets the filing rules. FIUs also run public-private information sharing and cooperate across borders through networks like the Egmont Group. This is how a pattern found in one country can be linked to a case in another.

Each major jurisdiction handles reporting a little differently, and these differences matter in daily work. In the US, a SAR goes to FinCEN through the BSA E-Filing System. In the UK, it goes to the UK Financial Intelligence Unit inside the NCA, and the UK adds something most regimes don't have: the **Defence Against Money Laundering (DAML)** request. If a UK firm suspects funds are criminal property but needs to process a transaction, it can ask the NCA for consent first. The NCA has seven working days to respond, and silence counts as consent. In India, reporting entities file STRs to FIU-IND through its FINnet portal.

Plenty of FIUs don't build their own systems at all. They use **goAML**, reporting software developed by the UN Office on Drugs and Crime and adopted by dozens of FIUs, including the UAE's. That's why the same structured report format appears in very different jurisdictions.

#### Q HOW FIUs ACTUALLY USE YOUR REPORT

FinCEN's alerts now include a specific "key term" to enter in SAR field 2 and the narrative. Its October 1, 2026 alert on Russia's A7 sanctions-evasion network asks filers to use **FIN-2026-A7NETWORK**. It looks like a small admin detail, but it is how one SAR from one bank gets matched to thousands of others about the same network. If the key term is missing, even a well-written SAR can be left out of the pattern analysis.

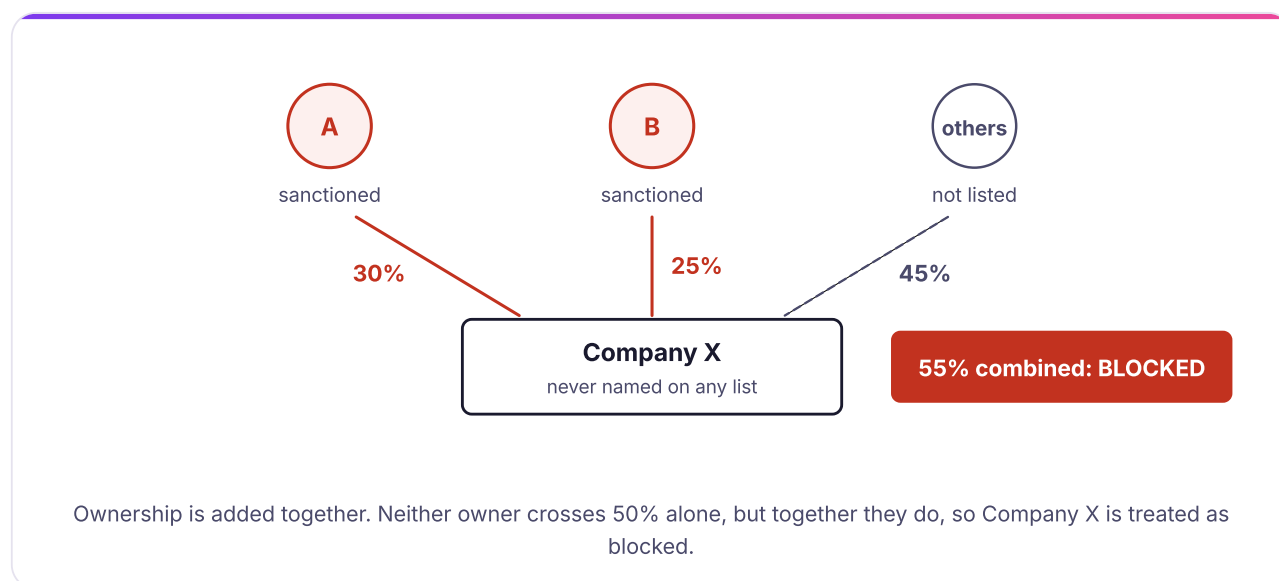
#### F RED FLAGS

- An STR or SAR narrative with no specific dates, amounts, or counterparties
- A case closed with no explanation for why it was ruled out
- A typology pattern that matches a recent FIU advisory but wasn't cross-referenced against it

## 09 Sanctions Compliance

A **sanction** is a government-imposed restriction on dealing with a specific person, company, or country. A simple example is an asset freeze on a named individual. Any institution holding their funds must freeze the account and cannot process any transactions for them.

Sanctions and AML are related, but they are not the same job. A sanctions hit isn't about whether something looks suspicious. It's about whether it's specifically prohibited. If you mix these up, you either miss a true match or create too many false positives (alerts that are not real matches) for the screening team. Ownership and control rules, like OFAC's 50 percent rule, matter more than new AML professionals often expect: a company might not appear on any list, but if one or more sanctioned persons own 50% or more of it, individually or in aggregate, it's treated as sanctioned too. Say a sanctioned individual owns 60% of Company X. Company X was never named on any list, but under the 50% rule it's blocked property anyway. If you screen only the company's name and never check who owns it, you miss the match completely.



Screening splits into two related jobs. **Name screening** checks who's involved (a customer, a counterparty, a beneficial owner) against sanctions lists and watchlists. **Payment screening** checks the transaction message itself, often a SWIFT message, for any sanctioned party appearing anywhere in the payment chain. They catch different things. A customer can pass name screening at onboarding and still trigger a payment screening hit years later, because a sanctioned party appears in one field of a wire. There is also transliteration, which means writing a name in a different alphabet. A name in Arabic, Cyrillic, or Chinese script can be spelled in English letters in several ways, and screening logic has to allow for that or it will not catch the match.

The lists themselves (save these links): OFAC's SDN search (US), the UK OFSI consolidated list, the [EU consolidated list](#), and the [UN Security Council consolidated list](#). Many institutions do not screen against them by hand. Instead, they pay for combined screening data from providers like [Dow Jones Risk & Compliance](#) or [LSEG World-Check](#), which combine sanctions, PEP, and adverse media data in one feed.

#### 🚩 RED FLAGS

- A name match with high fuzzy-logic similarity (the names are close but not identical) but a different date of birth or nationality. This is usually a false positive, but always confirm it rather than assume
- A company structure where the ownership percentages don't clearly show who owns it
- A transaction routed through an intermediary jurisdiction to avoid a direct screening hit
- Payment messages with fields removed or changed, known as stripping. This is a deliberate way to avoid screening: details that identify the sender (originator) or receiver (beneficiary) are deleted or edited so automated screening has nothing to match against

### PART III

## Know Your Customer

KYC is how an institution knows who it is dealing with. It has three layers, CIP, CDD, and EDD, that new AML professionals often mix up. They are not the same thing, and confusing them is a common cause of errors early in a career.

#### 10 KYC, CIP, CDD & EDD

### | What is KYC?

**KYC (Know Your Customer)** is the general term for everything an institution does to understand who it's dealing with, before the relationship starts and for as long as it lasts. It isn't one check. It is three layers built on top of each other, and the depth of each one grows with risk. Regulators don't expect every customer to get identical treatment. They expect the effort to match the risk, and the reasoning to be written down.

#### Q THE THREE LAYERS OF KYC

- **CIP:** who is this? Identity verification at onboarding.
- **CDD:** what should we expect from them? Purpose, expected activity, and source of funds (SoF), kept up to date.
- **EDD:** what extra do we need because they're higher risk? Deeper checks, senior approval, closer monitoring.

For businesses rather than individuals, the same process is often called **KYB (Know Your Business)**, and it adds the beneficial ownership work covered in Module 11 (p. 25).

## | CIP: Customer Identification Program

**CIP** verifies identity and answers one question: is this person who they say they are? In the US, the CIP rule requires a bank to collect at least four data points before opening an account: **name, date of birth, residential address, and an identification number** (a Social Security number for US persons, or a passport or other government ID number for non-US persons). The bank then verifies those details, either *documentary* (checking a passport or driving licence) or *non-documentary* (matching against credit bureau or public records data), and checks the customer against government lists. Other countries describe it differently, but every country's rules have a similar first step.

## | CDD: Customer Due Diligence

**CDD** goes further and builds the customer profile that everything else depends on: why this customer wants the relationship, what activity is realistically expected, and where their money comes from. That picture becomes a **risk rating** (typically low, medium, or high) and an expected-activity baseline that transaction monitoring later measures against. For legal entities, CDD also means identifying the **beneficial owners**, the real people who own or control the business. And it is not a one-time task: the profile is kept up to date as the relationship changes.

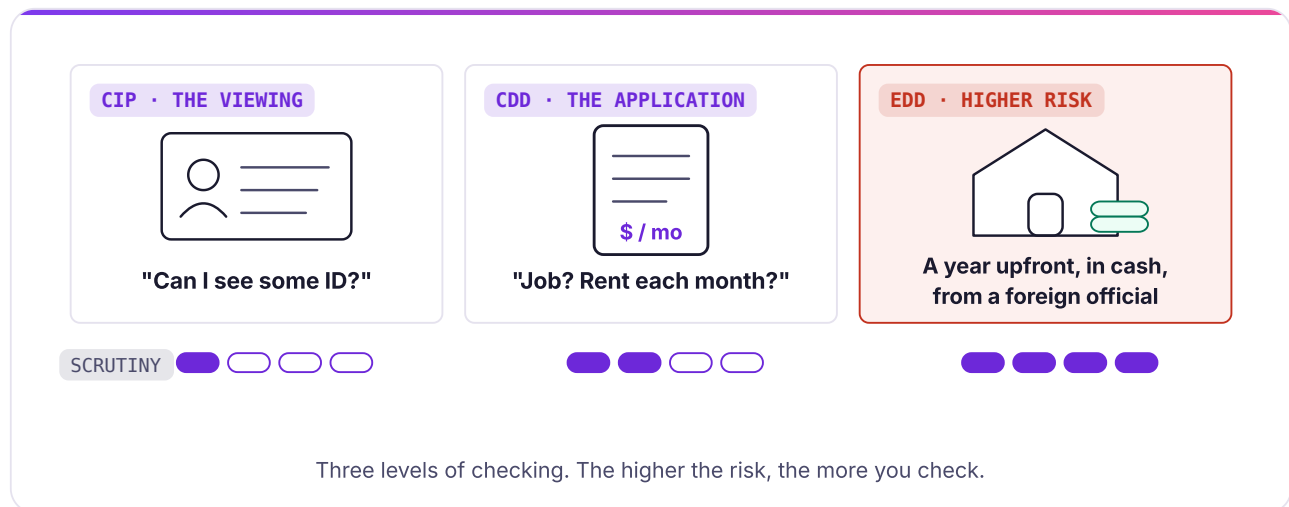
## | EDD: Enhanced Due Diligence

**EDD** is a deeper, more detailed version of CDD, applied when specific risk factors call for it. Common triggers: politically exposed persons (PEPs), customers linked to high-risk jurisdictions, correspondent banking relationships, complex or opaque ownership structures, and cash-intensive businesses. Typical EDD steps: verifying source of wealth (SoW) as well as source of funds (SoF), senior management sign-off before onboarding, adverse media screening, more frequent reviews, and tighter ongoing monitoring.

## | How the three layers fit together

A simple comparison is renting out an apartment. CIP is checking the applicant's ID at the viewing. CDD is asking what they do for a living and how they'll cover rent each month. EDD is what happens when that applicant turns out to be a foreign official

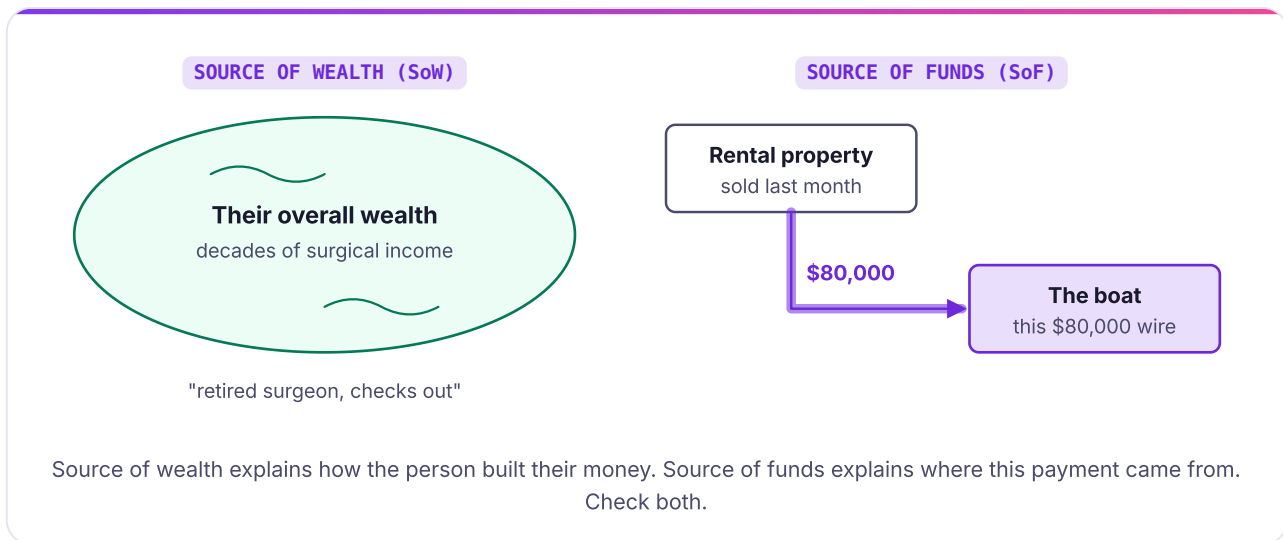
offering to pay a full year upfront, in cash. Now there is much more to verify before the landlord hands over the keys.



| Layer      | The question                                      | When it applies                        | Typical evidence                                                                              |
|------------|---------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>CIP</b> | Is this person who they say they are?             | Every customer, at onboarding          | ID document, date of birth, address, ID number, list screening                                |
| <b>CDD</b> | What should we expect from them?                  | Every customer, onboarding and ongoing | Purpose of account, occupation or business, expected activity, beneficial owners, risk rating |
| <b>EDD</b> | What extra do we need because the risk is higher? | Only when risk factors are present     | Verified source of wealth, senior approval, adverse media, more frequent reviews              |

## Concepts that trip people up

**Source of funds (SoF)** and **source of wealth (SoW)** confuse people often, even experienced AML professionals, because they sound alike but mean different things. Source of funds asks where *this specific payment* came from. Source of wealth asks how this person built their *overall net worth*. Take a retired surgeon wiring \$80,000 to buy a boat. Source of wealth is easy: decades of surgical income, backed up by tax filings or employment history. Source of funds for that particular \$80,000 might be something else entirely, like last month's sale of a rental property. If you check source of wealth ("retired surgeon, checks out") and stop there, without asking where this specific \$80,000 came from, you've done only half the job.



A current change worth knowing: **perpetual KYC**. The old model refreshed a customer's file on a fixed calendar, every one, two, or three years depending on risk tier, no matter what happened in between. Perpetual (or continuous) KYC replaces the fixed schedule with triggers, meaning specific events. An unusually large transaction, a new PEP designation, a sanctions list hit, or a change in company ownership prompts an immediate review instead of waiting for the next scheduled refresh. More and more, regulators see fixed cycles as too slow, because customer risk can change quickly. Interviewers may expect you to know the term.

Two more concepts to learn early. **Residual risk** is the risk left over after controls are applied to inherent risk (the risk before any controls). A high-risk customer with strong, verified controls can carry lower residual risk than a medium-risk customer with weak documentation, which is why the starting rating alone does not give the full picture. And **tipping off** is a legal rule, not just good manners at work: once a SAR or investigation is underway, alerting the customer that they're under review, directly or indirectly, is itself an offence in most jurisdictions. Some new AML professionals learn this through a costly mistake, such as one harmless-sounding line in an email to a customer.

Many institutions now run identity checks through a dedicated eKYC provider rather than manual document review. Names worth recognizing: [Onfido](#), [Sumsu](#), and [Trulioo](#).

#### Q TRUE STORY

In September 2026, Revolut disclosed that it had handed sensitive customer records (names, dates of birth, passport and driving licence copies, verification selfies, IBANs, and full transaction histories) to fraudsters who never breached its systems at all. Instead, the attackers got into a genuine government agency's email domain and used it to send what looked like a routine official information request. The email came from a real, authenticated government address, so Revolut treated it as legitimate and complied. Its systems weren't hacked. The failure was in verification: no one checked the real-looking request with the actual requesting officer or case reference before the sensitive KYC data was sent out. The same rule this module uses for onboarding (verify, don't just accept what looks right) applies to anyone who asks an institution to share data, including government requesters.

#### 🔍 WHAT A KYC FILE ACTUALLY CONTAINS

- **Identity:** verified ID document, date of birth, and residential address
- **Profile:** occupation or nature of business, and the purpose of the account
- **Expected activity:** typical transaction types, volumes, and countries involved
- **Source of funds**, and for higher-risk customers, **source of wealth**
- **Screening results:** sanctions, PEP, and adverse media checks, with how any matches were resolved
- **Risk rating:** the score and, just as important, the written rationale behind it
- **Review history:** every periodic or trigger-based review, what changed, and what was decided

If a reviewer opened the file for the first time, could they tell who this customer is and why the institution was comfortable taking them on? That's the test every KYC file has to pass.

#### 🚩 RED FLAGS

- Expected activity on file that looks nothing like the actual activity six months later
- A source of wealth explanation that's plausible but undocumented
- EDD triggers present in the file but never acted on
- A customer who resists providing documents, or whose stated purpose keeps changing between conversations

#### 🔍 AMLIFT TAKE

An AML professional writes "customer is a business owner" as source of wealth and stops there. That names a type of customer, but it explains nothing. Where is the business registered? What does it actually do? Does the transaction volume fit a business that size? That is the difference between just filling in a form and truly assessing someone.

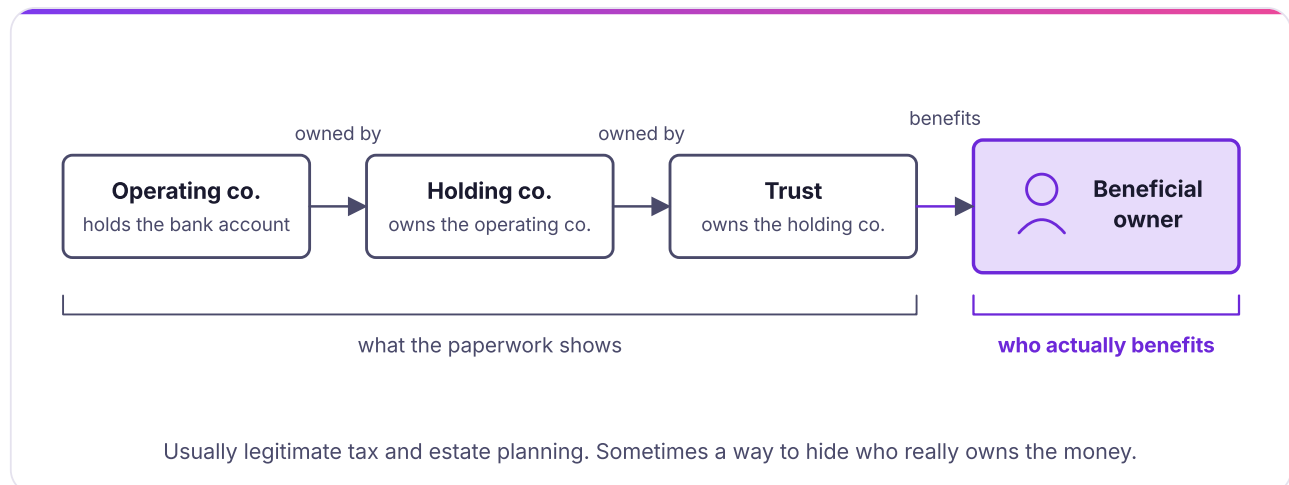
#### 🔍 IF IT COMES UP IN AN INTERVIEW

**"What's the difference between CDD and EDD?"** A strong answer: CDD applies to every customer and builds the expected-activity picture; EDD is additional, risk-triggered work on top of it, such as verified source of wealth, senior approval, and more frequent review. Then give one concrete trigger, like a PEP or a high-risk jurisdiction, to show you know when it actually applies.

## 11 Beneficial Ownership

A **beneficial owner** is the real, living person who ultimately owns or benefits from an account or company, even if their name never appears on the paperwork. Often a lawyer, a trust, or a chain of holding companies is listed on paper instead of them.

Ownership tells you who benefits financially. Control tells you who actually makes the decisions. They're not always the same person. Layered structures (a trust owning a holding company that owns the operating company) usually exist for perfectly legitimate tax and estate reasons, but they're also a common way to hide who's really behind an account.



Where to actually look this up: [UK Companies House](#) is free and covers registered UK entities directly. In the EU, national registries connect through the [Business Registers Interconnection System](#). For cross-border structures, [OpenCorporates](#) collects company filings from around the world, and the [GLEIF LEI search](#) shows which legal entities sit above or below each other through Legal Entity Identifier parent data. One limit for EU checks: since a 2022 EU court ruling, most national beneficial ownership registers are no longer fully public, and access usually requires showing a legitimate interest, which banks and other regulated firms usually have. The US has no public federal UBO registry. Ownership information collected under the Corporate Transparency Act sits with FinCEN, not in a searchable public database, so US entity ownership usually gets traced through individual state Secretary of State filings instead. Each state runs its own website, so finding the right one takes time. [e-SecretaryOfState.com](#) is a useful shortcut: a free directory linking out to every state's official Secretary of State business search page. Note: it is a privately run service (published by InCorp Services, a registered-agent and business-formation company), not a government source itself. It just points you to the right one.

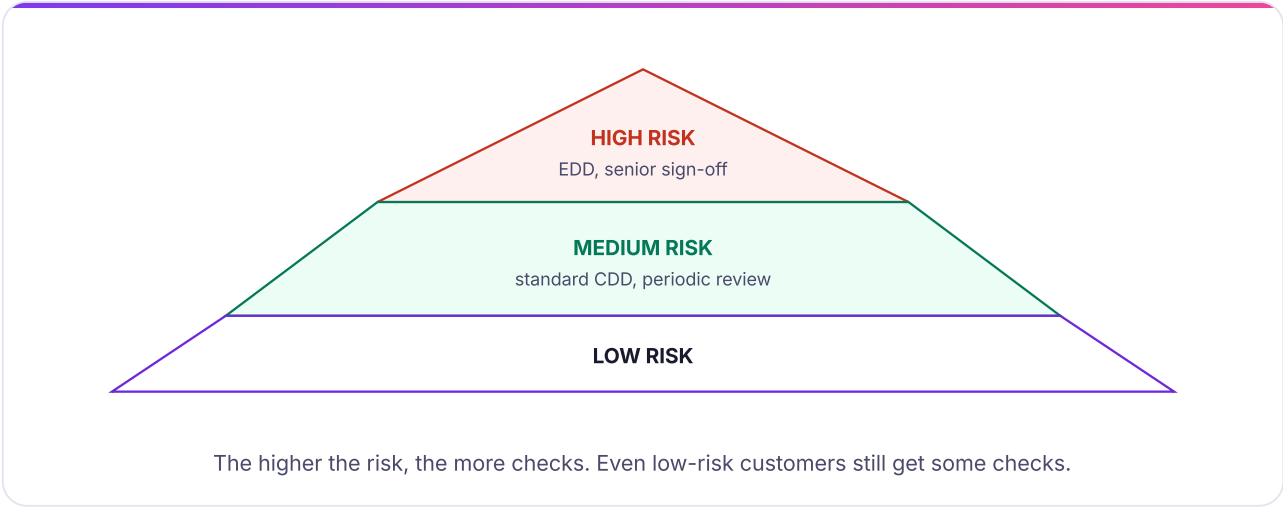
#### 🚩 RED FLAGS

- An ownership chain that ends in a jurisdiction with weak corporate registries
- Nominee directors with no apparent connection to the business
- A beneficial owner who changes shortly after account opening with no clear commercial reason

## 12 Customer Risk Rating

A risk score tells you where to start looking closely. It is not a final decision. A common early-career mistake is treating a low-risk rating as permission to stop looking. Geography, product, channel, and transaction behavior all feed the score. If any one of

them changes (say, a low-risk customer suddenly starts using a high-risk product), that should trigger a reassessment rather than waiting for the next scheduled review.



Risk models typically score four groups of factors. Know them well. **Customer:** individual or entity, occupation, PEP status, ownership complexity. **Geography:** residence, nationality, and where funds come from and go to, with FATF's grey and black lists as a baseline input. **Product and service:** a basic savings account carries very different risk from private banking or correspondent services. **Delivery channel:** face-to-face versus fully remote onboarding, or business introduced through a third party.

This is how they work together. A salaried resident opening a current account in person scores low on every factor. Change one input (the same customer starts receiving regular transfers from a grey-listed jurisdiction) and the geography score moves. Change two (a remotely onboarded business account with a nominee director) and the rating should reach the level that needs EDD. The exact math is not the point. It's that every factor is documented, so anyone reviewing the file can see exactly why the rating landed where it did.

|                                                                | CUSTOMER | GEOGRAPHY | PRODUCT | CHANNEL | OUTCOME   |
|----------------------------------------------------------------|----------|-----------|---------|---------|-----------|
| <b>Salaried resident,</b><br>current account in person         | Low      | Low       | Low     | Low     | Low       |
| <b>Same customer + transfers</b><br>from a grey-listed country | Low      | Higher    | Low     | Low     | Re-assess |
| <b>Remote business account</b><br>with a nominee director      | High     | Low       | Low     | High    | EDD       |

Changing one risk factor changes the score. Changing two can push the customer into EDD. Record every factor.

#### 🚩 RED FLAGS

- A risk rating that hasn't moved despite a material change in customer activity
- A scoring model that gives geography so much weight that it hides signals from customer behavior
- Manual overrides to risk scores with no documented justification

## 13 High-Risk Customers & Relationships

A **PEP (Politically Exposed Person)** is someone who holds, or is closely connected to someone who holds, a prominent public position: a government minister, a judge, a senior military officer. Close family members and known close associates count too. They're flagged high-risk not because they've done anything wrong, but because their position gives them more opportunity to take bribes or misuse public funds than the average customer. **Correspondent banking** is when one bank holds an account for another bank, usually so the second bank's customers can access foreign currency or make international payments without the second bank opening its own branch abroad. An **MSB (Money Services Business)** is a company, like a money transmitter or currency exchange, that moves money for other people rather than for itself.

PEPs, correspondent banking, MSBs, cash-intensive businesses, and virtual-asset customers are all labeled high-risk for different reasons, and a one-size-fits-all EDD checklist misses what actually matters for each. A PEP's risk is about influence and corruption exposure. An MSB's risk is about being a pass-through: it doesn't just hold its customers' money, it moves it onward, so a single MSB account can carry thousands of other people's transactions. A cash-intensive business's risk is about how easily criminal cash can be mixed in with legitimate daily sales.



#### PEP

##### Influence

The position itself creates the opportunity for bribes or misuse of public funds.



#### MSB

##### Pass-through

One account can carry thousands of other people's transactions.



#### CASH-INTENSIVE BUSINESS

##### Blending

Dirty cash hides easily inside legitimate daily takings.

#### 🔍 RECENT SHIFT: DOMESTIC PEPs IN THE UK

In January 2024, the UK amended its Money Laundering Regulations so that domestic PEPs (UK politicians and senior officials) start from a lower risk position than foreign PEPs unless other risk factors are present. The change followed public complaints from politicians about bank accounts being refused or closed. It's a useful reminder that "PEP" is a label that triggers an assessment, not an automatic EDD verdict, and that regulators expect the response to match the actual risk.

#### 🚩 RED FLAGS

- A PEP relationship with no documented source-of-wealth review
- A correspondent account with no visibility into the respondent's own underlying customers
- A cash-intensive business whose declared revenue doesn't match deposit patterns

## PART IV

# Products, Monitoring & Casework

The products you review (accounts, wires, cards, wallets), how alerts are created, and how to write a case that another person can follow later.

## 14 Business Entities & Legal Structures

An **LLC (Limited Liability Company)** is a business structure that legally separates its owners' personal assets from the company's debts and liabilities. It's a real operating entity with its own name and bank account. A **trust** is a legal arrangement where one party (the trustee) holds and manages assets on behalf of someone else (the beneficiary), often used to plan how assets pass to family, or to protect assets for future generations. A **shell company** is a registered business with no real operations, employees, or physical presence. It exists on paper only.

#### 🔍 EASY TO CONFUSE: SHELL vs. SHELF

These two sound almost identical and mean different things. A **shell company** has no real activity, ever. It's created to hold or move money and nothing else. Example: someone registers "Apex Trading LLC" purely to receive wire transfers, with no product, no employees, and no office. A **shelf company** is a real, legally registered company that was set up and then left untouched ("sitting on a shelf") so it can later be sold to someone who wants a business with an older incorporation date. Sometimes the reason is legitimate, since a longer history can help win contracts or open accounts. It is also a known way to make a brand-new business look like it has been running for years. The warning sign is not that a shelf company is fake (it is truly registered). The warning sign is that its age does not match its actual activity.

Knowing these structures matters. It tells you what documents to expect and what a red flag really means. A trust with no clear beneficiary listed is normal for some estate-planning trusts and a serious concern for others. You can't tell which without knowing what the structure is for.

#### 🚩 RED FLAGS

- A private company with no operating history that immediately sees high-value activity
- A trust structure whose stated purpose doesn't match its transaction pattern
- A registered address that's a known mail-forwarding address with no other business presence

## 15 Accounts, Products & Transaction Types

Every product carries its own kinds of risk. Wires move fast and cross borders easily. Cards generate large numbers of small transactions that are hard to review by eye. P2P (person-to-person) apps and payment wallets often have lighter KYC checks than traditional accounts. That is why they often show up in newer fraud and money mule typologies (known crime patterns).

Two changes are affecting product risk right now. The first is **instant payments**. India's UPI, the US FedNow service launched in 2023, and the UK's Faster Payments all settle in seconds and can't be recalled. This is good for customers, but it also helps fraudsters. A mule account (an account used to pass on criminal money) can receive and forward stolen funds before a monitoring rule has even finished running.

The second is liability (who pays for fraud losses). Since **7 October 2024**, UK payment firms must reimburse most victims of authorised push payment (APP) fraud, up to **£85,000** per claim, with the cost split equally between the sending and the receiving firm. The 50/50 split changed how banks behave, and quickly. Receiving banks now share the cost when scam money lands in a mule account they hold, so checking incoming payments now matters as much as checking outgoing ones.

Up to £85,000 per claim, back to the victim

SINCE 7 OCT 2024

**Sending firm**  
pays 50%

**Receiving firm**  
pays 50%

|  
**the bank hosting the mule account**  
now pays for it too

#### 🔍 HOW EACH PRODUCT GETS ABUSED

- **Wires:** moving value across borders quickly during layering
- **Cards and prepaid:** loading illicit cash, then withdrawing it abroad
- **P2P apps and wallets:** mule networks moving scam proceeds in small amounts
- **Trade finance:** over- and under-invoicing to shift value between countries
- **Loans:** borrowing legitimately, then repaying early with unexplained funds, an old integration technique

## RED FLAGS

- A savings account suddenly behaving like a business operating account
- Wire activity with no apparent commercial purpose
- A P2P wallet receiving many small inbound transfers from unrelated sources

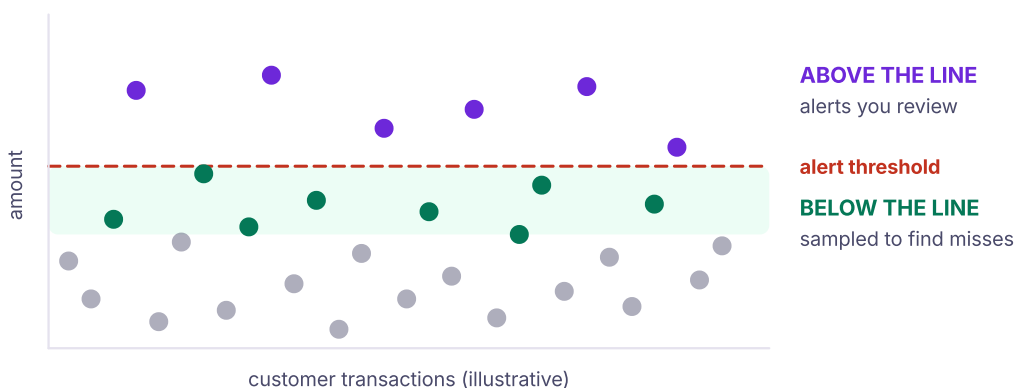
## 16 Transaction Monitoring Fundamentals

**Transaction monitoring (TM)** is the mostly automated process of scanning a customer's transactions and flagging anything that doesn't fit an expected pattern, so a human AML professional can take a closer look. It runs on **scenarios**: pre-built rules that check for a specific pattern, like a **threshold** (a transaction over a set amount) or a **velocity check** (an unusual number of transactions in a short window). Every one of these rules creates false positives (alerts on activity that turns out to be normal), because a rule can't see the full story. It only sees numbers.

The key skill is not writing a perfect rule. It is adjusting thresholds to fit your real customers, so the alert queue shows real risk instead of flooding AML professionals with alerts that don't matter.

A few scenarios are standard in TM systems. **Rapid movement of funds**: money arriving and leaving within a short window, with little balance left behind. **Structuring**: cash deposits kept just under a reporting threshold. **High-risk geography**: transfers to or from FATF-listed jurisdictions. **Profile deviation**: activity well above the customer's expected volume. **Repeated round amounts** to the same counterparty.

Tuning means adjusting thresholds so they catch real risk without flooding the team with false alerts. It is the skilled part of the job. Teams run **above-the-line** testing, reviewing what the current threshold produces, and **below-the-line** testing, sampling activity just under the threshold to see what is being missed. US regulators also expect TM systems to be tested and approved under model risk management guidance. So every threshold change needs a written reason, not just a lower alert count.



#### 🔗 AMLIFT TAKE

FinCEN's 2026 alerts can be turned almost directly into monitoring rules. Its September 2026 scam-center alert grouped red flags into three areas: payments from victims, activity on "guarantee" marketplaces (online markets that sell money laundering and scam services), and laundering techniques. A team that turns those red flags into scenarios within weeks makes a much better impression in a regulatory exam than one that files the alert and does nothing more.

#### 🚩 RED FLAGS

- An alert volume so high that AML professionals start skimming alerts instead of actually reviewing them
- A scenario that hasn't been tuned since it was first switched on, despite a changing customer base
- Recurring false positives from the same rule with no review of why they keep happening

## 17 Alert Investigation & Case Analysis

An **alert** is just the system's way of saying "this activity matched a pattern, take a look." It lands in an AML professional's queue when a monitoring rule is triggered. It isn't a verdict. It's a starting point. Next comes the investigation. Good investigation starts with a chronology (a timeline): rebuild what happened, in order, before deciding what it means. If you decide on a conclusion first and then look for evidence to support it, you are working the case backwards. This always shows in the write-up.



Reconstruct the order of events before you decide what they mean

#### 🚩 RED FLAGS

- A case narrative that states a conclusion in paragraph one and works backward
- Open-source research that wasn't documented (without a screenshot, there is no proof it was done)
- A closure rationale (the reason for closing the case) that doesn't address the original alert trigger

## ♀ AMLIFT TAKE

The first thing a good quality review checks: does the closure rationale actually answer the question the alert raised? Plenty of cases describe the customer in general terms ("long-standing customer, business appears legitimate") without ever explaining why this specific transaction triggered the rule.

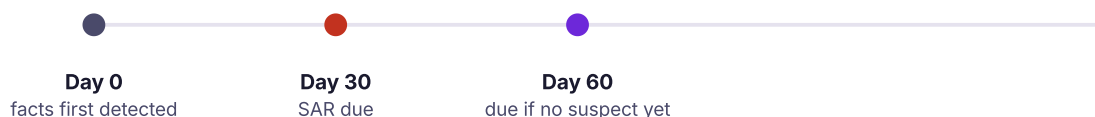
## 18 SAR & Narrative Writing

Quick refresher: a **SAR** is the formal report a financial institution files when it can't reasonably explain a customer's activity. The **narrative** is the written section inside it, the paragraph where an AML professional explains, in their own words, why the activity looked suspicious enough to report. The rest of this module is about writing that paragraph well.

A good SAR narrative answers who, what, when, where, why, and how, in plain, factual language. It lets the evidence make the case, not strong descriptive words. "The customer is likely laundering money" is a conclusion your evidence must support. Do not write it just because it feels true. Tie every transaction you mention back to a typology where you can. This makes the narrative useful to the investigator who reads it later, not just compliant on paper.

Deadlines are strict. In the US, a SAR is due within **30 calendar days** of first detecting facts that may require filing, which can be extended to **60 days** if no suspect has been identified. Continuing activity is reviewed on a **90-day** cycle, with any follow-up SAR due within 120 days of the previous filing. In India, STRs go to FIU-IND within **7 working days** of concluding that a transaction is suspicious. The UK sets no fixed deadline, but reports are expected promptly, and the DAML process from Module 08 (p. 18) applies when a transaction is still pending.

### FIRST SAR



### CONTINUING ACTIVITY



US timelines, drawn to scale in calendar days. India: 7 working days for an STR. UK: promptly.

A structure that works well in review: open with a one-paragraph summary covering who, how much, over what period, and why it's suspicious. Follow with the chronology, transaction by transaction. Then the investigation steps taken and what they found.

Close with the action taken on the account. Where a FinCEN alert applies, include its key term, such as FIN-2026-A7NETWORK from October 2026, so FinCEN can link the report to others about the same activity.

1

Summary

who, how much, when, why

2

Chronology

transaction by transaction

3

Investigation

steps taken + findings

4

Action

action on the account

+ FinCEN key term, if any

**CATCH THESE IN YOUR OWN DRAFT**

- Unsupported adjectives like "suspicious" or "clearly illicit" with no evidence sentence behind them
- A chronology that skips steps a reader would need to follow the logic
- A narrative so general it could fit five different customers, instead of being specific to this one

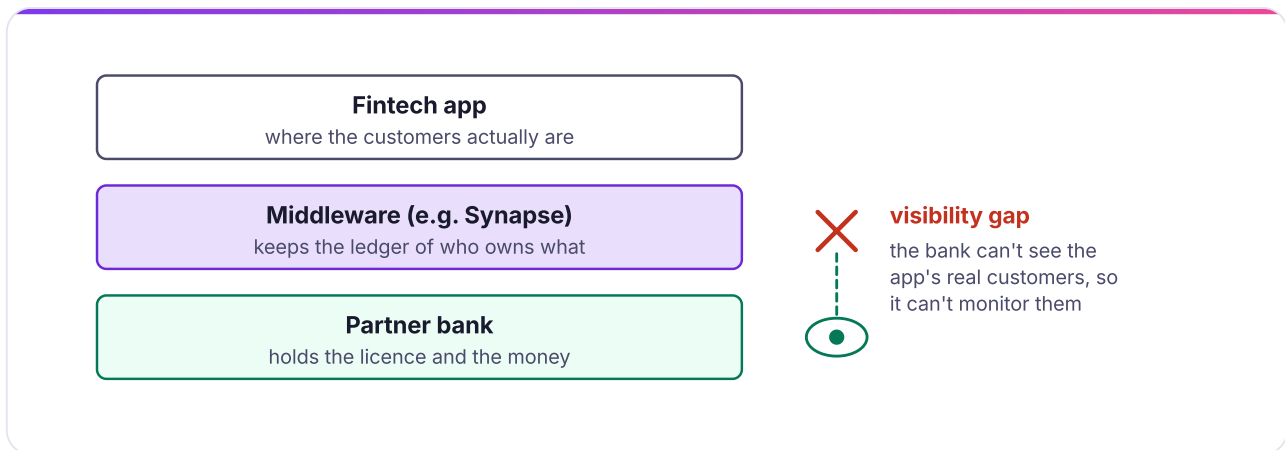
PART V

# Fintech & Crypto

A fast-changing area of AML. In instant onboarding and on-chain tracing (following crypto payments on the blockchain), practical skill matters more than theory.

## 19 Fintech & Digital Payments

**Embedded finance** is when a non-financial company (a ride-hailing app, an e-commerce platform) offers banking-like features (a wallet, a debit card, a loan) inside its own app, using a licensed bank's infrastructure behind the scenes instead of becoming a bank itself. Fintech didn't invent new ways to launder money. It removed the checks and delays that used to slow the old ones down. With instant onboarding, embedded finance, and automated account opening through APIs (software connections), a criminal can open, fund, and empty an account faster than traditional bank controls were designed to react.



#### Q TRUE STORY

Synapse, a banking-as-a-service (BaaS) firm that connected fintech apps to their partner banks, filed for bankruptcy in April 2024. After it collapsed, the banks and Synapse could not match which customer owned which funds, leaving thousands of app users locked out of their money for months. Around the same time, US regulators took enforcement action against several BaaS sponsor banks, including Evolve Bank & Trust, over weak oversight of their fintech partners. The AML lesson: if a bank can't clearly see its partner's customers, it can't monitor them either.

#### 🚩 RED FLAGS

- An account opened and immediately used for high-velocity activity with no gradual build-up
- Digital onboarding where document verification technically passed, but the documents look inconsistent on closer inspection
- Embedded-finance flows where the regulated partner has limited visibility into the platform's real customers

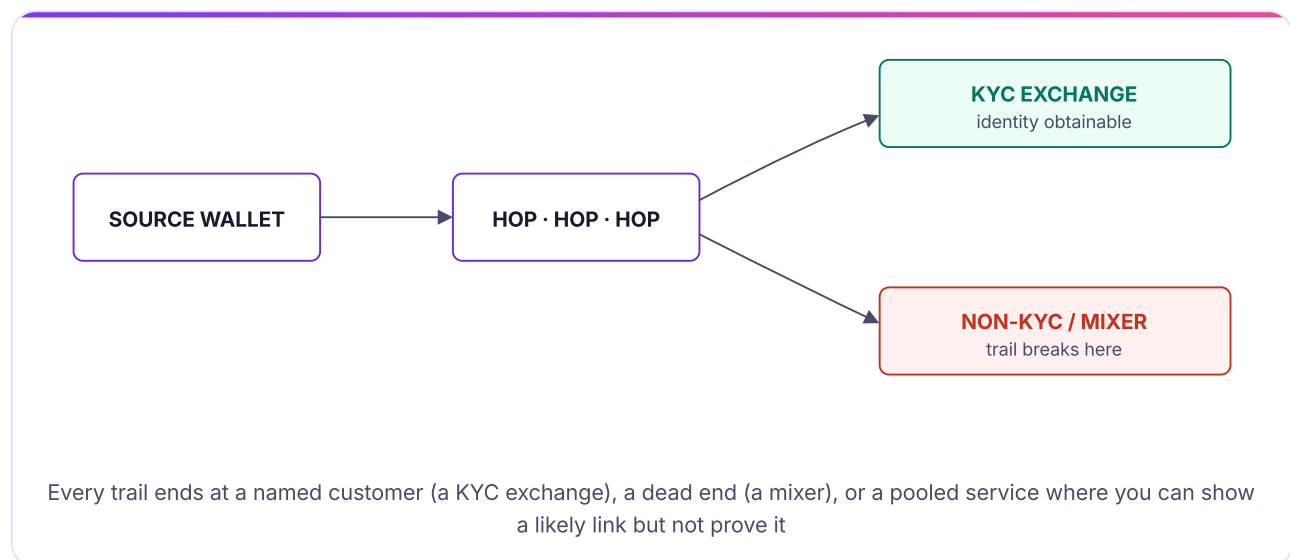
## 20 Cryptocurrency & Virtual Assets

First, some basics before the AML part. A **blockchain** is a public, shared record of every transaction ever made in a given cryptocurrency, kept by a network of many computers, not by one company. A **wallet** is what holds someone's crypto (in practice, a pair of cryptographic keys). A **wallet address** is the public string of characters people send funds to. It works like a bank account number, except no name is attached to it anywhere on the blockchain.

Blockchains are transparent but pseudonymous (users appear as addresses, not names). Every transaction is public, but the wallets stay nameless until one of them uses a service that runs KYC. Investigation means tracing: follow each transfer (hop) until you reach an exchange with identity records, a mixer (a service that blends funds to hide their source) that breaks the trail, or a swap service without KYC that pools funds into a shared reserve, where the on-chain link can no longer be proven. In most major

jurisdictions, VASPs (crypto service providers, such as exchanges) are now regulated like banks. They must meet a similar KYC standard, even though no single party controls the asset.

The EU has gone further with MiCA, the Markets in Crypto-Assets Regulation. It is a dedicated set of rules for issuing crypto-assets, holding them for customers (custody), and licensing exchanges. It adds to the AML duties AMLD5 already placed on VASPs. It does not replace them. Since 30 December 2024, the EU's crypto travel rule has also required sender and recipient details to travel with every crypto transfer a regulated provider handles, the same principle bank wires have followed for years. Don't mix these up: MiCA is mostly about market conduct and prudential standards (how firms behave and how much capital they hold). AML duties for crypto firms still come from the AMLD/AMLR rules. A VASP can be fully MiCA-licensed and still fail an AML exam.



Two different tool categories do the work here. For **blockchain analytics and tracing** (the tools that follow each hop shown in the tracing diagram), know [Chainalysis](#), [TRM Labs](#), and [Elliptic](#). **Crypto-specific KYC and onboarding**, the identity checks VASPs run when onboarding customers, is a separate category, where providers like [Sumsbit](#) sit. Different job, different tool. Don't mix them up in an interview.

#### Q TRUE STORY

Binance's 2023 settlement with US authorities, roughly \$4.3 billion across DOJ, FinCEN, and OFAC actions for Bank Secrecy Act and sanctions violations, is a clear signal that VASPs are held to the same standard as banks, not a lighter one. The case centered on the exchange knowingly serving customers in sanctioned jurisdictions and failing to file required reports: exactly the KYC and screening gaps this module covers.

The story continued. By mid-2026, Binance still didn't hold a MiCA license in the EU, after withdrawing its application in Greece when regulators raised concerns about its AML controls and whether founder Changpeng Zhao, who had pleaded guilty to BSA violations in the 2023 case, could pass MiCA's "fit and proper" ownership test. Without a license, Binance had to start closing its EU retail business when the EU's transition period for licensing ended on 1 July 2026, while competitors like Coinbase,

Kraken, and OKX had secured theirs months earlier. The lesson: a past AML enforcement record does not go away. It affects every licensing decision about the firm afterward.

#### 🚩 RED FLAGS

- A peeling chain: one large balance moved through a long series of fresh addresses, with a small amount peeled off at each hop
- Rapid fan-out from one wallet to many new wallets with no economic reason
- A swap through a service with weak or no KYC right before funds land on a regulated exchange
- Chain-hopping (moving funds between different cryptocurrencies) with no economic reason other than hiding the trail
- A wallet's activity touching an address already flagged for sanctions exposure

#### 🔗 AMLIFT TAKE

A common mistake in crypto write-ups: treating a match in timing and amount across a swap service as proof, instead of as strong circumstantial (indirect) evidence. It usually is strong evidence. Write it that way, not as a certainty the public blockchain can't actually give you.

## PART VI

# Typologies & Predicate Crime

The same few methods (split the money into small amounts, use someone else's name, make it look like trade or business income), repeated across all asset types, jurisdictions, and crime types.

## 21 Common Money Laundering Typologies

A **typology** is a known, named pattern of how money laundering usually happens. Here are five common ones. Each works differently, but they all have the same goal: making criminal money look like it came from a legitimate source.

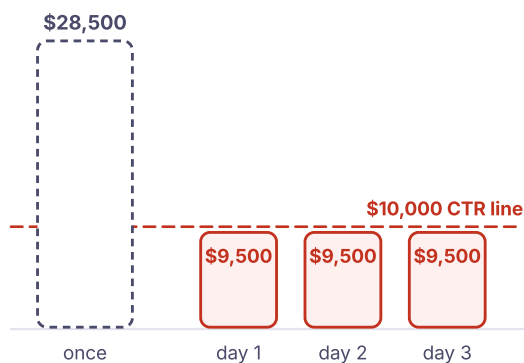
### | Five classic typologies

**Structuring:** splitting one large transaction into several smaller ones specifically to stay under a reporting threshold. For example, depositing \$9,500 on three days in a row instead of \$28,500 once is structuring. In the US, structuring is a crime by itself, even if the money is fully legal.

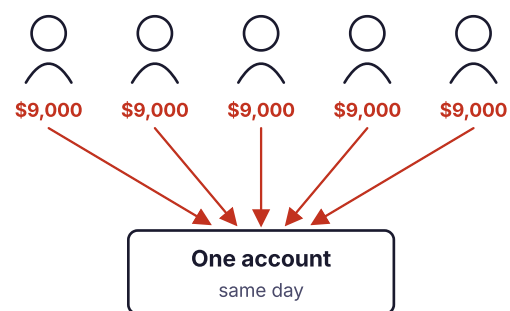
#### Q EASY TO CONFUSE: STRUCTURING vs. SMURFING

People often use these two words as if they mean the same thing, but there is a small difference. Structuring is the general term for splitting a large sum into smaller amounts to avoid a threshold, and one person can do it alone: three separate \$9,500 deposits over three days by the same individual is structuring. **Smurfing** is one type of structuring where several different people, often recruited for this job, each make a small deposit so that no one person's activity looks unusual. If five different people each deposit \$9,000 into the same account on the same day, that's smurfing: structuring done by many people instead of one. Every case of smurfing is structuring; not every case of structuring is smurfing.

##### STRUCTURING • ONE PERSON



##### SMURFING • MANY HANDS



Every case of smurfing is structuring. Not every case of structuring is smurfing.

**Funnel accounts:** one account that receives lots of small deposits from different people or places, then quickly forwards the combined total elsewhere. In short, money comes in from many sources and leaves as one amount.

**Mule networks:** groups of people who let their own bank accounts be used to receive and pass on someone else's criminal money, in return for a share. Many are recruited without fully understanding what they are agreeing to.

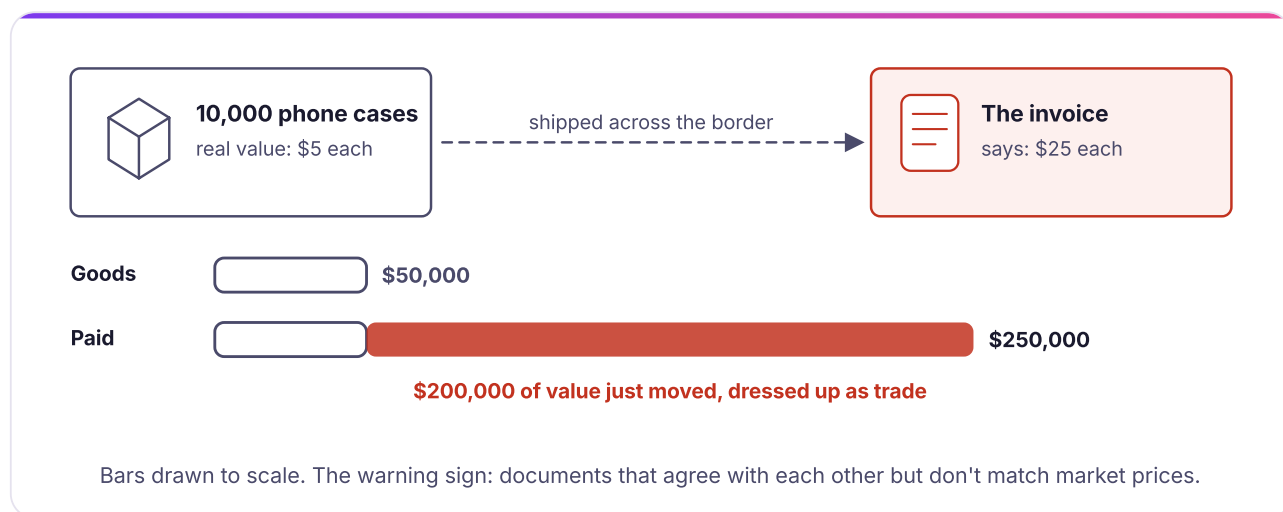
**Shell companies:** businesses that exist on paper, with a registration and a bank account, but do no real trading or operations. They make a transfer look like normal business activity when there is no real business behind it.

#### Q EASY TO CONFUSE: SHELL vs. SHELF COMPANY

Think of two shops on the same street. A **shell company** is a shopfront with a sign and a bank account but nothing inside: no stock, no staff, no customers. It exists only so money can pass through a name that looks like a business. A **shelf company** is a real shop that was registered years ago and then left closed, so someone can buy it later and say "established 2015." A shell company hides that there is no real business. A shelf company hides how new the business really is. Look more closely at either one when its paperwork does not match its activity. Module 14 (p. 29) covers both in more depth.

**Trade-based laundering:** hiding the movement of value inside an import or export deal that looks legitimate, usually by putting a price that is too high or too low on the invoice, so the money moves as if it were normal trade.

Worked example: a company exports 10,000 phone cases worth \$5 each, so \$50,000 of goods, but invoices them at \$25 each. The overseas buyer pays \$250,000 for \$50,000 of product, so \$200,000 of value has crossed the border looking like normal trade income. If the price is set too low instead (under-invoicing), value moves the other way. The warning sign: documents that agree with each other but do not match market prices.



These five methods are connected. The same few methods are used again and again across all asset types and jurisdictions. Once you learn the pattern, you can spot it in a bank statement or in a block explorer (a website that shows crypto transactions).

| Typology               | The move           | What it tends to look like in the data                                            |
|------------------------|--------------------|-----------------------------------------------------------------------------------|
| <b>Structuring</b>     | Break it up        | Repeated cash deposits just under the reporting threshold                         |
| <b>Funnel accounts</b> | Collect it         | Many small deposits from different places, combined and sent out fast             |
| <b>Mule networks</b>   | Borrow a name      | Ordinary personal accounts suddenly receiving and forwarding third-party funds    |
| <b>Shell companies</b> | Fake a business    | Round-number "invoices" with no staff, premises, or trading footprint behind them |
| <b>Trade-based</b>     | Misprice the goods | Invoice prices far from market value, or goods that don't match the shipment      |

## **| New and emerging typologies**

**Pig butchering:** a long-running investment scam where criminals build the victim's trust for weeks, usually through dating apps or "wrong number" messages, then push them to invest on a fake crypto trading platform. Many of these scams are run from scam

compounds in Southeast Asia, where the workers are trafficking victims. FinCEN's September 2026 alert tied nearly \$13 billion in suspected activity to these scam centers.

**Chinese money laundering networks:** brokers who buy US dollars earned from drug sales from cartels, then sell those dollars to Chinese nationals who want to get around China's capital controls (limits on moving money out of the country). FinCEN issued a dedicated advisory on this typology in 2025.

It's a modern version of the **Black Market Peso Exchange**, the classic typology from the 1980s and 1990s. Colombian cartels sold US dollar drug proceeds at a discount to peso brokers, who then used those dollars to pay for goods that Colombian importers were buying from the US. The drug money left the country looking like payment for legal imports. The modern version uses the same idea, with different brokers and different capital controls.

**Sanctions evasion through intermediaries and stablecoins:** FinCEN's October 2026 alert on Russia's A7 network describes front companies (companies used to hide the real party) in other countries listed as the payers on trade documents, alongside a ruble-linked stablecoin, A7A5, used to move value outside sanctioned banking channels.

**Mule recruitment through social media:** "easy money" job posts aimed at students and young adults, offering a share of the money for receiving and passing on funds. Many recruits don't realize they're committing a crime until their account gets frozen.

#### Q TRUE STORY: SEVERAL TYPOLOGIES IN ONE NETWORK

US prosecutors say one network run by Da Ying Sze moved more than \$470 million through TD Bank, much of it as large cash deposits made by couriers into accounts the network controlled, then wired out to other jurisdictions. Some bank employees accepted gift cards worth tens of thousands of dollars and kept processing the deposits. This one case shows placement, funnel accounts, and bank staff helping the criminals, and it is a big part of why TD paid \$3 billion in 2024.

#### Q HOW TO SPOT A MULE ACCOUNT

- A newly opened account, often held by a student or young adult, that suddenly receives transfers from many unrelated people
- Money leaving almost as soon as it arrives, usually in one or two large outbound payments
- Logins from several devices or locations, or from a location that doesn't match the account holder
- Payment references that don't fit the customer's profile, such as "invoice" or "rent" on a student account

#### 🚩 RED FLAGS

- Multiple deposits just under a reporting threshold on the same day or across related accounts
- One account receiving many small inbound transfers and rapidly forwarding them out
- Invoice values that don't match the goods described, a classic trade-based laundering sign

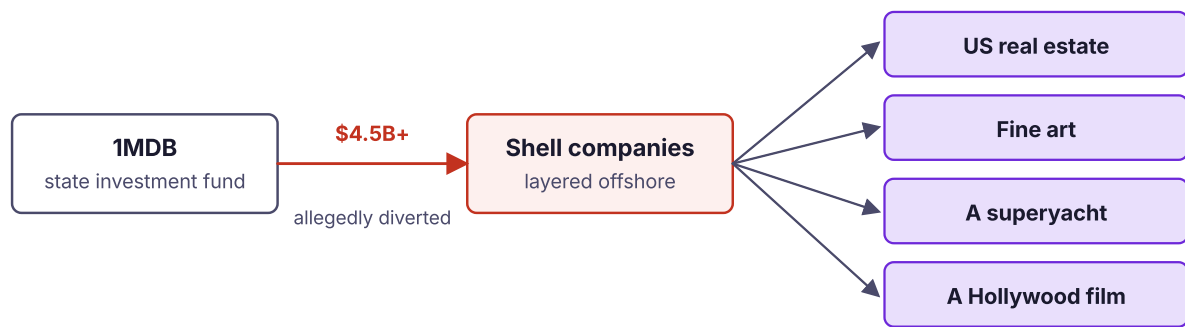
## 22 Corruption, Trafficking & Predicate Crimes

**Corruption** covers offences like bribery (offering or accepting something of value to influence an official decision) and embezzlement (someone entrusted with funds, such as an employee or an official, stealing them for personal use). **Trafficking** covers the illegal trade of people, drugs, or goods. Human trafficking specifically means moving or holding people through force, fraud, or coercion for exploitation. A **predicate crime** is the underlying offence that generated the illicit money in the first place: bribery, embezzlement, trafficking, drug dealing, cybercrime. AML deals with the money these crimes produce. You don't need to prove the predicate crime yourself. You need to recognize financial patterns consistent with one, and document them clearly.

Human trafficking leaves recognizable financial signs: several workers' wages paid into one account, accounts opened by a third party who also "translates" for the customer, rent and travel paid for groups of people by one individual, and frequent late-night payments to online classified ad sites. The forced labor inside the scam compounds from Module 21 (p. 37) shows how trafficking and fraud now often share the same case.

#### 🔍 TRUE STORY: 1MDB

Malaysia's state investment fund 1MDB is a well-known modern kleptocracy case (leaders stealing from their own country). US authorities allege more than \$4.5 billion was diverted from the fund and laundered through shell companies, US real estate, fine art, a superyacht, and even the financing of a Hollywood film. Goldman Sachs, which arranged bond deals for the fund, paid more than \$2.9 billion in 2020 to resolve US investigations, and former Prime Minister Najib Razak was convicted in Malaysia. The warning signs are typical of a PEP case: state money moving into private accounts, layered offshore entities, and luxury assets far beyond any explainable income.



A typical PEP case: state money, offshore layers, luxury assets far beyond any explainable income

#### RED FLAGS

- Payments to or from a party connected to a PEP, with no clear commercial reason
- Wages paid in a pattern that doesn't fit the stated job, such as several workers' pay landing in one account
- Transaction memos or counterparties matching known extortion or ransomware payment patterns

## 23 Terrorist & Proliferation Financing

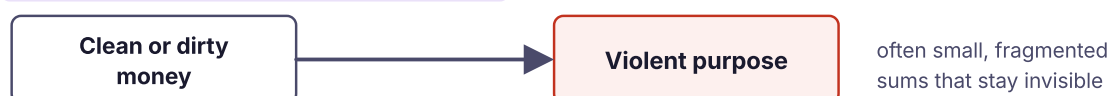
**Terrorist financing (TF)** is providing or collecting funds, from either legal or illegal sources, intending or knowing they'll be used to carry out a terrorist act. **Proliferation financing (PF)** is the same idea applied to weapons of mass destruction: funding the development, acquisition, or transport of nuclear, chemical, or biological weapons, usually tied to a sanctioned state's weapons program.

TF often works the opposite way to money laundering (ML). Instead of large sums that need to look legitimate, TF often uses small, split-up transactions that need to stay hidden, sometimes sent through non-profits or informal channels. Because PF is usually linked to sanctioned states, it overlaps a lot with sanctions work and is reviewed from both the AML side and the sanctions side.

#### MONEY LAUNDERING · HIDE WHERE IT CAME FROM



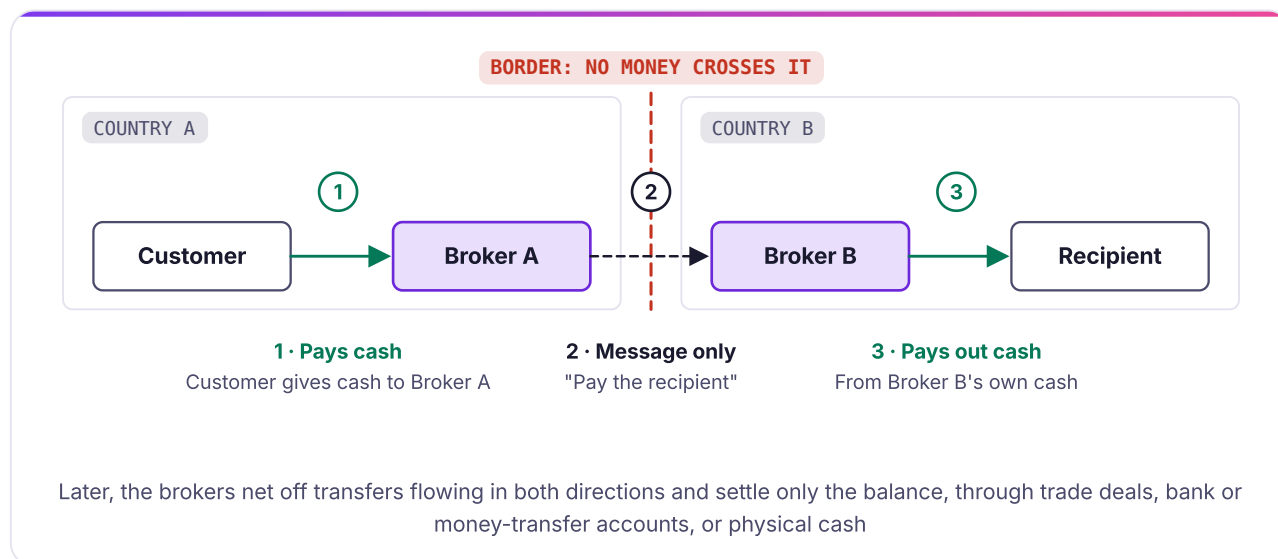
#### TERRORIST FINANCING · HIDE WHERE IT'S GOING



Laundering hides where money came from. Terrorist financing hides where it is going.

**Hawala** and similar informal value transfer systems move value without any money physically crossing a border. A broker in one country takes cash from a customer, a partner broker in another country pays out the equivalent, and the two brokers settle up later. Often no money moves at all for each transfer: payments flowing the other way are netted off against each other, and only the balance left after a few weeks or months gets settled. That balance is usually cleared through trade (one broker pays for goods the other needs, sometimes with over- or under-priced invoices), through transfers between bank or money-transfer accounts, or by moving physical cash across the border. Hawala is legitimate and widely used by migrant communities to send money (remittances) home, which is why abuse is hard to spot.

Non-profits need the same balanced approach. FATF Recommendation 8 asks countries to protect non-profits from TF abuse in a targeted, risk-based way, not by de-risking (cutting off) the whole charity sector.



#### Q TRUE STORY: PROLIFERATION FINANCING GOES CRYPTO

In February 2025, hackers stole roughly \$1.5 billion in crypto assets from the exchange Bybit, the largest crypto theft on record. The FBI attributed the attack to North Korea, and UN monitors have long reported that stolen crypto helps fund the country's weapons programs. That makes exchange security a proliferation financing issue, not just a cybersecurity one. Within days, the stolen funds were being swapped and moved across chains, the same tracing problem described in Module 20 (p. 35).

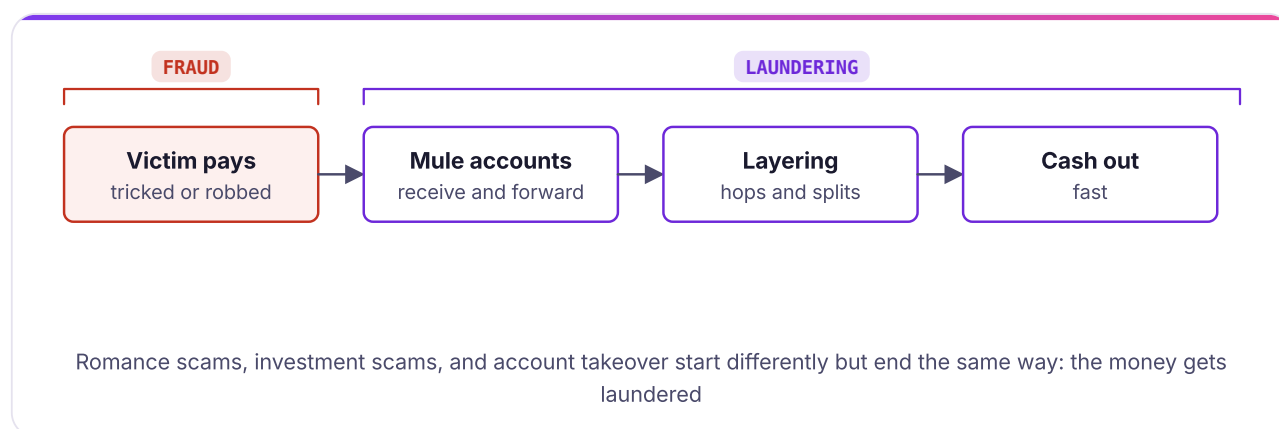
#### 🚩 RED FLAGS

- Many small transactions just below reporting or monitoring thresholds moving toward a common destination
- A non-profit whose donation pattern does not match its stated mission or the region it says it serves
- Trade financing for dual-use goods (items with both civilian and military uses) routed through intermediaries in sanctioned or high-risk jurisdictions

## 24 Fraud & Financial Crime

**Fraud** is intentionally deceiving someone to gain a financial benefit or cause them a financial loss. A **romance scam** builds a fake relationship, often over weeks or months, before asking for money. An **investment scam** promises returns that don't exist to get someone to hand over funds. **Account takeover** is gaining unauthorized access to someone else's real account and draining it.

Fraud and money laundering are related, but in law they are different crimes. Fraud is how the money became illegal. Laundering is what happens to it afterward, so a good AML professional treats a fraud case as the start of a laundering trail, not the end of the investigation. Romance scams, investment scams, and account takeover all follow the same path once the victim's money moves: through mule accounts, into layering, and out as cash, fast.



### Q TRUE STORY

FTX's 2022 collapse shows how fraud and weak financial-crime controls often go together. Customer deposits were mixed with company money, moved into a related trading firm, and misused, and auditors and investors were misled about this for years before the exchange failed. The lesson for AML professionals: mixing customer funds with company money, combined with weak internal controls, let the fraud run undetected for years.

### 🚩 RED FLAGS

- An elderly customer suddenly sending large sums to a new relationship or investment contact
- Account access from a new device or location immediately followed by high-value outbound activity
- Funds matching a recently reported scam pattern that are then rapidly forwarded onward
- A customer who seems to have been told what to say: reading from a script, insisting a transfer is urgent, or saying they've been told not to discuss it with the bank

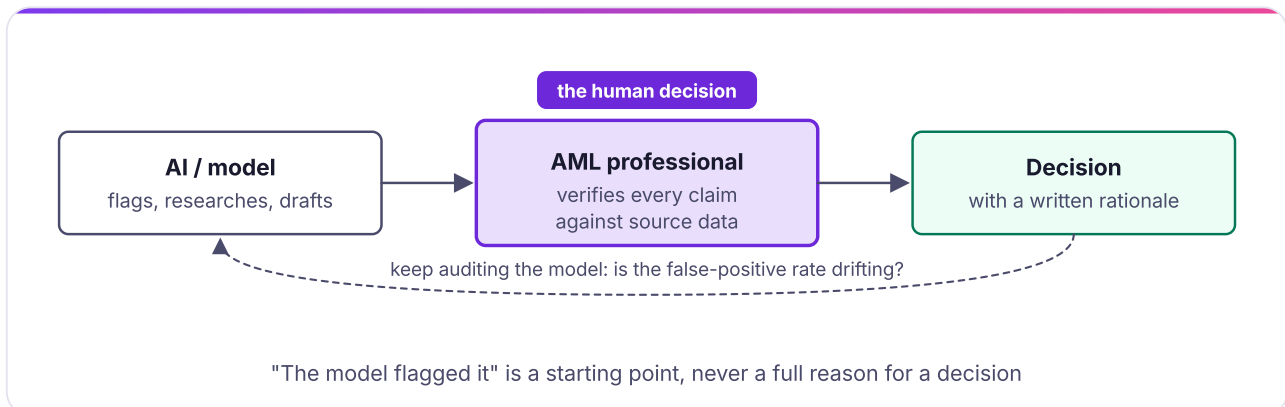
# Technology & Career

What AI really changes about this job, and how compliance hiring actually filters resumes.

25

## AML Technology, Data & AI

Machine learning models in AML depend on the labeled data and assumptions used to train them, and "the model flagged it" is never a full reason on its own. Being able to explain a result matters as much as accuracy, especially once a regulator asks why a specific customer was flagged, or wasn't. AI does speed up research, finding patterns, and writing first-draft narratives. It does not replace the human decision on whether the evidence really supports a conclusion. Treating it as if it does leads to weak cases being filed.



Criminals use the same technology. FinCEN issued an alert in November 2024 on fraud schemes using **deepfake media**: AI-generated identity documents, photos, and video used to pass remote onboarding checks. Red flags include images that look edited or inconsistent, customers who can't complete live verification and blame "technical glitches," and devices or IP addresses that don't match the stated identity.

Regulators are getting explicit about AI too. The EU AI Act treats AI used for creditworthiness assessment as high risk, but it excludes systems used only to detect financial fraud. Across jurisdictions, supervisors expect firms to explain any model that drives a compliance decision, which is why being able to explain models is now a real job requirement on monitoring and model-validation teams.

#### 🚩 RED FLAGS IN A TECH-ASSISTED WORKFLOW

- An AI-drafted narrative accepted without the AML professional verifying every factual claim against source data
- A model whose false-positive rate keeps rising with nobody auditing why
- Automation used for a decision that really needs human judgment

26

## Career Development & Applied Practice

For freshers (new graduates), the usual path into AML starts with KYC or basic transaction monitoring, not investigations. Get strong at that work first. SAR writing, harder cases, and later quality-review duties come with time. Certifications like [CAMS](#), [ICA](#)'s qualifications, or [ACFCS](#)'s CFCS, all well recognized across the industry, help more with passing an ATS (Applicant Tracking System, the software that scans resumes before a human ever sees them) filter and a recruiter's checklist than with teaching you the job.

Their value has also changed. Five to ten years ago, mostly senior professionals took these certifications. Now freshers and people with one or two years of experience take them just as often, so many more people hold the same certification than before. As a result, the certification now helps at an earlier stage. It used to help you get the job. Now it mostly gets your resume past the first filter and gets you an interview. After that, the interview decides, along with how current and useful your knowledge is. You still learn the job itself by working cases, and from a reviewer who explains why your work was sent back.

Job descriptions do not usually mention this. Once you know the basics, most of the work is making decisions you can defend and documenting them to a set standard. There is often no single correct answer. Two AML professionals can close the same alert for opposite reasons and both be right, as long as the reasoning is written clearly enough to make sense to someone reading it years later: an examiner, an auditor, or a new hire trying to reconstruct what happened. The decision itself (close or escalate) is the smaller part. The real skill is knowing what an examiner will later ask for, and writing the file today so it already answers that question.

Every AML professional works a little differently. Every manager runs a team a little differently. Every institution covered by AML rules, whether a bank, a fintech, or a crypto exchange, builds its own process and its own shortcuts. But once a file is closed, one question matters more than all of that, in every role and every type of institution: does the reasoning still make sense when a regulator reviews it?

### ♀ FOR FRESHERS: QUALITY BEFORE VOLUME

New AML professionals often feel pressure to choose between closing more cases and closing them well. Choose early. Understanding the product, the process, and the workflow behind a case is what makes you fast. Speed comes from understanding. It is not a shortcut around it. Pushing for volume before you have that understanding does not make you productive. It only builds up hidden risk in the file, which can come out later in a quality review, an audit, or a regulator's request. Focus on understanding first. Speed will follow.

### 🔴 FIX THESE IN YOUR OWN RESUME

- Generic bullet points that could describe anyone's KYC role, not what you specifically reviewed and decided
- Certifications listed with no context for how you've actually applied them
- No mention of volume, jurisdiction, or the specific controls you worked on, which are exactly what compliance hiring managers filter for

## | Questions that come up often in AML interviews

### ♀ INTERVIEW PREP

- **"Walk me through how you'd investigate a TM alert."** They want an answer in time order: alert trigger, customer profile and KYC, transaction history, counterparties, open-source research, then a documented decision. See Module 17 (p. 32).
- **"What's the difference between source of funds and source of wealth?"** The retired-surgeon example in Module 10 (p. 21) is a strong answer.
- **"What makes a good SAR narrative?"** Who, what, when, where, why, and how, with evidence behind every claim. See Module 18 (p. 33).
- **"What would you do if a customer asks why their account is under review?"** This tests tipping-off (telling a customer they are being reviewed or reported). Don't disclose anything. Escalate to your manager or MLRO.
- **"Tell me about a recent AML development."** Have one ready, such as the June 2026 FATF grey list changes or FinCEN's 2026 scam-center alert, both covered in this handbook.
- **"How do you balance quality and productivity?"** Say that speed comes from understanding the product and the process, and that pushing volume before you understand a case only builds up risk that shows up in a later review. That's exactly the answer hiring managers want to hear.

### ♀ WHY AMLIFT EXISTS

AMLift was built after seeing strong AML candidates get rejected because of general resume advice that did not understand what compliance hiring looks for in the FCA, FinCEN, or FIU-IND jurisdictions. A resume tool that doesn't know the difference between a SAR and an STR can't help anyone get past the first screen.

# Where this field actually leads

Where freshers start, how AML professionals move up, and how teams are set up at different types of employers.

## Where freshers actually start

Very few people start in investigations. These four roles are the common starting points, and each one teaches a different part of the work.

ENTRY ROLE

**KYC / CDD Analyst**

Reviewing new customer files, checking identity documents, and judging how risky each customer is. A very common first role, and a fast way to learn the basics of CDD.

ENTRY ROLE

**Transaction Monitoring Analyst**

Working through alerts that rules flagged and deciding which need a closer look. Quickly builds skills in building timelines and spotting patterns.

ENTRY ROLE

**Sanctions / Screening Analyst**

Closing or escalating alerts where a name matches a watchlist. Narrower than TM, but a fast way to learn precision and to back each decision with evidence.

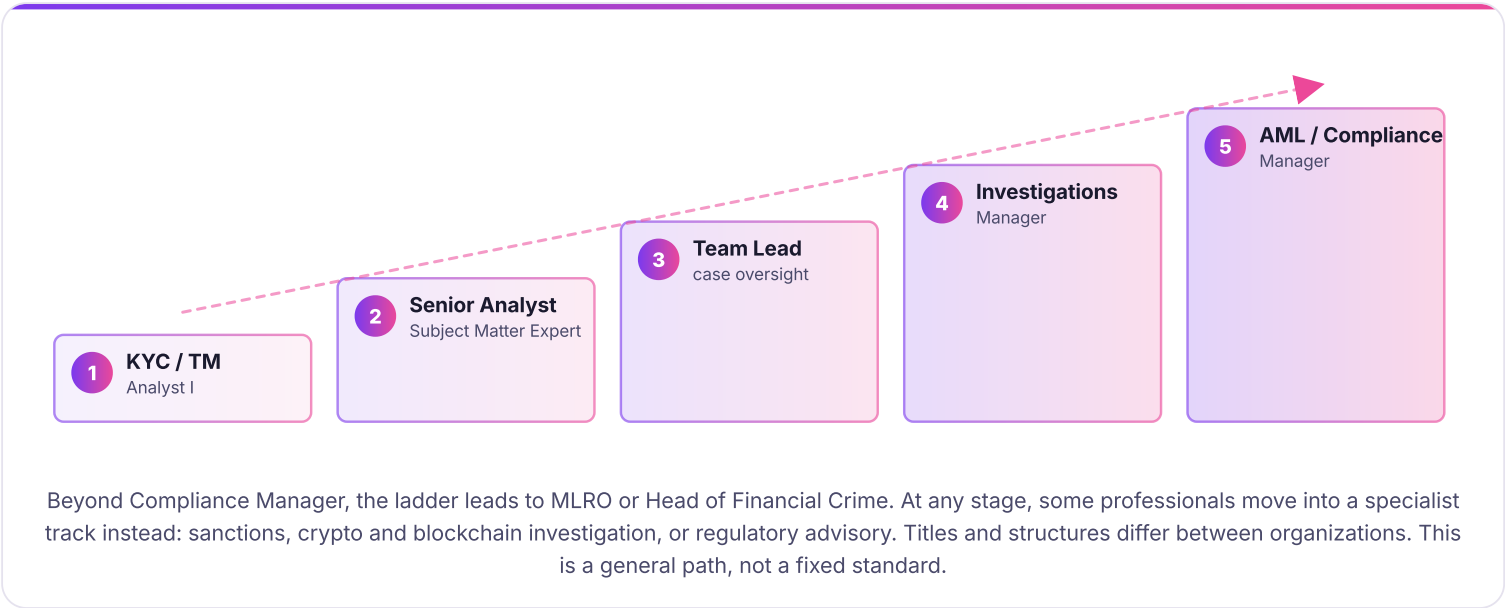
ENTRY ROLE

**Onboarding / CIP Analyst**

The first check on who new customers are, often at a fintech or payments company. The work is fast and high-volume, and it is a good path into wider CDD work.

## The ladder

Not every organization uses these exact titles, but this is a common progression. Some people follow it into management. Others move into a specialist area instead.



# Typical team structures, by industry

The structure varies by type of employer. Each list runs from most senior (top) to most junior (bottom).

TRADITIONAL BANK

Financial Institution

MLRO / Head of Financial Crime

AML Program Manager

Investigations Manager

Team Lead, KYC or TM

Senior Analyst / SME

KYC, TM, or Screening Analyst

FINTECH & PAYMENTS

Leaner, Faster-Moving Teams

Head of Compliance / MLRO

Financial Crime Manager

Investigations Lead

Senior Compliance Analyst

Onboarding / CDD Analyst

CRYPTO / VASP

Compliance Often Sits Close to Product

Chief Compliance Officer

Head of Financial Crime / Investigations

On-Chain Investigator / Blockchain Analyst

Sanctions & Screening Analyst

KYC / Onboarding Analyst

CONSULTING & ADVISORY

Project-Based, Client-Facing

Partner / Director

Engagement Manager

Senior Consultant

Consultant / Associate

Analyst (often remediation or lookback projects)

## | Specialist tracks worth knowing

After the fundamentals, some AML professionals choose to specialize. **Sanctions** specialists move into screening strategy, OFAC and OFSI licensing, and export controls. This area has grown quickly since the 2022 Russia sanctions. **Crypto and blockchain investigators** work at exchanges, analytics firms, and law enforcement agencies, where practical skill in tracing funds counts for more than certificates. **Financial crime advisory** roles at consulting firms focus on remediation, lookbacks (re-reviewing past activity after a control failure), and program design. Many institutions are also joining their **fraud** and AML teams into one financial crime team, so demand is growing for AML professionals who understand both.

# People worth following

Two people whose posts are worth having in your LinkedIn feed. One keeps you current on AML itself, the other on the fintech businesses that AML professionals monitor.

AML & FINANCIAL CRIME

**Marco Beranzoni**  
Founder, FinCrime Agent

Shares the latest findings and developments in AML: what is happening across the field and what is changing in financial crime compliance. A quick way to stay current between handbook updates. His website has videos and training resources.

[linkedin.com/in/marco-b-8121922](https://www.linkedin.com/in/marco-b-8121922) →  
[fincrimetagent.com](https://www.fincrimetagent.com) →

FINTECH

**Marcel van Oost**  
Connecting the dots in FinTech

Writes about fintech business models, acquisitions and expansion into new markets. His posts are not about AML directly, but they explain the businesses AML professionals monitor: how a fintech makes money, what changes when it is acquired, and what a new product or market means for customer risk and compliance controls.

[linkedin.com/in/marcelvanoost](https://www.linkedin.com/in/marcelvanoost) →

REFERENCE

# Glossary

Key terms to learn before your next interview.

**AML**  
Anti-money laundering. The rules and controls that stop money from crime from entering or moving through the financial system.

**AMLA**  
The EU's Anti-Money Laundering Authority, operational since mid-2025. Will directly supervise around 40 high-risk cross-border financial groups from 2028.

**AMLD**  
Anti-Money Laundering Directive. The EU's older AML directives (AMLD1 through AMLD6), which each country had to turn into its own law. Now being replaced by the AMLR.

**AMLR**  
Anti-Money Laundering Regulation. The EU's new single set of AML rules, which applies directly in all member states from July 2027.

**APP fraud**  
Authorised push payment fraud. The victim is tricked into sending the money themselves, for example to a fake investment or to a fraudster posing as their bank.

**AUSTRAC**  
Australia's AML regulator and FIU in one. Its Tranche 2 reforms added lawyers, accountants, real estate agents, and trust and company service providers to the regime from 1 July 2026, and widened its crypto rules.

**Beneficial owner**  
The real person who owns or controls an entity, even if someone else is named on paper. Also see UBO.

**BSA**  
Bank Secrecy Act. The 1970 US law that most American AML duties come from.

**CDD**  
Customer Due Diligence. Understanding a customer's purpose, expected activity, and source of funds.

**Chain-hopping**  
Moving crypto across several blockchains or coins to make it harder to trace.

**CIP**  
Customer Identification Program. Verifying who a customer actually is.

**CTA**  
Corporate Transparency Act. US law requiring companies to report their real owners. Since 2025 it applies only to foreign companies registered to do business in the US.

**CTR**  
Currency Transaction Report. Filed in the US when a customer's cash transactions in the same direction (all deposits, or all withdrawals) total more than \$10,000 in a single business day.

**DAML**  
Defence Against Money Laundering. A UK request asking the NCA for permission before a firm processes a transaction it suspects involves criminal property.

**DNFBP**  
Designated Non-Financial Business or Profession. Lawyers, accountants, real estate agents, and similar "gatekeeper" jobs that many countries now place under AML rules.

## **ECCTA**

Economic Crime and Corporate Transparency Act 2023. UK law that created the "failure to prevent fraud" offence for companies, in force since September 2025.

## **EDD**

Enhanced Due Diligence. Deeper CDD checks, used for higher-risk customers.

## **Egmont Group**

A global network that lets FIUs safely share financial information with each other across borders.

## **FATF**

Financial Action Task Force. Sets the global standards most national AML laws are built on.

## **FCA**

Financial Conduct Authority. The UK's primary financial services regulator, supervising firms under the Money Laundering Regulations.

## **FinCEN**

Financial Crimes Enforcement Network. The US Treasury office that runs the BSA and sets what AML exams expect across the country.

## **FINTRAC**

Canada's FIU. It oversees the PCMLTFA and has detailed reporting rules.

## **FIU**

Financial Intelligence Unit. The national body that receives and analyzes suspicious activity reports.

## **Funnel account**

An account that gets many small deposits that look unrelated, then quickly sends the money somewhere else.

## **Hawala**

An informal money transfer system. Brokers in two countries pay out money for each other and settle later, so no money actually crosses a border.

## **Integration**

The last stage of laundering, when money comes back into the economy looking like legal income or assets.

## **KYC**

Know Your Customer. The general term that covers CIP, CDD, and EDD.

## **Layering**

Moving money through many accounts or products to hide where it came from.

## **MAS**

Monetary Authority of Singapore. Singapore's central bank and integrated financial regulator, including AML supervision.

## **MiCA**

Markets in Crypto-Assets Regulation. The EU's rules for how crypto markets must operate. These are separate from the AML duties VASPs have under AMLD/AMLR.

## **MSB**

Money Services Business. Includes money transmitters, currency exchangers, and check cashers.

## **Mule account**

An account used to move criminal money for someone else, often owned by a person recruited for this.

## **Mutual evaluation**

FATF's peer review that publicly rates how well a country really enforces its AML standards.

## **NCA**

National Crime Agency. Runs the UK's FIU function (UKFIU) and receives SARs from UK reporting entities.

## **OFAC**

Office of Foreign Assets Control. Administers US sanctions programs.

## **Peeling chain**

A crypto laundering pattern where a large balance moves through a long line of new addresses, and a small amount is split off at each step.

## **PEP**

Politically Exposed Person. A person who holds an important public position, or is closely linked to someone who does.

## **Perpetual KYC**

Also called continuous KYC. Updating a customer's file when something changes their risk, not on a fixed schedule.

## **Pig butchering**

A slow investment scam where criminals build trust with victims for weeks, then push them to invest on a fake crypto trading platform.

## **Placement**

The first stage of laundering, when criminal money first enters the financial system.

## **Predicate crime**

The original crime (such as fraud, corruption, or drug trafficking) that produced the money being laundered.

## **Residual risk**

The risk left after controls are applied to the starting risk. A high-risk customer with strong controls can have lower residual risk than a medium-risk customer with weak ones.

## **Risk-based approach**

FATF's main principle: the level of checks should match the real risk, not be the same for every customer.

## **SAR**

Suspicious Activity Report. Filed (in the US with FinCEN, in the UK with the NCA) when an institution suspects activity may involve crime and can't reasonably explain it.

## **Shelf company**

A real, registered company kept inactive on purpose so it can later be sold with an older start date. Often confused with a shell company.

## **Shell company**

A registered business with no real operations, employees, or physical presence. Exists on paper only.

## **Smurfing**

A type of structuring where several people each make a small deposit, instead of one person doing it all.

## **SoF**

Source of funds. Where a specific payment or deposit came from, such as a salary, a property sale, or a loan.

## **SoW**

Source of wealth. How a customer built their overall net worth over time, such as a career, a business, or an inheritance.

## **STR**

Suspicious Transaction Report. The equivalent of a SAR in India, Singapore, the UAE, and several other jurisdictions. The UK uses the term SAR.

## **Stripping**

A way to avoid sanctions by removing or changing details in a payment message so screening systems find nothing to match.

## **STRO**

Suspicious Transaction Reporting Office. Singapore's FIU, operating under the Singapore Police Force.

## **Structuring**

Breaking one large transaction into smaller pieces to stay under a reporting threshold.

## **Tipping off**

Letting a customer know, directly or indirectly, that they are the subject of a SAR or investigation. A crime in most jurisdictions, not just a policy breach.

**TM**

Transaction Monitoring. Automated rules that flag unusual account activity for review.

**Tranche 2**

Australia's 2026 change that put AML/CTF duties on lawyers, accountants, real estate agents, and other "gatekeeper" jobs not covered before.

**Typology**

A known pattern or method used to launder money. Structuring and trade-based laundering are both typologies.

**UBO**

Ultimate Beneficial Owner. The real person who owns or controls an entity, directly or through others.

**VASP**

Virtual Asset Service Provider. A crypto exchange or platform, now under AML-equivalent rules in most major jurisdictions.

**VDA**

Virtual Digital Asset. The term used in Indian regulation for crypto and similar digital assets.

**Wolfsberg Group**

A group of major global banks that publishes practical AML guidance. Firms often follow it before formal rules catch up.

WHAT'S NEXT

More handbooks are coming

This one covers the fundamentals. Three more are on the way.

COMING NEXT

AML: Advanced Topics

The topics this handbook left out on purpose: deeper typologies, complex structures, and the hard decisions that come up once you know the basics well.

COMING NEXT

Crypto Basics & Investigations

A full, practical guide to blockchain tracing, laundering patterns at exchanges, and the tools real investigators use, building on Module 20 (p. 35) of this handbook.

COMING NEXT · DEDICATED PAGE

Interview Questions by AML Role

A dedicated page with one interview handbook for each role. Click your designation and that role's interview questions open as their own downloadable handbook, built for self-study before the interview.

- AML Analyst
- KYC Analyst
- EDD Analyst
- Transaction Monitoring Analyst
- Sanctions Analyst
- Quality Assurance Specialist
- Regulatory Compliance Manager
- + more roles

**"A defensible AML decision is one an examiner, an auditor, or a stranger reading it years later can follow and understand exactly why it was made."**

THE PRINCIPLE THIS WHOLE HANDBOOK IS BUILT AROUND

YOUR NEXT THREE MOVES

**01**

**Re-read the red flags**

Before any interview, skim every red flags box in this handbook. Together they work as a list of likely interview topics.

**02**

**Rehearse the interview questions**

Say the answers from Module 26 out loud until they sound like you, not like a script.

**03**

**Audit your resume**

Run it through HirePath, free at [amlift.tech](https://amlift.tech), to see how it measures up against what compliance hiring managers look for.

**Continue at [amlift.tech](https://amlift.tech) →**

HirePath, the AMLift career tool, checks your resume and LinkedIn against what compliance hiring managers look for in the FCA, FinCEN, AUSTRAC, CBUAE, and FIU-IND jurisdictions, then compares you with real job descriptions. No signup needed.

© 2026 AMLift · Original work · [amlift.tech](https://amlift.tech)