


Technical note on

# **Anti-Money Laundering and Countering the Financing of Terrorism legislative package**

**Final (Official Journal of the EU) version**

- 
1. General overview

---
  2. Regulation establishing a new EU AML and CFT Authority

---
  3. Regulation on the prevention of the use of the financial system for ML/TF

---
  4. Regulation on fund transfers to trace transfers of cryptoassets

---
  5. Directive on AML/CFT prevention mechanisms

---
  6. Directive on access by competent authorities to centralized bank account registers

---
  7. Why Management Solutions?

---
  - A. Annex I

---



# 1 | General overview

## Executive summary

### The new AML package will protect EU citizens and the EU's financial system against money laundering and the CFT






#### Context

- The EC published in May 2020 an Action Plan for an EU policy on AML and CFT setting out the EC's commitments to strengthen EU rules in this area.
- To implement this Action Plan, in July 2021, the EC presented a package of legislative proposals to strengthen EU rules in this area and in November 2021, a proposal for a Single Access Point Directive. In April and May 2024, the proposal was adopted by the EP.
- Finally, in June 2024, the **AML and CFT legislative package** has been **published** in the **OJEU**.

#### Objective

- The aim of this package is to improve the **detection** of **suspicious transactions** and **activities** and to close loopholes that allow the **laundering of illicit proceeds** or the **financing of terrorist** activities through the financial system.

#### Contents of the package

-  Regulation establishing a new EU AML and CFT Authority
-  Regulation on the prevention of the use of the financial system for the purposes of money laundering of AML and CFT
-  Regulation concerning transfers of funds to trace transfers of crypto-assets
-  Directive on AML/CFT prevention mechanisms
-  Directive on access by competent authorities to centralized bank account registers

#### Next Steps

Applicable as of **July 1, 2025**

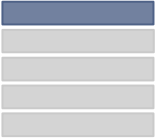
As a general rule, applicable **36 months** after its publication.

Applicable as of **December 30, 2024**




Member States will have to implement the Directives within **three years from the entry into force (by July 9, 2027)**.

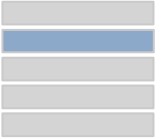
# 2 Regulation establishing a new EU AML and CFT Authority

## Main aspects



New authority on anti-money laundering and countering terrorist financing (AMLA) is established to ensure efficient supervision of high-risk entities, strengthen common supervisory approaches for other entities, and facilitate cooperation between FIUs

Scope 	Main Content 
<div>Obligated entities</div> <ul style="list-style-type: none"><li>Credit institution, a financial institution, or a group of credit institutions or financial institutions at the highest level of consolidation in the EU in accordance with applicable accounting standards.</li></ul>	<div>The <b>Authority's tasks regarding ML/TF risks</b> include:</div> <ul style="list-style-type: none"><li>Monitoring and assessing <b>ML/TF threats</b> within the internal market;</li><li>Evaluating <b>the impact of third countries'</b> AML/CFT systems on the internal market;</li><li>Collecting and analyzing information on <b>weaknesses</b> in AML/CFT rule application, risk exposure, sanctions, and remedial actions from its activities and those of other supervisors;</li><li>Maintaining a <b>central AML/CFT database</b> with up-to-date information from supervisory authorities and the Authority's activities;</li><li>Analyzing and <b>sharing database information</b> with relevant authorities on a need-to-know and confidential basis;</li><li>Supporting risk analysis and compliance with <b>financial sanctions</b>;</li><li>Facilitating <b>cooperation and information exchange</b> between entities to develop a common understanding;</li><li><b>Issuing publications, providing training</b>, and raising awareness about ML/TF risks.</li></ul>
<div>Non-obliged entities</div> <ul style="list-style-type: none"><li>Those that are <b>not directly under the AMLA's scope for AML/CFT supervision</b>. However, they may still be subject to scrutiny or indirect supervision through cooperation with other supervisory bodies .</li></ul>	
<div>Objective </div> <ul style="list-style-type: none"><li>The objective of the AMLA shall be to <b>protect the public interest</b>, the <b>stability</b> and <b>integrity</b> of the Union's financial system, and the <b>proper functioning</b> of the <b>internal market</b> by, among others, preventing the use of the EU's financial system for the purposes of ML and TF.</li></ul>	



## Exhaustive harmonization of AML rules for the first time throughout the EU, closing legal loopholes for fraudsters

### Scope

The **following entities are required** to comply with the regulation:

- Credit Institutions
- Financial Institutions
- Natural or Legal Persons in Professional Activities <sup>(1)</sup>

### Main content

#### Cross-border operations

- Obligated entities shall **notify their home state supervisors** about plans to operate in another Member State, as soon as the obliged entity takes steps to carry out the activities, and, in the case of establishments at least 3 months prior to the commencement of those activities.
- Entities must follow **the national rules** of each Member State where they established.
- A **central contact point** must be appointed to ensure compliance with applicable laws if required.

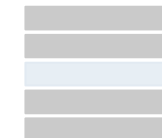
#### Internal policies of obliged entities

- Obligated entities shall have in place **internal policies, procedures, and controls to ensure compliance**. These measures should mitigate and manage the risks of ML, TF, and the risk of non-implementation and the evasion of targeted financial sanctions.
- Obligated entities shall take **appropriate measures**, proportionate to the nature of their business, including its risks and complexity, and their size, to identify and assess the risks of ML and TF.
- The **business-wide risk assessment** drawn up by the obliged entity shall be **documented, kept up-to-date and regularly reviewed**, including where any internal or external events significantly affect the ML and TF risks associated with the activities of the obliged entity.

### Exemptions

- Member States may decide to exempt, in full or in part, **providers of gambling services** from the requirements on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.
- Member States may decide to exempt **professional football clubs**: i) if they participate in the **highest division of the national football league** and have a total annual turnover of less than EUR 5 000 000, or the equivalent in national currency, for each of the previous 2 calendar years from the requirements set out in this Regulation on the basis of the proven low risk posed by the nature and the scale of operation of such professional football clubs; ii) if they participate in a **division lower** on the basis of proven low risk posed by the nature and the scale of operation of such professional football clubs.
- **Legal or natural persons engaged in financial activities** on an occasional where there is little risk of ML or TF from the requirements set out in this Regulation, provided that all of the following criteria are met: i) the financial activity is limited in absolute terms; ii) the financial activity is limited on a transaction basis; iii) the financial activity is not the main activity of such persons; iv) the financial activity is ancillary and directly related to the main activity of such persons; v) the main activity of such persons is not some of the obliged entities as auditors; and v) the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

1) Auditors, External Accountants, Tax Advisors, Notaries, Lawyers, Independent Legal Professionals; Trust or Company Service Providers; Estate Agents and Real Estate Professionals; Precious Metals and Stones Traders/High-Value Goods Traders, Gambling Service Providers; Crowdfunding Service Providers and Intermediaries; Cultural and High-Value Goods Traders/Intermediaries; Credit Intermediaries; Migration Operators; Non-Financial Mixed Activity Holding Companies; Football Agents; and Professional Football Clubs.



## The regulation on fund transfers now includes provisions to trace transfers of crypto-assets, in addition to traditional funds

### Scope

This Regulation applies to entities that engage in the following activities:

- **Transfers of funds**, in any currency, sent or received by a payment service provider (PSP) or an intermediary payment service provider established in the EU and **transfers of crypto-assets**, including those executed by crypto-ATMs, where the crypto-asset service provider, or the intermediary crypto-asset service provider, of either the originator or the beneficiary has its registered office in the EU.

The following activities are **excluded**:

- **Some services listed in the Directive on payment services in the internal market**, as the payment transactions made exclusively in cash, without any intermediary intervention or the professional physical transport of banknotes and coins.
- **Transfer of funds where some conditions are met**, as it involves the payer withdrawing cash from the payer's own payment account or it constitutes a transfer of funds to a public authority as payment for taxes, fines or other levies.
- **Exclusion of persons with no activity other than converting paper documents into electronic data** and that do so pursuant to a contract with a PSP, or to **persons with no activity other than providing PSPs with messaging or other support systems** for transmitting funds.

### Subject

*On payment or crypto-asset service providers*

*On the payment service provider of the payee*

*On intermediary payment service providers or crypto-asset service provider between others*

### Main content

- Rules on the **information on payers and payees accompanying transfers of funds** and on the information on **originators and beneficiaries accompanying transfers of crypto-assets**, for the purposes of preventing ML and TF, where at least one of the payment service providers or crypto-asset involved in the transfer of funds or crypto-assets is established or has its registered office, as applicable, in the EU.
- Rules on **internal policies, procedures and controls** to ensure **implementation of restrictive measures** where at least one of the payment service providers or crypto-asset involved in the transfer of funds or crypto-assets is established or has its registered office, as applicable, in the Union.

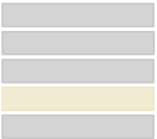
- Transfers of funds shall be accompanied by the payer's information or some information on the originator, such as the name or the payment account number.

- i) detection of missing information on the payer or the payee; or ii) implementation of effective risk-based procedures for determining whether to execute a transfer of funds lacking the required complete payer and payee information

- i) retention of information on the payer and the payee or the originator or beneficiary accompanying the transfer; ii) detection of missing information on the payer or the payee or originator or the beneficiary; iii) establishment of effective risk-based procedures for determining whether to execute a transfer of funds lacking the required payer and payee information or a transfer of crypto-assets lacking the required information on the originator.

# 5 Directive on AML/CFT prevention mechanisms

## Main aspects



The directive will improve the organization of national AML systems by establishing clear rules on how FIUs and supervisors work together

### Scope

- **Member States of the EU**, which are required to establish mechanisms to prevent the use of their financial systems for ML or TF.
- **Financial entities and professionals** acting as gatekeepers of the Union's financial system, who will need to adhere to stricter requirements and undergo training and integrity verification.
- **Sectors identified with specific risks** related to ML and TF, which will be subject to AML/CFT requirements as assessed by Member States.
- **Investor residence schemes**, which are highlighted as potential risks that Member States need to mitigate.
- **Legal entities and arrangements**, which will be under scrutiny to prevent their misuse for money laundering, with requirements for maintaining beneficial ownership information in central registers.
- **The public**, who will have conditional access to beneficial ownership information to ensure transparency and integrity of financial dealings.

### Main content

#### Identification of exposed sectors at national level

- A Member State may extend the AML/CFT package to additional sectors if they identify money laundering and terrorist financing risks in those areas.



#### Bank Account information and FIUs

- Member States must establish **centralized automated mechanisms**, like central registers or electronic data retrieval systems, to identify individuals and entities holding or controlling accounts identified by IBAN or virtual IBAN within their jurisdiction. This information must be immediately and directly accessible, without filtering, to Financial Intelligence Units (FIUs) and the AMLA. Additionally, each Member State shall establish a FIU to prevent, detect, and combat money laundering and terrorist financing. The FIU will receive, analyze, and disseminate reports from obliged entities to competent authorities.



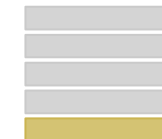
#### Registers and single access point to real estate information

- Member States must establish centralized mechanisms, such as central registers, to provide immediate, direct, and free access to information necessary for identifying real estate properties, their owners, and beneficial ownership of entities and trusts. These systems must allow competent authorities and the AMLA to electronically retrieve digital-format, ideally machine-readable, information essential for analyzing real estate transactions and ownership details without alerting the legal entities involved.



#### Risk assessment

- Each Member State must assess ML/FT risks and evasion of financial sanctions, conduct **a national risk assessment updated every 4 years**, and maintain **comprehensive** statistics to review the effectiveness of their AML/CFT frameworks.



The Directive on AML/CFT prevention mechanisms provides access to the single access point to FIUs. National competent authorities will have access to these records through the single access point, ensuring harmonization of the format of bank statements

### Subject

- Measures to **facilitate access to and the use of financial information and bank account information by competent authorities** for the prevention, detection, investigation or prosecution of serious criminal offences;
- Measures to **facilitate access to law enforcement information by FIUs** for the prevention and combating of money laundering, associate predicate offences and terrorist financing and measures to facilitate cooperation between FIUs;
- Technical **measures to facilitate the use of transaction records by competent authorities** for the prevention, detection, investigation or prosecution of serious criminal offences.
- Procedures under national law under which authorities competent for the **prevention of serious criminal offences** can require financial institutions and credit institutions to provide transaction records, including time-limits for providing transaction records.

### Main content



#### Designation of competent authorities

- Each Member State shall designate the **competent authorities** empowered to access and search its national centralised bank account registry. Those competent authorities shall include at least the **Asset Recovery Offices**.



#### Transaction records

- Financial institutions, credit institutions, and crypto-asset service providers shall **comply with specified technical requirements** when responding to requests for transaction records as part of criminal investigations.
- These requests include **tasks** like **identifying, tracing, and freezing assets** linked to such investigations, conducted under national law.
- The EC has the authority to establish these **technical specifications** through **implementing acts**, which define the electronic structure and technical means for providing transaction records.
- Member States shall ensure that FIUs are able to invite **Europol** to support them when carrying out the joint analysis.



#### Access by competent authorities to bank account information

- Member States shall ensure that the competent national authorities have the power to **access and search, bank account information in other Member States** available through the bank account registers interconnection system (BARIS) where necessary for the performance of their tasks for the purpose of preventing, detecting, investigating or prosecuting a serious criminal offence or supporting a criminal investigation concerning a serious criminal offence.
- Access to and searches of bank account information shall be performed only on a **case-by-case basis**.



# 7 | Why Management Solutions?

**Our extensive knowledge and experience in Financial Crime initiatives positions us as leaders in the provision of services in this area**

## Management Solutions



+4,000 employees worldwide with multidisciplinary profiles (computer scientists, business administration, engineers, economists and mathematicians).



Multidisciplinary skills: Analysis of business / regulatory informational requirements, combined with project management skills and extensive experience in the development and implementation of Informational Platforms.



Stable vendor for financial institutions within the realm of FC transformation program



Recognized commitment and proven ability to deliver quality and meet deadlines.

## System Implementation and IT Transformation



Implementation of FC industry systems, i.e.: Norkom, Oracle FCCM, HotScan, Actimize, Bridger, in relevant UK and US Financial Institutions



Data Management support for the FC function (Datamarts, DQ & Lineage)



Deep expertise in the implementation of Information Systems, from functional, technical and intermediary perspectives.



Identification of data sources and, definition and development of ETL processes.



User Acceptance Testing for systems of diverse background.



Support on the stabilization phase.



Project Management Office.

## Management and Regulation



Assessment of the FC function for global and national Financial Institutions.



Definition, design and development of a proprietary AML solution (Paladin 2.0), implemented in 15 Financial Institutions.



Gap Analysis of the regulatory coverage of FC framework; special focus on FFIEC Red Flags.



Governance and Use, and Regulatory compliance: coverage analysis of regulatory requirements such as BSA/AML, FFIEC Red Flags or DFS504, roadmap definition.



Processes re-engineering of the alert and case analysis process (workflow definition, methodology and criteria for the analysis, objective prioritization of alerts).

## Analytics



Model development/calibration: i.e. rules and scenario definitions, algorithm and watch list management, quantitative and qualitative approaches to rating models, testing, for both internal and vendor models (SAS AML, Oracle FCCM, Bridger, FircoSoft, Norkom, etc.)



Model validation (SR11-7), including functional coverage, customer segmentation, threshold setting, optimization and performance, preparation of testing cases,



Data analytics: analysis of rules and decisions, optimization of alerts, application of advance techniques for productivity enhancement and risk reduction (i.e. Machine Learning). Management Solutions has a proprietary solution for this, Paladin 2.0. See more information in the next slide.

# 7 Why Management Solutions?

## Paladin 2.0: Benefits and differentials

Paladin 2.0 comes as a response to the weaknesses identified in the dominant solutions in the market, focusing on E2E management of alerts and dossiers, regulatory and management reporting and allowing a transparent integration of engines

1 Comprehensive management of alerts, consolidating case analysis information on the front end and using graphs to analyse files and alerts. Integration of the communication process with the supervisory body.

2 Easy visualisation of dashboards and indicators, separated into executive, managerial and operational modules, allowing the management of accesses in different hierarchies for a more precise and faster decision.

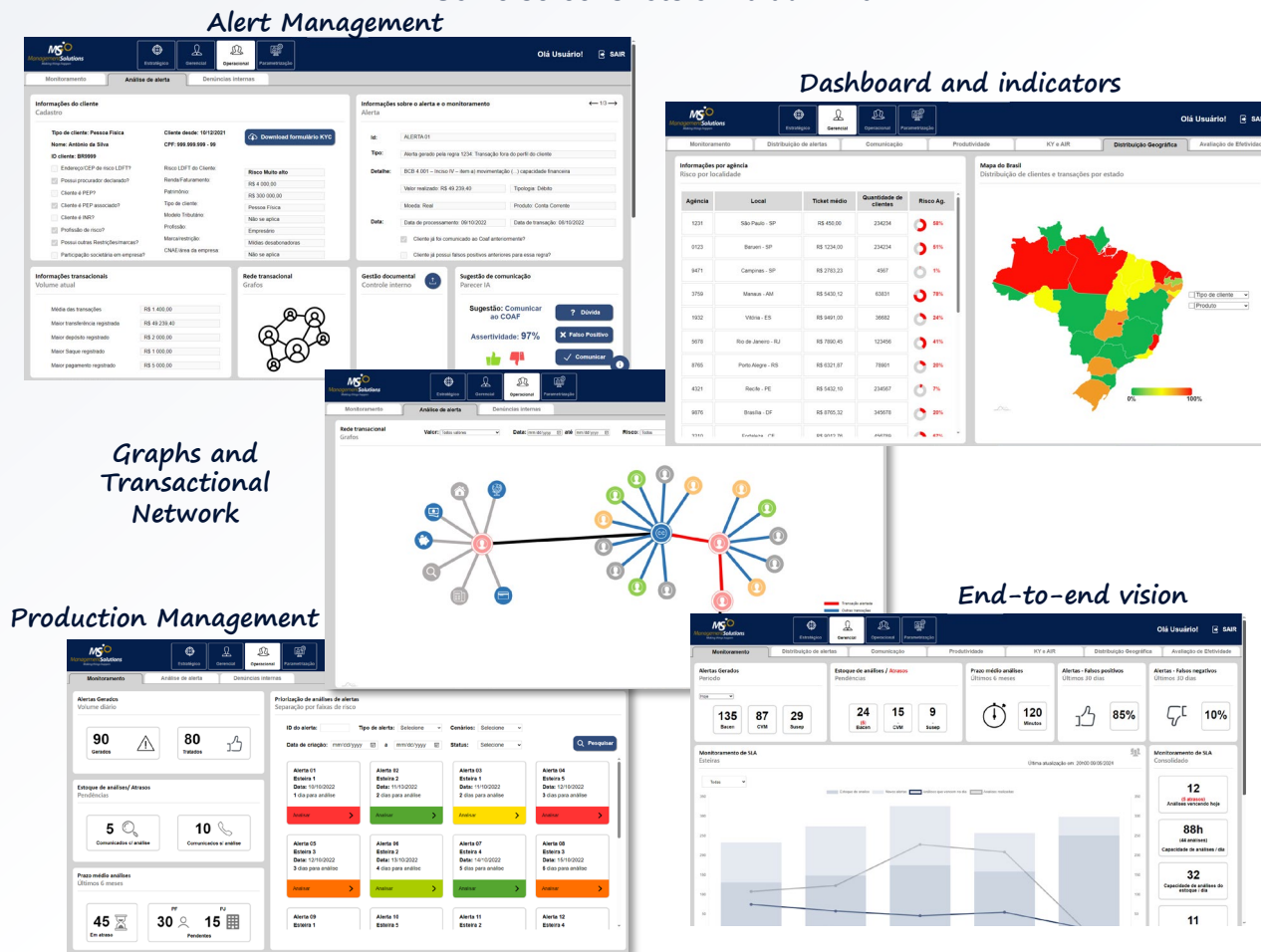
3 As an end-to-end tool, it can aggregate customer, product, transaction and other relevant AML information (PEP, sanctions, negative news) with a visualisation in a transnational network of graphs, facilitating customer analysis with transactional alerts.

4 It allows for the integration of AI in the prioritisation process and communication to the supervisory body, the system offers suggestions for communication or archiving.

5 The system has a high degree of customisation flexibility in its modules, and can be integrated autonomously with market solutions and with the institution's internal developments.

6 Paladin 2.0 offers the entire AML management process (i.e. monitoring, alert analysis, communication to the regulator, internal reporting,...) independently of the engines, facilitating the decoupling of IT from management and preserving business processes.

Some screenshots of Paladin 2.0...



## A

## Annex I: Abbreviations

<b>AML</b>	Anti-money-laundering
<b>AMLA</b>	EU AML and CFT Authority
<b>BARIS</b>	Bank Account Registers Interconnection System
<b>BS</b>	Balance Sheet
<b>BSA</b>	Bank Service Act
<b>CASPs</b>	Crypto-Asset Service Providers
<b>CFT</b>	Countering the Financing of terrorism
<b>Crypto-ATM</b>	Cryptocurrency Automated Teller Machine
<b>DTL</b>	Deferred Tax Liabilities
<b>EC</b>	European Commission
<b>EIOPA</b>	European Insurance and Occupational Pensions Authority
<b>EP</b>	European Parliament
<b>ESRB</b>	European Systemic Risk Board
<b>EU</b>	European Union
<b>FC</b>	Financial Crime
<b>FFIEC</b>	Federal Financial Institutions Examination Council
<b>FIUs</b>	Financial Intelligence Units

<b>IBAN</b>	International Bank Account Number
<b>LACDT</b>	Loss Absorbing Capacity of Deferred Taxes
<b>LTG</b>	Long-Term Guarantees measures
<b>ML</b>	Money Laundering
<b>NCA</b> s	National Competent Authorities
<b>OF</b>	Own Funds
<b>OJEU</b>	Official Journal of the European Union
<b>ORSA</b>	Own Risk and Solvency Assessment
<b>PSPs</b>	Payment Service Providers
<b>QRT</b>	Quantitative Reporting Templates
<b>RMBS</b>	Residential Mortgage-Backed Security
<b>SAS</b>	Statistical Analysis System
<b>SCR</b>	Solvency Capital Requirement
<b>TF</b>	Terrorist Financing
<b>TP</b>	Technical Provisions
<b>UFR</b>	Ultimate Forward Rate



International  
*One Firm*



Multiscope  
Team



Best practice  
*know-how*



Proven  
Experience



Maximum  
Commitment

© Management Solutions, 2024

All rights reserved. Cannot be reproduced, distributed, publicly disclosed or transformed, whether totally or partially, free of charge or at no cost, in any way or by any means, without the express written authorization of Management Solutions.

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intended to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

**Rafael Poza**

Partner at Management Solutions  
rafael.poza@managementsolutions.com

**Marta Hierro**

Partner at Management Solutions  
marta.hierro@managementsolutions.com

For more information please visit

[www.managementsolutions.com](http://www.managementsolutions.com)

Or follow us at: [in](#) [x](#) [f](#) [@](#) [v](#)