

A guide to AMLA: The EU's Anti-Money Laundering Authority

*A guide to everything you need to know about
the EU Anti-Money Laundering Authority*



A guide to AMLA:

The EU's Anti-Money Laundering Authority

| | |
|--|-----------|
| Purpose of the EU AMLA | 3 |
| How it all began | 4 |
| A brief history | 4 |
| Why EU AMLA was enacted | 5 |
| Why was EU AMLA created? | 6 |
| The 5 challenges of EU AMLA | 7 |
| The establishment of EU AMLA | 9 |
| Key features of EU AMLA | 9 |
| What does EU AMLA mean for EU and UK companies? | 12 |
| EU companies | 12 |
| UK companies | 13 |
| Getting ready for AMLA | 14 |
| Conduct a gap analysis | 14 |
| Implement policies | 14 |
| Enhanced Due Diligence | 15 |
| Leverage technology | 15 |
| Engage experts | 16 |
| Monitor developments | 16 |
| The cases that mattered: What led to EU AMLA | 17 |
| The Danske Bank scandal | 17 |
| The Swedbank scandal | 19 |
| The Deutsche Bank scandal | 21 |
| How VinciWorks can help | 23 |

The EU Anti-Money Laundering Authority (EU AMLA) is a regulatory body established under the EU's anti-money laundering and counter-terrorist financing (AML/CTF) framework. It was developed as part of legislative reforms introduced in 2021 to centralise and strengthen AML/CTF supervision across the EU.

The goal of AMLA is to unify, streamline and strengthen the EU's approach to combating financial crime in a globalised and increasingly complex financial landscape. It is anticipated that the authority will enhance transparency, improve supervision and ensure consistent enforcement of AML/CFT standards across member EU states.

The authority will be based in Frankfurt and will have direct supervisory powers over selected high-risk financial institutions operating across multiple member states. EU AMLA aims to ensure uniform application of AML rules across the EU by:

- Directly supervising "selected obliged entities" that are considered high-risk or operate in at least six member states
- Imposing sanctions on entities that fail to comply with AML regulations
- Coordinating with national regulators to improve information sharing and enforcement actions

EU AMLA is expected to be fully operational by late 2025, but its selection process for "selected obliged entities" will begin in 2027, with direct supervision starting in 2028.

Purpose of the EU AMLA

To harmonise regulations

The authority will ensure consistent implementation of AML/CTF rules across member states to address discrepancies in national laws.

To enhance supervision

The authority directly oversees high-risk financial institutions and coordinates with national authorities to enforce compliance.

To promote transparency

The authority introduces stricter measures for identifying beneficial ownership and detecting illicit financial flows.

To combat emerging threats

The authority addresses risks associated with digital assets, cross-border transactions and other modern financial crime methods.



How it all began

A brief history

The EU AMLA was formally proposed by the European Commission in July 2021. Its purpose was to address persistent weaknesses in the EU's AML/CTF programme. Specifically, there were significant issues in the enforcement and coordination of AML efforts across the EU. This was indicated by a number of high-profile money laundering scandals in Europe, including some involving major banks like Danske Bank, Swedbank and Deutsche Bank. The need for a more centralised and consistent approach was increasingly evident.

Life before AMLA

Before AMLA, AML/CTF responsibilities were fragmented, with each member state implementing directives through their national authorities. This patchwork approach often resulted in loopholes, inefficiencies and uneven enforcement. Essentially, the EU relied on a patchwork system where member states implemented EU AML directives through national laws and agencies.

These directives required member states to strengthen customer due diligence (CDD), enhance beneficial ownership transparency and improve cross-border information sharing.

But enforcement was left to national authorities which meant inconsistent application of the directives. Some countries were slow to implement them and the levels of actual enforcement varied wildly. Of course, criminals exploited these gaps to launder money across borders. It became increasingly clear that the lack of a central authority to monitor and coordinate AML efforts was a significant flaw in the programme.

Key milestones leading to AMLA's creation include:

Fourth AML Directive - 2015: Introduced risk-based supervision and beneficial ownership transparency.

Fifth AML Directive - 2018: Enhanced customer due diligence measures and broadened the scope of obliged entities.

Sixth AML Directive - 2021: Strengthened criminal penalties for money laundering and expanded the list of predicate offenses.

AML Package (2021): Proposed a centralised EU authority, culminating in AMLA, to ensure uniform application of AML standards.

Why EU AMLA was enacted

The establishment of EU AMLA was driven by growing concerns about the effectiveness of AML/CTF efforts across the EU. The key factors that precipitated its creation:

1. Money laundering scandals

Several major money laundering scandals exposed significant weaknesses in the EU's decentralised AML/CTF framework:

- **Danske Bank Scandal (2018):** Over €200 billion in suspicious transactions were funnelled through the bank's Estonian branch, highlighting failures in national oversight.
- **Swedbank and Deutsche Bank Cases:** These incidents involved large-scale money laundering through cross-border transactions, revealing vulnerabilities in EU-wide coordination.

These scandals damaged public trust and underscored the need for stronger supervision.

2. Fragmentation of national systems

AML/CTF supervision within the EU was historically handled by national authorities, leading to inconsistent enforcement, varying standards and regulatory arbitrage. Some member states were criticised for inadequate implementation of EU AML Directives, creating gaps that criminals exploited.

3. Emerging financial crime threats

The rise of digital assets, increased use of anonymous shell companies and complex cross-border transactions posed challenges that existing frameworks struggled to address. Criminals increasingly exploited regulatory loopholes and technological advancements to launder money and finance illicit activities.

4. Ineffective coordination

While institutions like the European Banking Authority (EBA) provided some oversight, their limited mandate and lack of enforcement powers made it difficult to address systemic weaknesses or hold member states accountable.

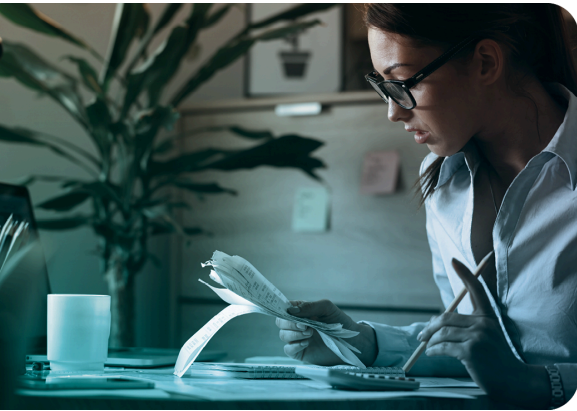
5. Regulatory momentum

The EU introduced several AML Directives, most recently the 5th and 6th AMLDs, to tighten regulations, but enforcement remained a challenge. Recognising the need for a centralised authority, the European Commission proposed the EU AMLA in 2021 as part of a comprehensive AML/CTF package. This package also included the creation of a single AML rulebook to unify standards across the EU.

6. Global reputation

The EU aimed to protect its financial system's integrity and maintain its global reputation as a trusted economic bloc. Addressing AML/CTF weaknesses was critical for ensuring confidence among investors, businesses, and international partners.

Why was EU AMLA created?



Fragmentation and inconsistencies

Different member states had varying levels of resources, expertise and commitment to AML enforcement. This created loopholes for criminals and put legitimate businesses at a disadvantage.

High-profile scandals

High-value scandals revealed the inadequacy of national enforcement mechanisms. The Danske Bank scandal alone exposed over €200 billion in suspicious transactions flowing through its Estonian branch, largely due to weak oversight.

Weak cross-border coordination

Money laundering and terrorist financing are transnational crimes. The lack of a centralised body made it difficult to tackle cross-border cases effectively.

Reputational risk

The EU's global reputation was at stake. Its financial system risked being perceived as vulnerable to illicit activities, undermining investor confidence.

The 5 challenges of EU AMLA

The journey to achieving an effective, centralised AML framework has not been a simple one. As AMLA seeks to unify and enhance AML efforts across member states, it faces a number of challenges. These include jurisdictional tensions between national governments and the centralised authority, questions about the agency's capacity to handle the scope of its mandate, delays in its implementation timeline, and the difficulty of balancing strict regulation with business interests. And then there's the transition from fragmented national laws to a harmonised EU rulebook that poses significant logistical and legal obstacles. Addressing these challenges will be critical to ensuring AMLA's success and bolstering the EU's resilience against money laundering and terrorist financing threats.

Challenge #1: Jurisdictions

Many EU member states view the centralised oversight by AMLA as a potential encroachment on their sovereignty. Financial crime enforcement has historically been closely tied to national jurisdiction, allowing governments to tailor their regulatory frameworks to local conditions. This decentralisation has been a source of tension in building consensus around AMLA's role, as some states fear losing control over their domestic financial institutions. Resistance from these member states may result in slower decision-making and could undermine the agency's authority in regions where national interests clash with AMLA's objectives.

Challenge #2: Scope

The EU's financial system is vast and complex, spanning thousands of institutions, varying regulatory cultures, and intricate cross-border financial activities. This raises questions about how AMLA will effectively manage its responsibilities. Concerns about the authority's capacity include whether it will have adequate staffing, technological resources, and funding to monitor, supervise, and enforce compliance across the bloc. Sceptics warn that an overburdened AMLA could lead to inefficiencies, such as delayed investigations or uneven enforcement, which would compromise its credibility and effectiveness.

Challenge #3: Implementation

Although AMLA was proposed in 2021, its full operational capability isn't expected until 2026. This creates an extended transitional period during which existing vulnerabilities in the EU's AML framework can be exploited. The long implementation process also risks eroding confidence in AMLA's ability to be effective. And, of course, the prolonged timeline gives bad actors opportunities to adapt and exploit regulatory loopholes, potentially undermining AMLA's impact once it does launch.



Challenge #4: Business interests

While the EU's goal is to implement stringent AML measures to combat financial crime, it does not want to stifle innovation. Businesses, in particular smaller ones, may find it difficult to drum up the resources to comply with more rigorous regulations. For the policymakers, the challenge is to develop regulations that both combat money laundering and still ensure a vibrant financial playing field for companies. Striking this balance is critical for businesses that are already dealing with economic and competitive pressures.

Challenge #5: Unified rules

One of AMLA's primary goals is to harmonise AML laws across the EU, creating a unified rulebook. Member states currently operate under a patchwork of national regulations, often reflecting unique legal, cultural and economic factors. Transitioning to a standardised framework involves logistical hurdles, such as training regulators, aligning enforcement mechanisms and amending entrenched national laws. Countries with established but distinct AML systems may resist adopting rules that could dilute their existing practices, creating friction and delaying the harmonisation process.

The establishment of EU AMLA

The European Commission's proposal for AMLA was part of a broader legislative package. Other elements of the legislation involved:

- A single AML rulebook to harmonise regulations across the EU
- Expanded requirements for due diligence and beneficial ownership transparency
- Enhanced coordination with non-EU countries

AMLA's primary roles include:

- Monitoring high-risk financial institutions across the EU
- Ensuring consistent enforcement of AML/CTF laws by national regulators
- Facilitating the exchange of information between national authorities, Europol and international bodies

Key features of EU AMLA

Directives and Regulations

The EU's approach to AML relies on a combination of directives and regulations to establish a robust legal framework.

Anti-Money Laundering Directives (AMLDs):

The EU has progressively introduced several AML Directives to combat money laundering and terrorist financing, with the 6th AML Directive (6AMLD) marking the most recent update. Adopted in December 2020, 6AMLD builds upon previous directives by expanding the scope of offenses, introducing tougher sanctions, and clarifying legal definitions. Directives set minimum standards for member states, requiring them to implement the rules into their national legal systems. However, the variability in transposition has sometimes led to inconsistent enforcement across the EU.

Regulations: Unlike directives, regulations are immediately enforceable in all EU member states without the need for national implementation. The upcoming EU AML Regulation is a key step toward harmonisation, aiming to eliminate discrepancies caused by varying interpretations of AML directives and ensuring a uniform legal framework. This regulation, alongside AMLA, seeks to provide consistent standards and enhanced oversight across the bloc.

Risk-based approach

The EU's AML framework emphasises a risk-based approach, requiring entities to tailor their efforts to the level and type of risks they face.

- Member states, financial institutions, and designated non-financial businesses and professions (DNFBPs) must assess risks based on specific factors such as customer profiles, geographic exposure, and transaction types.
- This approach ensures that resources are allocated proportionately, allowing for stricter controls in higher-risk areas (e.g., high-risk jurisdictions or politically exposed persons) while reducing burdens in lower-risk scenarios.
- The flexibility of the risk-based approach makes it adaptable but also demands that covered entities maintain robust risk assessment mechanisms and remain vigilant to evolving threats, such as those posed by virtual assets.

Obligations for covered entities

Entities subject to EU AML regulations are bound by stringent obligations aimed at preventing and detecting financial crimes:

Customer Due Diligence (CDD): Covered entities must implement Know Your Customer (KYC) procedures, identify beneficial ownership structures, and continuously monitor transactions to detect anomalies.

Reporting Suspicious Activity: Entities are required to submit Suspicious Transaction Reports (STRs) for activities that raise red flags, with the expectation that detailed transaction records be maintained for several years to aid investigations.

Enhanced Due Diligence (EDD): High-risk scenarios, such as dealings with politically exposed persons (PEPs) or clients from high-risk jurisdictions, mandate additional scrutiny, including verifying the source of funds or conducting deeper background checks.

Beneficial ownership registers

Enhancing transparency in financial dealings is a central pillar of the EU's AML strategy:

- Member states must establish centralised registers of beneficial ownership for corporate entities and trusts. These registers are designed to expose the true owners behind complex corporate structures, reducing opportunities for anonymity that facilitate financial crimes.
- While public access to these registers was initially mandated, legal challenges—such as the 2022 ruling by the European Court of Justice (ECJ) on privacy grounds—have resulted in adjustments, limiting access to certain stakeholders like competent authorities and entities with a legitimate interest. Balancing transparency with privacy rights remains a contentious issue.

Focus on virtual assets

As virtual assets gain prominence, the EU has expanded its AML framework to include Virtual Asset Service Providers (VASPs):

- Under the 5th and 6th AMLDs, VASPs are subject to the same obligations as traditional financial institutions, including CDD and reporting suspicious transactions.
- Recognising the unique risks of virtual assets, such as anonymity and cross-border transferability, the EU has sought to integrate these entities into its broader AML strategy while promoting innovation in the fintech space.
- Efforts like the Markets in Crypto-Assets Regulation (MiCA) aim to further regulate this emerging sector.

Sanctions and penalties

A uniform system of sanctions and penalties is critical to ensuring compliance across the EU:

- Non-compliance with AML obligations can result in severe consequences, including significant fines, loss of operating licenses, and reputational damage.
- Criminal sanctions under the 6AMLD hold both individuals and entities accountable, reinforcing the EU's commitment to deterring financial crime. Harmonising penalties across member states also reduces opportunities for regulatory arbitrage, where entities exploit less stringent jurisdictions.



What does EU AMLA mean for EU and UK companies?

For both EU and UK companies, the evolving regulatory landscape shaped by EU AMLA requires understanding and navigation. With AMLA's centralised framework hoping to harmonise AML efforts, businesses must adapt to ensure compliance, mitigate risks and avoid fines.



EU companies

Increased scrutiny

AMLA's direct supervision of high-risk sectors and cross-border operations indicates a more intensive focus on businesses operating in industries vulnerable to money laundering or terrorist financing. Specifically, this includes financial services, real estate and virtual asset providers.

Companies in these sectors may experience more frequent audits, on-site inspections and closer monitoring of their AML compliance frameworks. Businesses will need to be prepared to demonstrate compliance and address any deficiencies promptly.

Enhanced reporting obligations

EU companies are required to ensure timely, accurate, and detailed reporting of suspicious transactions to their Financial Intelligence Units (FIUs).

Compliance with beneficial ownership transparency requirements is critical. This includes keeping accurate and up-to-date records of beneficial owners in centralised registers, even as accessibility rules evolve. Non-compliance could result in significant fines or reputational damage.

Risk-based approach

Obligated entities will need to adopt a risk-based approach to identify, assess and mitigate risks associated with their operations.

This requires robust internal controls, ongoing risk assessments and the use of technology tools such as transaction monitoring systems and AI to detect and prevent suspicious activities. Firms will need to be aware of evolving threats, specifically in high-risk areas like cross-border transactions and virtual assets.

Staff training

Regular training on AML and CTF compliance is essential. Employees, particularly those in compliance, legal and finance roles, need to stay informed about the latest regulatory updates and red flags for financial crime.

Companies should establish mandatory training programs to build awareness, ensure adherence to internal policies and empower staff to identify and report suspicious activities effectively.



UK companies

While the UK is not a member of the EU, EU AML has an impact on its businesses. Companies with EU-facing operations or clients must align with the new framework to maintain compliance and ensure smooth operations in the EU market.

Cross-border compliance

UK firms with subsidiaries, branches or clients in the EU must implement compliance measures that align with AMLA. This includes stricter customer due diligence (CDD) and enhanced due diligence (EDD) requirements for high-risk transactions involving EU entities.

Non-compliance could lead to operational disruptions, reputational harm or penalties, making it critical for UK companies to maintain comprehensive AML policies across their EU-facing operations.

Collaboration with EU regulators

Strong communication channels with EU regulators and FIUs are essential to facilitate compliance and ensure a smooth exchange of information.

UK companies must be proactive in cooperating with EU supervisory authorities, particularly for cross-border investigations, reporting obligations and requests for beneficial ownership information. Establishing clear points of contact and robust processes for handling regulatory inquiries will be key.

Third-country equivalence

Post-Brexit, the UK is considered a "third country" by the EU. This means that UK companies are required to monitor third-country equivalence assessments closely, ensuring they meet the EU's standards for regulatory cooperation and AML compliance.

UK businesses must stay informed about any changes to their equivalence status and adjust their compliance frameworks accordingly to maintain seamless operations within the EU.

Getting ready for AMLA

EU AMLA provides both challenges and opportunities for businesses operating within or engaging with the EU. While increased regulatory scrutiny and evolving requirements may place additional burdens on companies, proactive compliance efforts will not only mitigate risks but could also enhance credibility in the global marketplace. In either case, the authority represents a significant shift in how financial crime is addressed in the EU. Businesses, particularly those operating in high-risk sectors or cross-border environments, will need to adapt. What can companies do to prepare for AMLA?

Conduct a gap analysis

This will identify shortcomings in existing AML and CTF measures compared to AMLA's requirements.

- Review current policies, procedures and controls to assess their alignment with AMLA's unified rulebook.
- Identify areas where compliance falls short, such as CDD, transaction monitoring or reporting suspicious activity.
- Benchmark practices against AMLA standards, which emphasise harmonisation and stricter enforcement across the EU.

The gap analysis will provide a roadmap for addressing deficiencies and implementing targeted improvements before AMLA supervision begins.

Implement policies

AMLA introduces a unified AML framework that eliminates inconsistencies between national regulations, requiring companies to adopt standardised policies.

- Update AML/CTF policies to reflect AMLA's focus on high-risk sectors, cross-border transactions and beneficial ownership transparency.
- Ensure policies include clear guidelines for employee responsibilities, escalation procedures for suspicious activities and risk management practices.
- Regularly review and revise policies to account for emerging threats and regulatory updates.

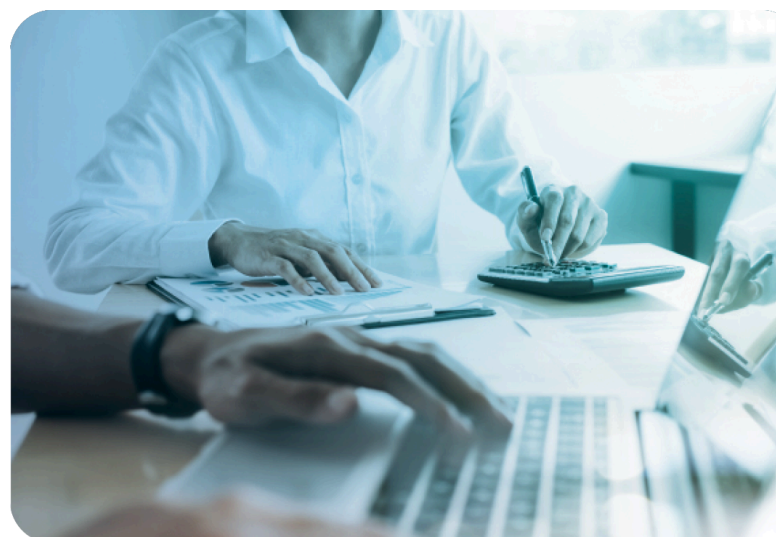
Clear AMLA-compliant policies will help mitigate risks and demonstrate a company's commitment to regulatory adherence.

Enhanced Due Diligence

CDD processes are central to AML compliance. Companies must strengthen these processes to address higher transparency and risk management standards.

- Implement EDD measures for high-risk customers, such as politically exposed persons (PEPs) or clients from high-risk jurisdictions.
- Verify beneficial ownership information to ensure compliance with AMLA's transparency requirements.
- Integrate continuous monitoring to identify unusual or suspicious behaviour over the lifecycle of customer relationships.

EDD processes will ensure compliance with AMLA's focus on identifying and mitigating risks associated with complex ownership structures and high-risk entities.



Leverage technology

Technology plays a critical role in ensuring effective and efficient compliance with AML requirements. AMLA encourages the use of innovative solutions to strengthen financial crime prevention efforts.

- Invest in advanced transaction monitoring systems capable of identifying unusual patterns or high-risk transactions in real-time.
- Leverage AI tools to enhance risk assessment, fraud detection and predictive analytics.
- Utilise regulatory technology platforms to automate reporting and streamline compliance workflows.

By leveraging technology, companies can increase efficiency, reduce manual errors and ensure timely compliance with AMLA's stringent requirements.

Engage experts

Navigating AMLA's unified rulebook can be complex. Engaging legal and compliance professionals ensures companies are adequately prepared.

- Consult legal experts familiar with AMLA to interpret regulatory requirements and their impact on specific business operations.
- Engage external consultants to conduct independent audits and validate the effectiveness of AML measures.
- Provide staff training with the support of AML/CTF professionals to build awareness and improve compliance culture.

Expert guidance will help businesses navigate the complexities of AMLA, minimise compliance risks and strengthen their overall AML framework.

Monitor developments

Businesses must stay informed about regulatory updates and emerging trends in financial crime.

- Subscribe to updates from the European Commission, AMLA and other relevant bodies to track regulatory developments.
- Participate in industry forums, seminars and webinars to gain insights into best practices and compliance strategies.
- Establish an internal team or designate personnel responsible for monitoring changes and adapting company policies accordingly.

Proactively monitoring developments will enable companies to anticipate regulatory changes and maintain compliance with AMLA's evolving framework.

The cases that mattered:

What led to EU AMLA

The Danske Bank scandal



Danske Bank

The Danske Bank Scandal is one of the largest money laundering cases in European history, involving the suspicious movement of approximately €200 billion through the

bank's Estonian branch. The scandal exposed significant gaps in the EU's AML framework, highlighting the challenges of fragmented national oversight and regulatory enforcement.

What happened?

Danske Bank, Denmark's largest financial institution, operated in multiple countries. Between 2007 and 2015, the bank's Estonian branch facilitated the movement of vast sums of illicit funds, much of it originating from Russia and other former Soviet states. These funds passed through non-resident accounts held by foreign customers, often without proper due diligence or effective controls to detect suspicious activity.

There is a lot of blame to go around in this scandal but the main actors included clients, many of whom were from high-risk jurisdictions, particularly Russia, with complex ownership structures that obscured the origins of the funds. And then there's internal management. Whistleblower testimony and internal audits revealed that senior executives at Danske Bank were aware of the risks but failed to take sufficient action. And finally Estonian regulators, who ignored red flags and early warning signs

and didn't prevent the scandal from happening or adequately address it as it unfolded.

The scandal came to light in 2017 when Howard Wilkinson, a former employee of Danske Bank, alerted Danish authorities to suspicious transactions at the Estonian branch. His reports revealed systematic failures in the bank's compliance framework and a disregard for AML obligations.

Subsequent investigations, including an internal probe by Danske Bank and reports by regulators, revealed several alarming details:

- Over €200 billion in potentially illicit funds flowed through the Estonian branch between 2007 and 2015.
- Many accounts belonged to shell companies or had unclear beneficial ownership.
- The bank ignored multiple internal and external warnings about inadequate AML controls.

The scandal underscored weaknesses in the EU's AML system. Danske Bank's operations in Estonia were primarily overseen by Estonian regulators, with little coordination or intervention from Danish authorities or the European Central Bank. This fragmented approach allowed the bank to exploit jurisdictional gaps.

The revelations sparked outrage across Europe, with widespread calls for stronger regulatory oversight and accountability. Danske Bank faced significant reputational damage, with top executives resigning and its stock value plummeting. The scandal also resulted in investigations by authorities in Denmark, Estonia, the US and the UK.

What was learned

The scandal highlighted the challenges of decentralised AML enforcement in the EU, where national regulators have primary responsibility for oversight. This system created inconsistencies and allowed institutions like Danske Bank to exploit regulatory arbitrage.

It also pointed to weaknesses in cross-border coordination, despite the very cross-border nature of money laundering. EU member states often failed to share information or coordinate effectively. This lack of cooperation hindered early detection and enforcement.

The lack of a centralised authority also allowed regulatory failures to persist without clear accountability. Both Danish and Estonian regulators were criticised for their inaction, but no unified entity existed to address such lapses at the EU level.

Impact on EU AML policy

The Danske Bank scandal served as a wake-up call for the EU, exposing the urgent need for reform in its AML framework. In the aftermath of the scandal, the EU adopted the 5th and 6th Anti-Money Laundering Directives (AMLDs), which introduced stricter requirements for beneficial ownership transparency, expanded the scope of covered entities, and clarified legal definitions for money laundering offenses.

The scandal also underscored the importance of tracking the true ownership of corporate entities. The EU introduced measures to enhance the accessibility and accuracy of beneficial ownership registers, although recent legal challenges have raised questions about public access.

The case demonstrated the need for stricter sanctions to deter non-compliance. Under the 6th AMLD and AMLA's framework, penalties for AML violations have been standardised and significantly increased.

The Danske Bank scandal was a pivotal moment in European financial history, exposing deep flaws in the EU's AML framework and prompting widespread calls for reform. The scandal directly influenced the creation of the EU AMLA.

The Swedbank scandal



The Swedbank money laundering scandal exposed systemic failures in one of Sweden's largest financial institutions and revealed the vulnerabilities of cross-border money

laundering within the European Union. The scandal, involving the movement of at least €37 billion in suspicious transactions through the bank's Baltic operations demonstrated the need for a centralised EU-wide AML authority.

What happened?

Swedbank, headquartered in Stockholm, Sweden, is one of the largest banks in Northern Europe, with extensive operations in the Baltic region. Between 2010 and 2016, the Baltic branches became conduits for suspicious transactions involving non-resident clients, many of whom originated from Russia and other former Soviet states. These transactions raised serious concerns about money laundering, tax evasion and other financial crimes.

The scandal came to light in 2019 following investigative reporting by Sweden's SVT (Sveriges Television), which revealed that Swedbank had processed billions of euros in questionable transactions, often tied to offshore entities and high-risk jurisdictions. SVT's report detailed how Swedbank's Baltic branches had processed €37 billion in suspicious transactions. The report revealed that Swedbank's involvement in cross-border transactions were linked to shell companies with opaque ownership structures. It also demonstrated how the scandal had ties to the infamous Russian "laundromat" schemes, which funnelled illicit funds through European banks. Significantly, it highlighted the failures in due diligence, including inadequate

customer identification and monitoring processes.

The revelations sparked regulatory scrutiny, criminal investigations, and a public outcry, undermining trust in Swedbank and exposing broader flaws in the EU's AML framework.

The fallout

The scandal triggered a wave of investigations and enforcement actions across multiple jurisdictions:

- **Swedish Financial Supervisory Authority (FSA):** The Swedish FSA fined Swedbank €360 million in 2020 for serious deficiencies in its AML controls and management oversight.
- **Estonian and Latvian Regulators:** Authorities in the Baltic states criticised Swedbank's local branches for their role in facilitating illicit transactions and imposed stricter regulatory scrutiny.
- **US Authorities:** Swedbank faced investigations by the US DoJ and the Treasury's Financial Crimes Enforcement Network (FinCEN) due to the involvement of US dollars in the suspicious transactions.

The scandal also revealed a lack of accountability and oversight at the senior management level. It was noted that internal warnings about high-risk non-resident clients were ignored or inadequately addressed. The bank was found to have prioritised profits from its lucrative non-resident business in the Baltics over compliance with AML regulations. And then there was the board and executives, who were accused of failing to provide sufficient resources for AML compliance programs.

Lessons learned

The Swedbank scandal highlighted the challenges of regulating cross-border financial activities within the EU. Like Danske Bank, Swedbank operated under the jurisdiction of multiple national regulators, leading to fragmented oversight and inconsistent enforcement.

Swedbank's Baltic operations demonstrated significant failings in AML compliance, including poor CDD, weak transaction monitoring systems, and insufficient reporting of suspicious transactions. These failings allowed high-risk clients to exploit the bank for years without detection.

The scandal also exposed how banks operating in multiple jurisdictions could exploit regulatory gaps, particularly in smaller countries with limited resources for AML enforcement. Swedbank's Estonian and Latvian branches operated with minimal scrutiny, despite being critical nodes in the bank's cross-border operations.

The Swedbank scandal, following closely on the heels of the Danske Bank scandal, reinforced the need for comprehensive reform of the EU's AML framework. The case underscored the systemic vulnerabilities within the existing system and provided further impetus for the creation of AMLA.

The Swedbank scandal, alongside the Danske Bank scandal, underscored the need for a centralised authority to oversee AML efforts and ensure consistent application of rules across member states.

The Deutsche Bank scandal



Deutsche Bank

Deutsche Bank, one of the largest financial institutions in Europe, has faced multiple scandals involving money laundering and financial crimes over the years. Among the most

notable was its involvement in the "Russian Laundromat" scheme, which funnelled billions of dollars through illicit transactions. These incidents exposed significant shortcomings in the bank's AML controls and highlighted systemic vulnerabilities within the EU's regulatory framework.

What happened?

Deutsche Bank was implicated in two key scandals. One is known as the Russian laundromat scheme which took place from 2011 through 2015. The scheme involved the laundering of over \$10 billion from Russia through Deutsche Bank's Moscow, London and New York branches. The funds were funnelled using "mirror trades," where securities were bought in rubles in Moscow and simultaneously sold in US dollars in London to offshore entities.

The other scandal was the correspondent banking relationship scheme that took place between 2007 and 2015. Here, Deutsche Bank served as a correspondent bank for Danske Bank's Estonian branch, which was at the centre of a €200 billion money laundering scandal. Deutsche Bank failed to adequately monitor the suspicious flows of funds it processed on behalf of Danske Bank.

These cases highlighted the bank's systemic AML deficiencies, including weak transaction monitoring, poor internal controls, and a lack of accountability at the management level.

Key failures

The Russian laundromat scheme involved clients using Deutsche Bank's Moscow branch to execute trades that had no economic rationale but were designed to move money out of Russia covertly. Deutsche Bank's compliance systems did not flag the unusual trading volumes and patterns, which should have raised red flags. The bank also failed to verify the ultimate beneficial owners of the shell companies involved in the transactions and it exploited gaps in cross-border regulatory oversight, particularly between Russia, the UK, and the US.

As a correspondent bank for Danske Bank, Deutsche Bank processed billions of dollars in suspicious transactions from Danske's Estonian branch. In that case, Deutsche Bank did not adequately monitor high-risk transactions originating from Estonia, despite known concerns about Danske Bank's operations. The bank's internal reporting mechanisms also failed to escalate concerns to senior management or regulators in a timely manner.

Deutsche Bank's senior executives were criticised for prioritising profits over compliance, particularly in high-risk markets like Russia. Internal audits and whistleblower reports warning of deficiencies were often ignored or inadequately addressed.

The fallout

Deutsche Bank faced significant financial penalties for its involvement in money laundering:

- In 2017, the US and UK regulators fined the bank \$630 million for its role in the Russian mirror trading scheme.
- Deutsche Bank paid additional fines for its correspondent banking failures and other AML violations, totalling over \$1 billion globally.

The repeated scandals severely damaged Deutsche Bank's reputation, leading to increased regulatory scrutiny of its operations worldwide and a loss of trust among clients, investors, and the general public.

Lessons learned

The Deutsche Bank scandal highlighted the challenges of fragmented regulatory oversight within the EU. The bank operated across multiple jurisdictions, each with different AML enforcement standards, allowing it to exploit gaps in supervision.

It also demonstrated the lack of effective communication and coordination between national regulators, particularly in cases involving cross-border transactions, hindered the detection and prevention of money laundering.

Finally, the scandal demonstrated the need for robust internal controls, including effective transaction monitoring systems, enhanced due diligence for high-risk clients, and accountability at the senior management level.

The Deutsche Bank scandal reinforced the urgent need for a centralised authority to oversee AML efforts and ensure consistent enforcement across member states. The establishment of AMLA represents a significant step forward in addressing the systemic weaknesses revealed by the scandal.

How VinciWorks can help

Training your staff in anti-money laundering needs to be more than a tick-box exercise. Companies and law firms can easily fall out of compliance or get caught up in dirty money without a robust AML framework. Packed with realistic scenarios, real-life case studies and customisation options, our suite of AML courses will help you stay protected.

<https://vinciworks.com/courses/aml/>

Legal compliance suite

Compliance challenges are mounting. Law firms can be fighting multiple fires all at once. Omnitrack, the most widely used compliance workflow solution by law firms, is here to help. Our Legal Compliance Suite provides risk and compliance teams with one centralised portal to manage all of their critical compliance processes. Designed together with leading law firms, the platform can seamlessly adapt to each firm's specific workflow with customised reporting. Forget spreadsheets, manual processes, and inflexible reporting: stress-free legal compliance is here.

Your compliance challenges, solved

- 18 best practice forms & workflow templates
- Intuitive form builder for process customisation
- Conditional logic, automated reminders & custom reporting
- Audit trail & SRA compliance
- Implementation support & admin training

[Learn more](#)

eLearning Courses

VinciWorks makes compliance training and eLearning that works. Available in every language you speak. Built by us. *Ready for you.*

[Anti-Money Laundering Course](#)

About Us

We believe compliance enables business. Compliance is an opportunity to be one step ahead, so your organisation can focus on advancing the business.

For over 20 years, VinciWorks has been at the leading edge of re-envisioning compliance tools and training. Our creative and driven team works hard everyday, challenging the traditional compliance industry to become forward-thinking, interactive and engaging. From our vast library of 800+ courses, to the award-winning Omnitrack training and compliance management software, to a curated catalogue of world class resources, VinciWorks is here to support your organisation every step of the way.

We constantly have our finger on the pulse, being the first to adapt our products to new regulations and market changes that impact our customers' businesses. Our flexible solutions ensure that every one of our products is tailored to our customers' unique business needs, placing them at the heart of everything we do.



 www.vinciworks.com

 enquiries@vinciworks.com