Global Laundering Networks: The Architecture of Illicit Finance

An Interdisciplinary Analysis Across Financial, Behavioural, Legal, and Cyber Dimensions

Corresponding author: Aleksandra Kostanecka
Email: aleksandra.kostanecka@studbocconi.it

Abstract

Global laundering networks represent the most complex and resilient threats to financial integrity, democratic governance, and global security. Despite decades of international anti-money laundering initiatives, illicit financial flows persist via sophisticated multidimensional systems. Through an interdisciplinary qualitative analysis, this paper integrates key insights from behavioural psychology, law, cybersecurity, and financial forensics. Case study analysis and the use of academic research and investigative journalism provide bases for comparison across domains in the identification of recurrent structural and cognitive patterns. The paper proposes a new conceptual framework, the *Four-Pillar Money Laundering Model*, which stipulates that corruption is enabled through behavioural normalisation, shielded through legal fragmentation, veiled through cyber opacity, and legitimised through financial engineering. By synthesising cross-domain insights, this research provides a holistic view of global laundering dynamics and underscores the systemic interdependence enabling illicit capital to persist despite current enforcement efforts.

Keywords: money laundering; transnational financial crime; behavioral normalization; legal loopholes; cyber concealment; financial engineering; interdisciplinary research

Authors and Affiliations: Aleksandra Kostanecka with contributions from Simona Anzani[1], Maria Bozalo[1], Silvia Brancorsini[2], Luís Bueno[2], Sofia Bulycheva[4], Mateo Cristian[1], Livia De Guillebon[3], Maria Englert[1], Katherine Hanna[2], Maël Lejay[1], Salvatore Lorito[4], Giovanni Mangiatordi[1], Giulia Mastursi[3], Giacomo Mensi[2], Federico Moseley[4], Hiba Moumni[3], Nidal Oğur[4], Evelina Pîntea[2], Zoe Mejia-Ricart[2], Lorenzo Russo[3], Francesco Tasso[1]

[1]Financial Perspective, [2]Behavioural Perspective, [3]Legal Perspective, [4]Cybersecurity Perspective

November 2025 | Institutional Affiliation: Bocconi University, Milan, Italy

1 Introduction

1.1 Context and Significance

Global laundering networks are transnational systems that move, conceal and reintegrate illicit wealth. These networks often operate like structured organisations, with leaders, strategists, and executors who manage funds, set commissions, and ensure the smooth operation of their illegal activities across financial, legal, cyber, and social domains. Money laundering has developed into a systemic threat to global economic and political stability, rendering its study and mitigation increasingly indispensable. Estimates consistently indicate that between 2% and 5% of global GDP is laundered each year, equivalent to roughly USD 800 billion to USD 2 trillion, moving through opaque networks that erode the integrity of the global financial system (UNODC, n.d.). For instance, the Panama Papers leak (2016) exposed over 11.5 million documents containing information about more than 214,000 offshore entities that were used to hide assets for politicians, multinational corporations, and criminal organisations (Obermayer et al., n.d.). Similarly, the 1MDB scandal provides a clear illustration of state-level laundering: more than USD 4.5 billion was stolen from Malaysia's sovereign wealth fund and funnelled through a transnational web of shell companies, banks, and intermediaries across the United States, Switzerland, Singapore, and the Middle East (Jones, 2020).

1.2 Research Problem and Gap

Despite decades of AML frameworks, money laundering remains a persistent and evolving challenge. Criminal networks adapt rapidly, exploiting legal loopholes and weak enforcement mechanisms, particularly with the rise of increasingly sophisticated digital technologies. Moreover, existing AML tools often detect abuse only after it has occurred, prioritising damage control rather than proactive identification and prevention. Academic research, meanwhile, tends to frame money laundering primarily as a financial or legal phenomenon, with behavioural dimensions rarely examined and cyber components typically analysed in isolation. Consequently, there is limited work that conceptualises laundering as an interconnected system in which financial, legal, cybersecurity, and behavioural factors mutually reinforce one

another. This gap constrains a comprehensive understanding of how contemporary laundering networks operate, persist, and evolve.

1.3 Aim and Research Question

This paper examines how global laundering networks function as transnational systems maintained by behavioural normalisation, legal loopholes, cyber opacity, and financial complexity. It aims to analyse beyond purely financial and legal interpretations and offer an interdisciplinary explanation of how these laundering networks persist. The central research question, therefore, examines how these four dimensions interact to sustain laundering networks despite extensive AML regulations.

1.4 Methodology

This paper is based on qualitative and interdisciplinary research, combining four key perspectives: behavioural, legal, cyber, and financial. Since financial crime is not limited to a single domain, an interdisciplinary approach allows the study to capture the full ecosystem in which money laundering occurs. Each dimension examines money laundering events through its own lens, extracting commonalities, hypotheses, and differences.

Within the analysis of each discipline, three main case studies will be used and referenced: 1MDB, Danske Bank, and the Panama Papers. These specific cases were selected to ensure triangulation, with multiple and independent perspectives evidencing the same clear underlying patterns. The paper uses comparative analysis across the cases to identify recurring structures and weaknesses, and synthesise them into broader conceptual theories.

The study relies exclusively on credible, verifiable, and publicly accessible academic and institutional sources. Among these are extracts from the Financial Action Task Force (FATF), United Nations Office on Drugs and Crime (UNODC), and Transparency International.

1.5 Contribution to Literature and Paper Structure

The paper's primary contribution is the creation of a new interdisciplinary framework for understanding transnational laundering: the *Four-Pillar Money Laundering Model*. It aims to reframe money laundering as a systemic and adaptive phenomenon, sustained by

combining behavioural incentives, legal loopholes, technological concealment, and financial engineering. The study moves away from viewing laundering networks as merely financial crimes, but as multidimensional governance failures, with psychological factors being rarely explored in such crime analysis. Highlighting the human aspects, such as moral disengagement and cultural normalisation, grants a more holistic perspective as to why the phenomenon occurs, and helps identify potential money laundering schemes before they occur. This study lays the groundwork for cross-disciplinary policymaking, establishing a framework that can be replicated in other global cases and national anti-money-laundering (AML) systems.

The remainder of this paper is organised into three core sections: the main body, the integrative discussion, and the conclusion. The main body encompasses four disciplinary areas. The first area dissects financial mechanisms, detailing how illicit funds are placed, layered, and integrated into the legitimate economy. The second area explores the behavioural drivers behind money laundering, including key psychological drivers with reference to the *Fraud Triangle*, moral disengagement, and the normalisation of corruption within elite and institutional settings. The following area examines legal loopholes and systemic weaknesses that enable laundering, with a specific focus on Italian regulation, to illustrate how international laws and efforts apply in focused national settings. The final area analyses cyber concealment, showing how digital technologies, encryption, and open-source intelligence (OSINT) both facilitate and expose laundering networks. The integrative section brings together findings from all four domains to introduce the *Four-Pillar Money Laundering Model*, illustrating how behavioural normalisation, legal gaps, cyber opacity, and financial complexity reinforce one another. Lastly, the conclusion summarises key insights, presents the framework as the paper's contribution to knowledge creation, and discusses potential policy or reform suggestions for improving transparency, accountability, and cross-border enforcement. The conclusion also considers how the issue may evolve with the emergence of new technologies.

2 The Financial Architecture of Global Laundering Networks

2.1 Introduction and the Stages of Money Laundering

"The estimated amount of money laundered globally is 2-5% of global GDP, or $800 billion-$2 trillion in current US dollars" (UNODC, n.d.). These figures illustrate the

substantial economic impact of criminal activity and the difficulties regulators face in addressing increasingly complex laundering networks. Given the magnitude of illicit capital flowing through global markets, most individuals likely have handled funds unknowingly linked to money laundering. This paper examines the three-phase model that emerged in late-20th-century AML literature as a systematic framework for transforming "black money" into legitimate assets (Saliya, 2025).

Placement is the initial phase in which funds from criminal activities are introduced into the financial system, disguised as legitimate income. This is the most vulnerable stage, as it involves moving large sums of cash without raising AML suspicions. In the UK, for example, transfers over £3,000 fall under closer scrutiny and may require filing a "Defence Against Money Laundering Suspicious Activity Report" (UK Government, 2025). Common placement methods include smurfing, where large sums are divided into smaller deposits to avoid reporting thresholds (Fragoso, 2012); cash-intensive businesses such as casinos or restaurants used to mix illicit proceeds with legitimate revenue; cash purchases of high-value art or gold for resale; monetary instruments such as cashier's checks purchased under reporting limits; digital currencies purchased anonymously; and cross-border cash smuggling (AML Network, 2025).

Once illicit funds enter the financial system, they remain traceable unless further concealed. The layering phase disguises their origin through transactions that sever the link between the money and its criminal source. Offenders employ increasingly sophisticated methods, many of which go undetected due to limited reporting and enforcement capacity. Layering schemes often overlap, but four principal methods are typically observed:

International transfers: International transfers exploit disparities between national AML regimes despite calls for stronger international cooperation by the Financial Action Task Force (FATF, 2025). They involve fast multi-bank, multi-account, and multi-jurisdictional movements, making coordination particularly difficult and often overburdening investigative resources.

Shell companies: Shell companies are formed to conceal assets and exist only on paper. Typically incorporated in jurisdictions with strict privacy laws such as Switzerland, they "have no employees, do not engage in significant commercial activities, and rarely generate revenues" (AML Network, 2025, para. 3). Circular transactions and false invoicing mask beneficial ownership, making tracing difficult, which is further explored in the following chapter.

Cryptocurrencies: Because blockchain systems rely on pseudonymous rather than verified identities, they provide an initial layer of obscurity. Privacy-focused coins combined with mixing, which uses software to pool and redistribute cryptocurrency transactions, and chain-hopping, described as the rapid movement between different cryptocurrencies and blockchains, make tracing illicit flows exceedingly difficult (Liang et al., 2025).

Investments: High-value assets such as art, commodities, and securities are frequently used to disguise origins and may even yield returns. Criminals exploit the subjective valuation and anonymity of art markets, reselling works or holding them through shell companies to further complicate detection (Financial Crime Academy, 2025).

Integration is the final stage, returning laundered funds to the legitimate economy through credible accounts of lawful origin. At this point, illicit flows are virtually indistinguishable from legitimate ones, allowing offenders to freely use their assets. Common techniques include fictitious or inflated import-export operations, often conducted by shell companies or affiliated entities to make illicit proceeds appear as ordinary business revenue (Gilmour, 2024). Another method involves pre-arranged financial structures such as interest-free loans, loan-back schemes, and boomerang transactions that create sham money flows within normal business operations. The luxury market also plays a major role: high-end assets bought during or after the layering stage allow offenders to justify future income upon liquidation. Finally, offenders often reinvest illicit proceeds into legitimate businesses, directly or through complex ownership chains (OMNIO, 2024), declaring dividends or profits from sales as lawful income and completing the laundering cycle.

Although the three stages of money laundering described provide meaningful material for academic and training purposes, there is no consensus among scholars on its practical application (Cassella, 2018). By focusing solely on how dirty money is laundered, limitations appear in mitigating the techniques involved. The model does not issue in-depth information regarding “who” is perpetrating money laundering, which “limits the scope of both the money laundering statutes and the training of law enforcement agents to only a small part of the money laundering problem” (Casella, 2018, p. 495).

The second hindrance relies on its systemic approach. Real cases have shown that money laundering may be more complex than only placement, layering, and integration. In events such as Ponzi and pyramid schemes, illicit funds are already well-integrated into the financial system. Even though none of the three stages are involved, the process by which perpetrators maintain their fraudulent practice can be understood as a form of money laundering.

In an alleviation attempt, a more holistic perspective should be taken. Not all illicit proceeds are generated with laundering objectives: criminals regularly utilise cash for salary payments, bribery purposes, or other transactions deemed relevant for keeping activities running. Nevertheless, the 1980s model remains pertinent in apprehending typical structured money laundering practices and common financial strategies at a global scale.

2.2 Role of Correspondent Banking, Shell Companies, Offshore Havens, and Real Estate in Money Laundering

Most money laundering involves moving funds across borders to shield illicit proceeds from the jurisdiction and prosecution of the country where the offence occurred (Dupire, 2025). Converting these funds into the world's major currencies and investing them in stocks, real estate, or bank accounts obscures their origin and provides an additional layer of legal protection.

In most countries, a foreign bank must establish a domestic branch to operate, which can be costly when the customer base or transaction volume is limited (Dupire, 2025). To overcome this, banks rely on correspondent banking relationships. Correspondent banking is an arrangement in which one bank (the correspondent) provides services such as wire transfers, foreign exchange, and trade finance to another bank (the respondent), enabling access to foreign markets (European Bank for Reconstruction and Development, 2024). It benefits the respondent because the correspondent manages compliance, knows local regulations, and liaises with domestic authorities (Dupire, 2025).

Shell companies are a common vehicle for moving criminal funds. These entities, often privately held firms or trusts with no physical presence beyond a mailing address, can have legitimate purposes such as holding assets (Financial Crime Academy, 2025). However, they are frequently misused and display red flags when involved in financial crime: no active operations, minimal assets, and registration in jurisdictions with strict privacy laws. These companies create opaque ownership structures that conceal the identities of ultimate beneficial owners (UBOs) who profit from the transactions (Aliprandi et al., 2023). By establishing long, cross-border transaction chains, they overwhelm investigators and obscure the money trail. Often incorporated in multiple jurisdictions with varying regulations, they complicate investigations that require foreign cooperation, sometimes in states vulnerable to corruption (Red Flag Alert, 2023). Within the money-laundering process, shell corporations are a core component of the layering stage and are particularly prevalent in tax havens.

Tax havens are jurisdictions with zero or very low tax rates and favourable conditions that attract non-resident entities seeking to transfer assets and avoid home-country regulations. Strict financial privacy laws guarantee anonymity, making these jurisdictions attractive destinations for funds derived from corruption or conflict financing (Sabatino, 2020).

Lastly, real estate remains one of the oldest and most persistent channels for laundering illicit proceeds. Its stable value and potential for personal or rental use make it attractive, while property transactions lend an appearance of legitimacy and facilitate large monetary transfers - key characteristics of the integration stage. Although transactions are mainly related to residential and commercial real estate, any form of immovable property can be used. Indicators of potential money laundering in real estate include a mismatch between the buyer's income and the property's value; use of shell companies or trusts to ensure anonymity; under- or over-valued pricing; significant distance between buyer and property location; and lack of interest from the buyer, such as purchasing without viewing (Remeur, 2019).

Indices such as the Financial Secrecy Index help assess countries' attractiveness for money laundering by ranking their role in facilitating financial secrecy. The index combines two measures: a Secrecy Score, reflecting the extent of legal confidentiality, and a Global Scale Weight, showing the volume of financial services offered to non-residents. As of 2025, the United States ranks first, followed by Switzerland, Singapore, Hong Kong, and Luxembourg (Financial Secrecy Index, n.d.).

2.3 How Cartels, Corporations, and Political Elites use the same Global Mechanisms

Although motivations and scales differ - profit, political power, or market control - the same financial mechanisms recur across cartels, corporations, and political elites: offshore accounts, shell companies, complex transactions, and investment in legitimate assets such as real estate or foreign currencies (Isolauri & Ameer, 2023). Legal institutions and professionals may also manipulate systems or legislation, directly or indirectly, facilitating money laundering (Europol, 2021). Despite differing identities, cartels, corporations, and political elites share one financial goal: converting uncertain money into enduring power through similar financial tactics. The global illegal drugs trade, valued at roughly half a trillion USD annually, illustrates this dynamic. Money laundering secures political and personal power while influencing democratic and transitional states. Diverted public funds and illicit donations are recycled through offshore companies or campaign finance loopholes - a form of "political money laundering" whereby dark money enters democratic systems under the guise of legitimate contributions, weakening

accountability and undermining governance (Barnett & Sloan, 2018). Each group exploits the same loopholes in global finance, blurring distinctions between organised crime, corporate misconduct, and state corruption. The placement-layering-integration cycle thus functions as a universal template.

Cartels place illicit cash through front businesses or direct currency smuggling. While cases such as Wachovia and HSBC exposed large-scale laundering, the majority of proceeds circulate through cash-intensive enterprises - bars, clubs, gyms, restaurants, and construction firms - where oversight is limited (Berry & Gundur, 2025). Layering occurs via multiple accounts, shell entities, and cryptocurrency exchanges that obscure fund origins (Carabaña, 2025). Integration follows through investment in legitimate sectors, a process illustrated by TD Bank's USD 3 billion fine for facilitating drug-money transfers (Berry & Gundur, 2025).

Corporations employ the same sequence through legal mechanisms: placement via trade mispricing or fictitious invoicing, layering through subsidiaries and offshore entities often managed by firms exposed in the Panama Papers, and integration through profits booked in low-tax jurisdictions and returned as dividends or share buybacks. The Danske Bank case illustrates how corporate structures enabled large-scale laundering through opaque clients in its Estonian branch (Winkler, 2024). Furthermore, corporations utilise complex ownership chains, transfer pricing, and tax-haven subsidiaries to obscure real income flows and enable laundering by concealing beneficial ownership and exploiting transparency gaps (Transparency International, n.d.).

Political elites follow a similar pattern: placement through diversion of public resources, layering via offshore trusts and intermediaries, and integration through property acquisitions or foreign investments. The 1MDB scandal exemplifies this dynamic, as officials channelled billions through shell firms and accounts in multiple jurisdictions, exploiting weak oversight and regulatory capture that shield politically exposed persons (Barnett & Sloan, 2018).

Across all three actor types, the same cycle emerges: illicit funds enter legitimate systems, are layered through complexity, reinvested as clean capital, and used to reinforce power. Modern laundering thus transcends criminal, corporate, and political boundaries, exploiting the same global financial architecture that sustains legitimate commerce (Europol, 2021).

2.4 The 1MDB Case - Financial Dimension

The 1Malaysia Development Berhad (1MDB) scandal was selected for its unparalleled scale and the clarity with which it exposes the financial mechanics of global

money laundering. From a financial standpoint, the case is significant because it demonstrates how complex instruments - sovereign bonds, joint ventures, investment funds, and correspondent banking channels - can be manipulated to disguise the illicit movement of public capital. Analysing 1MDB through a financial lens allows for an understanding of how legitimate market structures were exploited to launder billions under the cover of lawful investment activity. It also reveals the vulnerabilities of international banking oversight, compliance culture, and risk management systems, providing crucial insight into how systemic financial corruption operates within formal economic frameworks.

1MDB began as a state-owned regional development initiative but evolved into one of the world's most notorious money-laundering scandals. Intended to attract foreign investment and promote national growth, it later became, as Wright and Hope describe in *Billion Dollar Whale*, "one of the greatest financial heists in history." Under Prime Minister Najib Razak, the initiative expanded in 2009 into a sovereign development fund financing large projects in energy, real estate, and tourism. Behind this vision, however, lay a sophisticated scheme that exploited legitimate financial systems to divert billions for private gain, exposing deep weaknesses in transparency and banking oversight (Financial Crime Academy, 2025).

The U.S. Department of Justice (DOJ) described 1MDB as "the largest kleptocracy asset recovery effort in the history of its Kleptocracy Asset Recovery Initiative" (Nick Tabor, 2025, para. 2). According to DOJ filings, roughly $1 billion was siphoned through a joint venture with PetroSaudi International, $1.4 billion raised by Goldman Sachs was diverted to a Swiss offshore account, and another $1.3 billion from a separate bond issue was routed through Singapore. Exposed in 2015 by a Malaysian parliamentary inquiry, the scheme misappropriated an estimated USD 4.5 billion. The funds passed through a network of shell companies, offshore entities, and bank accounts before enriching officials and associates, financing assets such as real estate, art, yachts, and film productions.

The scandal prompted investigations across multiple jurisdictions, including the United States, Switzerland, and Germany. Multiple individuals, among them former Prime Minister Najib Razak, were charged with corruption, abuse of power, and money laundering. In addition to political prosecutions, major financial institutions came under scrutiny for their role in facilitating or failing to detect suspicious transactions. In Switzerland, the Financial Market Supervisory Authority (FINMA) initiated enforcement actions against seven financial institutions, citing serious internal control failures, poor due diligence regarding politically exposed persons (PEPs), and inadequate transaction monitoring. These findings revealed

systemic weaknesses in AML frameworks and underscored how even established financial systems can be exploited for illicit purposes (Jones, 2020).

The 1MDB case shows how stolen state funds can be laundered through legitimate financial systems by exploiting regulatory gaps and weak oversight. It demonstrates that contemporary laundering often relies on legal instruments - bonds, investment funds, and asset purchases - rather than covert cash movements. The scandal underscores the need for stronger international cooperation, ownership transparency, and enforcement to prevent further misuse of legitimate institutions. It also exposes the complicity of global banks, auditors, and intermediaries that ignored suspicious transactions, eroding trust in governance and the global financial system. Ultimately, 1MDB highlights the necessity of accountability and political will, as corruption in one country can ripple across borders, destabilising national and global markets alike.

2.5 The Panama Papers Case - Financial Dimension

The Panama Papers leak comprised 11.5 million documents spanning nearly four decades and 2.6 terabytes of data, one of the largest exposures to date (Obermayer et al., n.d.). The files originated from Mossack Fonseca, one of the world's leading offshore law firms, and were first shared anonymously with a German newspaper before being analysed by the International Consortium of Investigative Journalists (ICIJ) in collaboration with over 350 journalists across 80 countries. An anonymous whistleblower, known as John Doe, agreed to share the documents on the condition that they be made available to government authorities. In a statement titled *The Revolution Will Be Digitalised*, John Doe justified the disclosure as a stand against corruption, inequality, and abuse of power (ICIJ, 2016). The data contained financial records, correspondence, and documentation on offshore entities, intermediaries, and beneficial owners, implicating politicians and business figures worldwide. The database listed over 200,000 offshore entities and thousands of related officers and intermediaries. It is important to specify that while not all offshore finance serves illicit purposes, the clear links between some entities and criminal actors indicate that tax havens facilitate a significant share of global money laundering and tax evasion.

The leak triggered widespread regulatory reforms, criminal investigations, and prosecutions. Mossack Fonseca's founders were arrested for money laundering, and the firm was ultimately dissolved. Firms named in the documents lost an estimated USD 174 billion in market capitalisation and experienced reduced sales (O'Donovan et al., 2019). The

revelations also paved the way for subsequent leaks, including the Paradise Papers (2017) and Pandora Papers (2021).

This leak also enabled systematic research into the role of tax havens in fiscal evasion. Kavakli et al. (2023) found that sanctioned entities shifted funds from sanctioning countries to tax havens, underscoring the global reach of offshore finance. Concluding, given the extreme impact that offshore finance has on the economic equilibria of the global economy, the Panama Papers event represented a significant milestone in the investigation into offshore finance and the initiation of a new phase in global anti-money laundering and anti-evasion enforcement.

2.6 Institutional Failures

Money laundering is not merely the product of criminal ingenuity, but of institutional fragility. Despite decades of AML regulation developments, compliance frameworks often collapse under commercial pressure, fragmented supervision, and political influence. Banks act as the first line of defence against illicit capital, and regulators the second; when either fails, the entire AML system weakens. According to the International Monetary Fund (IMF), the persistence of large-scale laundering reveals "systemic governance deficiencies" in risk assessment, supervision, and enforcement. The FATF likewise finds that only one in ten jurisdictions achieves "substantial effectiveness" in enforcing AML/CFT measures.

Weak and uneven supervision underpins laundering networks. Differing legal systems and resources produce inconsistent enforcement and encourage regulatory arbitrage, allowing criminals and corporations to exploit the least stringent jurisdictions. Regulators often rely on the same institutions they monitor for information, enabling under-reporting of suspicious activity. To enhance coordination, Europol established the Financial Intelligence Public-Private Partnership Steering Group (EFIPPP), a forum linking financial intelligence units, regulators, and financial institutions to share typologies and strengthen joint investigations (Europol, 2021).

Corruption weakens institutions by aligning governance with elite interests. Underfunded and politically influenced agencies lack the capacity or will to prosecute financial crimes, creating two enforcement systems - one for PEPs and another for ordinary actors. Transnational laundering networks further enable the export of illicit funds, especially from weaker states (Bahaj et al., 2025). Weak oversight of political financing similarly enables illicit capital to shape democratic processes. The Atlantic Council's *Democracy in the*

Crosshairs (Barnett & Sloan, 2018) documents how opaque donations and offshore accounts allowed hidden actors to fund campaigns - from Germany's AfD to offshore-linked Brexit financing. These patterns mirror compliance failures in banking: transparency gaps corrode accountability and require verified donor checks, global cooperation, and full ownership disclosure to restore trust in institutions.

Compliance within banks often functions as a box-ticking exercise rather than a risk-based culture. The Bank for International Settlements noted that many institutions view compliance as a constraint to be managed, not a core component of stability (BIS, 2019). Weak Know-Your-Customer (KYC) procedures, superficial due diligence, and ineffective transaction monitoring persist even in advanced markets. Governance failures arise when boards prioritise short-term profit, compliance officers report to revenue heads, and internal audit lacks authority to escalate concerns. Another issue concerns the relation between corporate governance and profits. The IMF argues that in competitive banking markets, compliance is often perceived as a cost centre rather than a safeguard. This profit bias explains why institutions repeatedly tolerate high-risk clients - PEPs, offshore vehicles, or opaque trusts generating lucrative fees (IMF, 2023). Similarly, Transparency International (2021) found that G20 banks often maintain relationships with high-risk customers even after regulatory sanctions, reflecting a "too big to punish" mentality. In addition, in G20 states, beneficial-ownership registers remain incomplete or inaccessible due to lobbying pressure from financial institutions resisting transparency (OECD, 2024).

The interaction between private compliance failures and public regulatory gaps becomes evident in global case studies. In Danske Bank, the lack of coordinated supervision between Danish and Estonian authorities allowed transactions linked to Russian and Azerbaijani clients to move unnoticed for nearly a decade. In 1MDB, Malaysian officials channelled over USD 4.5 billion through shell companies and global correspondent banks, exploiting weaknesses in cross-border information sharing. The Panama Papers further illustrated systemic weakness: thousands of offshore entities were created by legitimate law firms and serviced by major banks that failed to verify clients' ultimate beneficial owners. These leaks exposed how legal, corporate, and banking institutions cooperate, intentionally or not, to sustain global illicit finance.

Institutional weakness is both structural and cyclical. Each scandal prompts new regulations, yet reforms often remain cosmetic. Unless profit-driven incentives, fragmented supervision, and opaque ownership are addressed, money laundering will persist.

Recognising these failures is essential to restoring transparency, credibility, and stability to global markets.

3 Behavioural Dimensions of Money Laundering

3.1 Introduction and Key Psychological Drivers

Understanding global laundering networks requires an investigation of the human and organisational behaviours that produce them. It involves exploring the psychological, social, and institutional mechanisms that motivate and normalise illicit financial activity. This section investigates how individuals and groups within professional environments rationalise unlawful conduct and construct systems that sustain criminal economies under the guise of legitimacy. A behavioural analysis thus provides an essential foundation for interpreting how global laundering networks persist, despite public condemnation and formal efforts to fight it.

Applying the behavioural sciences (namely psychology, sociology, criminology and anthropology) to support the field of forensic accounting is of the utmost importance to achieve meaningful progress in facing the scourge of money laundering. The rationale for this is evident from the intuition that one needs to "think like a crook to catch a crook". The application of criminological approaches to study money laundering schemes has been occasional up to this point, despite its crucial relevance (Riccardi & Reuter, 2020). As the incidence of fraud continues to grow, placing the spotlight on behavioural factors may be an important approach not only to fraud detection, but to deterrence as well.

An important starting point in order to understand money laundering and fraud in general is the so-called *Fraud Triangle*. The structural elements of this model were used to propose a definition of fraud from an accounting perspective (Huber, 2017) by the American Institute of Certified Public Accountants (AICPA) in 2002. The Statement on Auditing Standards 99 clearly outlines the three key drivers of fraud, which are described as follows: "Three conditions generally are present when fraud occurs. First, management or other employees have an incentive or are under pressure, which provides a reason to commit fraud. Second, circumstances exist [...] that provide an opportunity for fraud to be perpetrated. Third, those involved are able to rationalise committing a fraudulent act" (AICPA, 2022, p. 8). It is believed that the components of this structure were first conceptualised by Dr Donald Cressey in 1953. The criminologist, after interviewing prisoners, noticed the manifestation of incentive, opportunity and rationalisation.

Pressure and incentives to engage in fraud can be high, especially if there is a need for financial targets to be met or to make up for past mistakes. Executive compensation structures often play a role in increasing perceived pressure to perform well. As Fuller and Jensen (2002, p. 42) argued, "over the last decade, companies have struggled more and more desperately to meet analysts' expectations. Executives often acquiesced to increasingly unrealistic projections and adopted them as a basis for setting goals for their organisations." The consequences of such expectations are extremely damaging, pushing generally law-abiding employees to commit crimes solely for the purpose of maintaining their career positions.

The element of opportunity is also significant, as it lifts the barrier between the fraudster's intention to commit money laundering and the material act. Opportunities arise in times of financial crisis: for example, if a company has recently laid off employees, maintaining roles can be harder, laying the path for individuals to act. Ramamoorti (2008) depicts the relationship between crimes and opportunities as being purely mathematical: the aggregate rate of white collar crimes varies directly with the supply of criminal opportunity, and inversely with the intensity of law enforcement.

The roots of rationalisation, defined as the need to justify wrongdoing to maintain self-coherence, lie in the theory of "cognitive dissonance". First proposed by Stanford University social psychologist Leon Festinger, cognitive dissonance is a state of distress that pushes the individual to modify one or both cognitions to restore coherence. Criminals feel the need to alter the justification of their actions to restore self-peace, which results in a series of excuses, such as: "everyone else is getting rich, so why shouldn't I?", or "I deserve this money as compensation for my hard work". Cressey (1973) exposed just how rationalisation can make a trusted person become a trust violator. These types of people often believe their problem is unshareable and see in committing a violation of financial trust an easy and secretive way out. This situation transforms financial crime into a small, justifiable secret, allowing the perpetrator's conscience to be cleared.

The *Fraud Triangle*, however, is not the only model used to describe fraud. Many have proposed variations on this scheme, or, as will be later mentioned, openly defied it. A meaningful addition to this analysis is the role of "capability" in money laundering dynamics, thus creating the so-called *Fraud Diamond*. Wolfe and Hermanson (2004) offer an interpretation of the "essential traits for committing fraud", the first of which is a person's position or function in a certain organisation. Some roles grant the positional authority to influence the timing and entity of several deals. In addition, the person must have the

intelligence to recognise the weaknesses in internal systems and be able to exploit them to their own advantage, as well as confidence that makes them convinced of their own "invincibility". The final qualities encompassed in the term "capability", according to the *Fraud Diamond*, are the ability to lie consistently and influence others to commit or conceal fraud.

Although this study certainly seems to have created a clear picture of what a fraudster can look like, the categorisation of fraud under these types of models has been met with scepticism. For instance, business professor Dennis Huber advocates for "the end of the fraud triangle" (Huber, 2017, pp. 28-29), his rejection stemming from the foundation of the matter. Huber believes the *Fraud Triangle* shouldn't be applied to fraud at all, and that its original ideation (which is owed to Cressey) is only appropriate to define embezzlement. Furthermore, he argues that any type of geometrical shape is inappropriate for correctly analysing fraud: "forensic accounting researchers and practitioners must recognize that the fraud triangle does not apply to fraud and must consider that there are n-dimensions of financial crime that must be accounted for in any model that attempts to explain, predict, prevent, detect and prosecute financial crimes, of which fraud is merely a subset" (Huber, 2017, p. 29). Indeed, the complexity of the matter makes it so that these drivers alone are not sufficient to correctly encompass the vastness of the problem. Exploring the behavioural aspect of money laundering implies delving into the mind of white-collar criminals and, in doing so, accepting that each of them has their own story and motivations.

These drivers are certainly insufficient to comprehensively understand the motives and rationales behind the actions of perpetrators; however, they represent a starting point in a much more complex system that we aim to gradually uncover.

3.2 Normalisation of Corruption within Elites

"All organisations are inherently criminogenic" (Gross, 1978, p. 56). Collective corruption within organisations emerges incrementally, consolidating through idiosyncratic practices that construct a behaviour that becomes institutionalised. This process, through which corruption cultivates within companies, leads to the normalisation of practices within the elite and professional environments. The phenomenon described reflects not mere individual deviance, but the convergence of psychological, sociological, and organisational forces that systematically erode ethical standards.

A key aspect to note is how the distribution of corruption is composed in terms of age, gender, and ethnicity. According to the Federal Bureau of Investigation (2019), 60.5% of embezzlement arrests are of White ethnicity, followed by 36.3% Black or African American. Further detailing reveals that 80% of white-collar offenders are men and 67% are white, aged 30-40 (LaBrie, 2022), who belong to the middle or upper class. This information is supported by a study conducted by the United Nations on Corruption in the public sector of Iraq, which concludes that bribery is higher amongst the country's most educated and with the highest per capita income, exactly 18.3% and 13.4% respectively. Analysing the motivation behind these bribes, 45.8% are in order to speed up administrative procedures, and 26.6% do so to receive better treatment or service (United Nations Office on Drugs and Crime, 2013). The data signals a pattern that can be identified throughout varying levels of a company.

The corruptive seed is planted initially through "the agents of social control," which are referred to as the dominant coalition (Jávor & Jancsics, 2016, pp. 533-534). These are members of management who influence company culture and behaviour. This level functions through heavy politics, producing coalition-building and bargaining among competing internal constituencies. The power concentrated in this tier then flows through the mediator zone and the bottom level. Within the mediator zone, technical experts and higher-level professionals who serve as enablers operate from a quantitative perspective. The skills and sensible information they manage make them a key agent for transforming the power of the elite into salary and opportunity boosts. Additionally, they mediate conflict with the lower level due to their proximity. When considering the bottom level, their most relevant role in the power dynamic relates to strategic positioning in the company. They are the company's most direct contact with the outside world and can therefore control organisational processes from an informal angle.

Once there is an established structure of corruption through normativeness, standardisation begins. The rationale behind this concept centres around how, once practices have been implemented in a repeated manner, showing the potential for continued success, a "power of ritual" is assumed. This is a turning point where "the expedient comes to seem necessary", or practices become habits (Ashforth & Anand, 2003, p. 13). Once this point has been reached, it becomes a culture of mindlessness where there is no longer a need to justify or question, and corruptive practices are a sign of admiration and success.

Given the complexities in moral disengagement, it is best to analyse the different psychological mechanisms that suspend self-sanctions. This rationale makes corruption psychologically tolerable, or re-labelled as "creative compliance". In elite organisations,

institutional complicity amplifies this psychology as compliance teams are co-opted or sidelined, oversight is hollowed out or buried in process, and leaders reward results over methods (Jávor & Jancsics, 2016).

3.3 Moral Disengagement

It is relatively rare that powerful political and financial elites truly regret the fraud or corruption they have committed. Within elite professional cultures, wrongdoing is reframed as competence, and complicity becomes part of the job. To be able to maintain a favourable self-image, people reframe unethical behaviour as professionalism or efficiency. This dynamic illustrates how moral perception can change under social and organisational influence (Kouchaki & Smith, 2013). Such a strange phenomenon reveals a profound psychological defence at work: moral disengagement, a process through which people suppress moral self-censure to act within corrupt systems without viewing themselves as immoral.

In laundering networks, moral disengagement reveals itself through a series of cognitive and linguistic mechanisms that make corruption appear either legitimate or necessary. Those who breach the law may justify their actions through moral justification, stating that it serves the greater good. People who violate the law in financial institutions often present their unlawful acts as a form of customer service or financial aid. Money laundering can be rebranded as “asset protection” or “tax optimisation”, thus turning criminal activities into compliance with the law. A lawyer who creates shell companies may convince themselves that they are only facilitating international investment. In such a way, individuals can disregard the ethical limits of their activity while remaining compliant with the law on paper (Dani & Kollwitz, 2025).

In this process, euphemistic language is essential. The ethical connotations of terms such as “concealment” or “evasion” are replaced with their softer versions, such as “tax optimisation”, “offshore structuring”, or “client confidentiality”. This is where linguistic sanitisation aids in the construction of a professional narrative in which illegality becomes administrative, almost routine, as evidenced through studies on the behavioural aspects of corporate fraud. The emotional dissonance disappears as the language neutralises the act, and procedural detachment replaces ethical awareness (Bandura, 2011).

Another important factor in moral disengagement is the diffusion of responsibility. It is rare that any one actor would feel clearly responsible in giant institutions because every

decision is diffused across several divisions. This collective dynamic weakens individual moral awareness, as hierarchical structures create a sense of detachment and moral indifference within the organisation (Anand, Ashforth & Joshi, 2004). When everyone is responsible, nobody is really responsible. Over time, these cognitive strategies become institutionalised in corporate culture, creating a moral infrastructure that "routinises'' unethical conduct.

Institutions do not just endure corruption; they facilitate it through implicit norms and established practices. Employees discover that outcomes take precedence over integrity since awards are given based on performance metrics instead of ethical conduct. Compliance teams' auditing and reporting mechanisms could ultimately serve as performative shields that enable hidden unlawful actions while maintaining the illusion of legality. This interplay illustrates what sociologists call "moral normalisation": the slow change of deviant actions into accepted norms. Hierarchical systems enhance this phenomenon: junior staff obey commands, middle managers rationalise the actions, and top executives detach themselves by keeping things vague and general. Consequently, whole organisations act immorally without recognising their corruption (Charlopova, Andon & Free, 2020).

In essence, moral disengagement transforms corruption from an ethical choice into a cognitive habit. It allows individuals to remain socially and professionally respected while actively sustaining criminal economies. The phenomenon is present in organisational design as well as personal psychology: hierarchical decision-making, bureaucratic systems, and coded professional language serve as psychological barriers. These dynamics drive many of the real-world crises that follow, when professional actors internalise moral disengagement to the point at which it becomes part of institutional culture.

3.4 The Panama Papers Case - Behavioural Dimension

The Panama Papers case was selected for this research as it represents one of the most revealing examples of how human behaviour interacts with complex financial systems to facilitate money laundering on a global scale. The analysis of this case is fundamental to understanding the behavioural aspect of money laundering, as it highlights how cognitive biases, motivations, and social dynamics influence the choices of offenders operating within the global financial environment.

Beyond its financial implications previously described, the Panama Papers offer a unique lens through which to examine the psychological foundations of corruption. A central

behavioural pattern in this case is the role of power in fostering moral disengagement and impunity, this relationship between authority and ethical erosion being widely explored in behavioural research. The Chr. Michelsen Institute, an independent research organisation in Norway, underlined in their study *The Cognitive Psychology of Corruption*, how "individuals holding power are more likely to act corruptly, especially when they work in organisations where unethical behaviour goes unpunished" (Dupuy & Neset, 2018, pp. 3-4). The protagonists of the Panama Papers case all share one common feature: they hold power, which is defined by the Institute as "certain individuals holding accountable degrees of authority over decision-making processes, creating lucrative windows of opportunity for unethical behaviour" (Dupuy & Neset, 2018, p. 5).

Most of the politicians involved held power in nations exhibiting hybrid or partially democratic regimes. To better conceptualise this dynamic, Robert Klitgaard's (2011, p. 33) corruption formula offers a useful analytical framework:

Corruption = monopoly + discretion – accountability.

Under this lens, monopoly can be interpreted as the control these figures exercised over governmental functions; discretion reflects their use of firms such as Mossack Fonseca to conduct transactions; and accountability connects to moral disengagement since, as reported by the ICIJ in 2016, "law firms and other offshore players have often failed to follow legal requirements that they make sure their clients are not involved in criminal enterprises, tax dodging or political corruption".

Another behavioural model that explains the persistence of corruption in this case is the previously mentioned *Fraud Triangle*. The increasing pressure from governments all over the world to control financial activities and prevent connections to terrorist organisations, following the 9/11 attacks, led investors and politicians to find new channels for their illegal activities. The opportunity was represented by offshore companies, managed with the help of legal firms in jurisdictions such as Panama, where such controls were not enforced (ICIJ, 2016). The final step was the rationalisation of these processes, the associates of the Mossack Fonseca law firm justifying their activities as complying with international laws.

The Panama Papers case underscores that financial crime is not only a product of regulatory loopholes and financial manipulation, but also of behavioural normalisation within powerful circles, underlining the importance of psychological analysis in understanding how

financial elites justify and perpetuate illicit practices within frameworks that appear legally permissible.

3.5 The Danske Bank Case - Behavioural Dimension

To this date, the Danske Bank event is referred to as the largest money laundering scandal in European History. Between February 2007 and April 2016, over EUR 200 billion in transactions originating from Russia flowed through the Estonian branch's non-resident portfolios (NRPs), according to Faccia et al. (2019). These transactions were deemed suspicious, prompting external investigations into the possibility of money laundering.

Danske Bank was named the largest financial institution in Denmark due to the size of its assets, and has undergone significant expansion since its establishment, Finnish Sampo Bank being one of the acquisitions. Sampo Bank held approximately 10,000 NRPs between 2007 and 2015, mostly in Russia and former Soviet countries that had no real connection to Estonia, but generated considerable and increasing profits for the branch (Bjerregaard & Kirchmaier, 2019). Before the acquisition, Sampo Bank received multiple warnings regarding weak KYC procedures and money-laundering allegations from Russia's Central Bank, yet this did not discourage Danske Bank from proceeding with the purchase. The Estonian Financial Supervisory Authority (FSA) also expressed concern surrounding the money laundering risks and size of NRPs in Sampo Bank to the Danish FSA in 2012 and 2013, after receiving warnings from Russia's Central Bank. However, Danske Bank reassured that the risk was under control, and the following investigation by the Estonian FSA concluded that no significant activity was found.

In 2014, the Estonian branch was first confronted with serious AML failures. A whistleblower repeatedly reported suspicious activity involving a UK-registered company, yet management failed to act despite internal audit recommendations for a full review of all non-resident portfolios. Remedial measures were taken only after Danish media coverage exposed the issue, revealing that the executive board had prioritised profit over compliance integrity (Bjerregaard & Kirchmaier, 2019). Following the loss of key U.S. correspondent banks as a result of this exposure, Danske Bank ultimately closed its non-resident portfolio in early 2016 (McConnell, 2020).

Reflecting on the sequence of events, it is evident that one reason Danske Bank was the perfect money laundering vehicle was because of its profit-driven mindset at the expense of effective risk safeguarding. This ideology permeated all levels of the bank's leadership,

overshadowing the responsibility of developing proper risk management systems, exhibited through the acquisition of Sampo Bank, regardless of existing warnings and doubts. Furthermore, the decision not to integrate Sampo into Danske Bank's risk management process on cost grounds indicates that the risk of illegal transactions was inferior to the profitability of the company. Another cultural norm instilled in the firm was avoiding scrutiny and accountability through silence and ignorance, evidenced by the disregard for the whistleblower and AML concerns that never reached the executive board. Employees were trained to comply rather than question, this being the simpler approach. Motivated blindness was also evident throughout the company, managers and subordinates convincing themselves and others that everything was under control, focusing on their priority of profitability. This was also reinforced in the later stages of their criminal involvement, entering a dangerous cycle where the bank was driven by the fear of its problems coming to light, motivated by pure denial and feigned innocence. Lastly, Danske Bank exhibited strong overconfidence bias, overestimating its ability to handle the new acquisition in a responsible manner, and underestimating the importance of risk management and AML controls, believing that the concerns raised by the Russian Central Bank were baseless and innocuous.

4 The Legal Environment of Money Laundering

4.1 Introduction and the Structural Conditions Enabling Money Laundering

This section explores how, despite the existence of international, European, and domestic regulatory frameworks, criminal activities based on money laundering continue to avoid such measures and pursue interests that are incompatible with legal systems. The primary factors that enable money laundering to flourish are not the absence of international control mechanisms, but rather the combination of elements such as the low degree of regulatory cohesion at the global, European, and national levels, and the professional and banking secrecy maintained by lawyers, notaries, and accountants, which result in limited cooperation with authorities and a significant slowing of administrative procedures.

It is useful to recall the Fraud Triangle, theorised by Donald R. Cressey and published in 1973, which is widely regarded as the key framework for explaining the underlying conditions of economic and financial crime: pressure, opportunity, and rationalisation. Regulatory gaps do more than merely create opportunities for misconduct; they also reinforce and even legitimise such behaviour by making it appear feasible, low-risk, or institutionally

tolerated. Since the late 1980s, international institutions have recognised the necessity for establishing laws and regulations aimed at ensuring justice across nations, seeking to limit and monitor illicit activities that arise precisely from inconsistencies and incompatibilities among different legislative systems. Lastly, to provide a more comprehensive analysis, the discussion, though primarily situated within an international framework, will draw on, compare, and define examples from the Italian legal system to illustrate the high level of regulatory cohesion and harmonisation with international conventions.

4.2 Key AML Institutions and the Italian Regulatory Framework

The Financial Action Task Force was established in 1989 by the G7 as the principal intergovernmental body responsible for setting global standards against money laundering. In 2001, its mandate was extended to counter terrorist financing. FATF issues internationally recognized recommendations addressing risk-based supervision (R.1-2), criminalization of money laundering and terrorist financing (R.3-5), confiscation (R.4), customer due diligence and record-keeping, suspicious-transaction reporting (R.10-21), transparency of beneficial ownership (R.24-25), and international cooperation among authorities and Financial Intelligence Units (R.36–40). In 2025, FATF's work is particularly focused on the regulation of virtual-asset service providers and increased risk supervision (FATF, 2012).

The United Nations provides the core international legal framework in combating money laundering through the Vienna Convention, 1988; Terrorist Financing Convention, 1999; and the Palermo Convention, 2000. Each of these instruments established obligations relating to criminalisation, asset seizure, and cross-border cooperation. Implementing these commitments, the UN created the United Nations Office on Drugs and Crime, formed in 1977 through the merger of the Drugs Control Programme and the Centre for International Crime Prevention. UNODC is the central coordinating agency for global action against money laundering, organised crime, and terrorism, working through a network of field offices worldwide. With Resolution 55/2 of 8 September 2000, Member States decided to intensify their efforts against transnational crime and to undertake concrete actions to counter terrorism. Since 1997, the Office has managed a specific initiative known as the Global Programme against Money Laundering (GPML). The programme’s main functions include investigative and operational assistance, training and capacity building, and the provision of technical support to States (Dipartimento delle politiche contro la droga e le altre dipendenze, 2023; UNODC, 2025).

The European Union adopted its first Anti-Money Laundering Directive in 1991 and has since developed an increasingly harmonised regulatory framework to protect the integrity of the internal market. Successive directives and regulations expanded AML obligations in response to evolving risks linked to technological innovation, globalisation, and the increasing ingenuity of criminals. The latest reform, Regulation (EU) 2024/1624, established the Anti-Money Laundering Authority (AMLA), entrusting it with direct supervisory powers over high-risk financial institutions and the ability to coordinate sanctions and enforcement across Member States. This aims to address the deficiencies of the past, which had resulted from fragmented national supervision and inconsistent regulatory implementation (Consilium Europa, 2024).

Italy's anti-money laundering system is primarily governed by Legislative Decree No. 231/2007, whose purpose is to prevent and suppress money laundering and terrorist financing while supporting judicial authorities. The decree was amended on many occasions to allow for the adaptation of domestic law to the successive EU Anti-Money Laundering Directives. Its implementation is organised around several key national authorities, each performing different supervisory and regulatory functions.

Banca d'Italia is known for its role in the implementation of internal control, customer due diligence, record-keeping and governance requirements through the monitoring of bank activity, e-money institutions and investment firms. This institution has the power to impose corrective measures or prohibit new operations when deficiencies are found within beneficial-ownership companies (Banca d'Italia, n.d.).

The Unità di Informazione Finanziarie (UIF) acts as a national Financial Intelligence Unit by analysing suspicious-transaction reports, maintaining data archives and cooperating with other entities such as the Direzione Investigativa Antimafia, which carries out judicial police investigations against mafia-type organised crime. Overall, despite the existence of multiple institutions whose role is to supervise AML standards, their fragmentation potentially weakens enforcement; however, the creation of the AMLA has allowed for more harmonisation to mitigate this issue (Unità di Informazione Finanziaria per l'Italia, n.d.).

Thanks to its Dipartimento del Tesoro, the Ministero dell'Economia e delle Finanze (MEF) has normative and sanctioning authority over money laundering activities. By coordinating with the Bank of Italy, UIF and Guardia di Finanza, the MEF may draft regulations that align with ALM standards and impose administrative sanctions such as fines, disqualifying managers and leaving cease-and-desist ultimatums for non-complying entities (MEF Dipartimento del Tesoro, 2021).

Including the Italian framework demonstrates how international standards are embedded into domestic law and practice. It provides a concrete example of how international principles translate into institutional structures, supervisory practices, and enforcement mechanisms within a specific legal system.

4.3 Analysis of Legal and Regulatory Mechanisms Governing AML

Following the overview of the conventions, regulations, and legal instruments governing anti-money laundering, this section examines the most significant provisions in greater depth through a comparative analysis of the institutions discussed above. The purpose of this analysis is to assess the actual degree of normative cohesion and harmonisation between the institutional sources (United Nations, FATF-GAFI, and the European Union) and their transposition into Italian domestic law (Legislative Decree No. 231/2007 and subsequent amendments). From an international standpoint, the main conventions incorporated into the Italian legal system are:

a. *Vienna Convention* (1988)

In the *Vienna Convention*, the United Nations adopted a set of preventive measures against money laundering, recognising the close connection between illicit trafficking and other forms of organised criminal activity that undermine legitimate economic systems. Article 3, paragraph 1(b) of the Convention criminalises the conversion or transfer of property derived from one or more serious offences, committed to conceal or disguise the illicit origin of such property or assisting any person involved in the commission of those offences. In the Italian legal system, this conduct is reflected in Article 648-bis of the Criminal Code, which establishes the offence of money laundering for anyone who replaces or transfers money, goods, or other assets derived from a crime in such a way as to obstruct the identification of their illicit origin. The current formulation of this offence was introduced by Law No. 328 of 1993.

b. *Palermo Convention* (2000)

The purpose of the *Palermo Convention* was to promote transnational cooperation to prevent and combat organised crime as effectively as possible. Its impact on Italian legislation included the introduction of provisions concerning judicial cooperation and the principle of mutual recognition. The latter responds to the need to eliminate discrepancies and asymmetries in the transposition of regulations, to ensure uniformity in their application, and to guarantee the effective mutual recognition of freezing and confiscation orders (Article 6).

Article 7, paragraph 1(a) of the Convention establishes measures to combat money laundering, including the obligation for each State Party to institute a comprehensive domestic regulatory and supervisory regime for banks, non-bank financial institutions, and other entities particularly vulnerable to money laundering.

c. European Union Instruments

Before proceeding with a comparative analysis between the Italian legal system and the measures adopted by the European Union, it is necessary to recall the fundamental difference between EU directives and regulations. Directives bind Member States only as to the result to be achieved, leaving them discretion in the choice of form and means of implementation. Regulations, on the other hand, are directly and fully binding on all Member States, without the need for transposition into national law (as in the case of Regulation (EU) 2024/1624). With this premise established, we can introduce the most significant regulatory framework within the European Union that has been incorporated into the Italian legal system, the so-called *AML Package*, namely the comprehensive reform package governing anti-money-laundering measures. More specifically, the *AML Package* comprises the Fourth Anti-Money Laundering Directive, which defines the mechanisms Member States must implement to prevent the misuse of the financial system, and the Anti-Money Laundering Regulation, which removes interpretative inconsistencies and introduces a uniform, comprehensive framework replacing the fragmented regime of earlier directives. The underlying rationale of this reform is that the State must also monitor non-traditional financial flows, identifying alternative channels through which illicit funds may circulate. Undoubtedly, the *AML Package* has modernised and strengthened the existing European regulatory framework; however, its most significant innovation lies in the broadened scope of entities subject to AML supervision in relation to financial transactions.

4.4 Conflict Between Domestic, International, and EU Law

Over the years, numerous tensions have emerged between domestic laws and European or international regulations governing anti-money laundering obligations. The judgment of 22 November 2022 serves as a particularly instructive example, illustrating how European directives and regulations, especially those concerning the prevention of money laundering and the financing of terrorism, can at times conflict with fundamental rights or core domestic legal principles.

In the joint cases C-37/20 and C-601/20, the Court of Justice of the European Union (CJEU) declared invalid the provision of Directive (EU) 2015/849. This was subsequently replaced and superseded by Directive (EU) 2024/1640 within the new EU AML Package, which required Member States to ensure that information on the beneficial ownership of companies and other legal entities incorporated within their territory is accessible to the public in all cases. Case C-37/20 concerned an action brought by a Luxembourg national, the beneficial owner of a company, against the Luxembourg Business Registers (LBR), whereas case C-601/20 involved a similar challenge brought by a company against national legislation implementing the EU Anti-Money Laundering Directive. In both cases, the applicants argued that unrestricted public access to personal data contained in the UBO register constituted a violation of the right to privacy, exposing the individuals and their families to real and current risks of intimidation, violence, extortion, kidnapping, or blackmail. The Court upheld the applications and declared Article 30(5)(c) of Directive (EU) 2015/849, as amended by Directive (EU) 2018/843, invalid insofar as it provided for general public access to the beneficial-ownership registers. According to the Court, such public access to registers, and therefore to personal information regarding beneficial ownership, constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Nevertheless, the Court recognised that economic transparency remains a legitimate objective in combating money laundering; however, it does not justify unlimited and indiscriminate access to personal data of individuals who are neither under investigation nor suspected of criminal activity.

Accordingly, the CJEU held that access must be limited to competent authorities and Financial Intelligence Units (FIUs), obligated entities under AML law, and to persons or organisations demonstrating a “legitimate interest” in obtaining such information. The main consequences of this ruling were the suspension or restriction of public access to UBO registers in several EU Member States, including Germany, France, Luxembourg, and Italy, and the European Commission’s subsequent recognition of the need to reform the AML framework to achieve a more appropriate balance between transparency and fundamental rights.

4.5 The Role of Notaries, Accountants, and Lawyers

In an increasingly globalised legal environment, the role of public notaries has expanded, particularly in cross-border transactions and international compliance processes shaped by successive waves of globalisation. In civil law jurisdictions, like those of Italy and Spain, notaries are highly trained legal professionals with public authority; they are not only mere witnesses to signatures, but they are also trusted legal officers with a quasi-judicial function. The notaries' core responsibilities include drafting, authenticating, and preserving legal documents. They ensure that all parties have full knowledge of the legal implications of their actions, as well as making sure that all transactions meet the mandatory legal requirements. Therefore, it is appropriate to say that notaries serve as neutral advisors who protect the integrity of legal transactions. However, notaries may be used by criminals to formalise incorporations or shell companies. If the notary does not verify the true beneficial owner, the company can serve as a front for illicit funds. Moreover, notaries often certify property transfers. If they do not exercise the necessary due diligence regarding the origin of funds or beneficial ownership, they may unintentionally legitimise dirty money, which commonly happens in real estate laundering (Consiglio Nazionale del Notariato, n.d.).

Accountants play an important role in the world of financial reporting and analysis, as they are necessary for transparency and accountability within organisations. They are responsible for the preparation and examination of financial statements, making sure data is accurate and compliant with relevant standards and regulations such as the Generally Accepted Accounting Principles (GAAP) and International Financial Reporting Standards (IFRS). Furthermore, accountants are also tasked with providing auditing analysis to present a "true and fair value" so as to prevent fraud and misrepresentation. In addition to that, accountants interpret complex tax laws and ensure that businesses pay the correct amount of taxes, as well as advising on lawful tax planning: distinguishing between legal tax avoidance and illegal tax evasion. Accountants operate within a highly complex and constantly evolving legal environment, marked by frequent changes in tax and reporting rules, and by the coexistence of IFRS, GAAP, and diverse national standards. This regulatory fragmentation increases compliance burdens and heightens the risk of inaccurate or unlawful reporting. Moreover, accountants must navigate persistent agency tensions, balancing client interests with their legal and ethical obligations, particularly in areas such as aggressive tax planning and AML reporting (Judijanto et al., 2024).

Financial law establishes the legal framework for financial transactions, markets, and institutions, with financial lawyers providing guidance on related issues, making sure that activities comply with legal requirements and promote market transparency, credibility, and stability. Lawyers are considered “gatekeepers” under international AML frameworks, as they must perform due diligence when setting up companies and trusts, and when handling client funds. However, legal privilege, particularly the confidentiality between a lawyer and client, can restrict transparency and create tension between AML obligations and the protection of client rights. In some cases, lawyers even invoke privilege to shield clients from scrutiny in matters involving potentially suspicious activities (Terrill, 2014).

4.6 Limitations and Vulnerabilities in Contemporary AML Systems

Structural fragmentation, uneven implementation, and persistent enforcement gaps keep existing anti-money laundering frameworks ineffective in many jurisdictions. While international standards, most notably the FATF's 40 Recommendations and various UN conventions, seek to create a uniform global approach, their application varies widely across countries, creating substantial opportunities for regulatory arbitrage.

While there are universal standards, there is inconsistent interpretation and application of AML rules. FATF Recommendations 1-2 call for a risk-based approach by states to be adopted, but the inherent flexibility of the model has produced divergent national frameworks and significant misalignment. Successive directives have been transposed unevenly within the European Union, with variable supervisory practices and differing thresholds for compliance. The creation of the EU Anti-Money Laundering Authority (AMLA) and Regulation (EU) 2024/1624 constitutes a response in light of this enduring fragmentation. Criminal networks exploit these asymmetries by relocating activities to jurisdictions with weaker beneficial-ownership transparency, slower information-sharing mechanisms, or inconsistent supervisory standards.

Although international instruments require transparency of beneficial ownership, most notably FATF Recommendations 24-25, implementation remains incomplete. Registers are often unverified, access remains limited, and complex corporate structures continue to obscure controllers of illicit assets. Concerns regarding data protection and privacy, especially within the EU, have further constrained the scope of disclosure requirements. This opacity allows money launderers to hide ownership through layered corporate vehicles, move

assets across jurisdictions before registers are updated, and exploit professional intermediaries such as lawyers and accountants by invoking confidentiality obligations.

Money laundering is inherently transnational, but enforcement remains essentially national. FATF Recommendations 37-40 call for mutual legal assistance, information exchange between FIUs, and coordinated investigations; the reality, however, is often delayed cooperation hindered by data-protection rules, incompatible procedures, and the continued dominance of state sovereignty. These barriers create jurisdictional gaps, which are leveraged by transnational criminal groups to move funds across borders with limited investigative continuity.

Sanctions also continue to be uneven and often do not act as a sufficient deterrent. In many jurisdictions, including Italy, AML violations are punishable mainly with administrative measures rather than criminal prosecution. Though FATF Recommendation 35 calls for "effective, proportionate, and dissuasive" sanctions, fines often stay below the cost of compliance.

The absence of a centralised global enforcement body allows systemic gaps to persist. At a structural level, supervisory responsibilities remain fragmented across multiple national authorities, reducing coherence and enforcement efficiency. Jurisdictionally, the principle of state sovereignty limits the reach of supranational measures and constrains the development of unified investigative and prosecutorial mechanisms. These vulnerabilities collectively provide space for criminal actors to evade oversight. As long as AML efforts remain focused on regulatory harmonisation at the expense of robust and enforceable mechanisms, money launderers will continue to exploit inconsistencies across legal systems and jurisdictions. What is required for effective deterrence is not just aligned standards, but also coordinated and well-resourced enforcement capable of responding to the fundamentally transnational nature of modern laundering networks.

4.7 The 1MDB and ENI-Saipem Cases - Legal Dimension

The 1Malaysia Development Berhad (1MDB) and ENI-Saipem (OPL 245) cases were chosen for their significance in exposing how legal and regulatory frameworks can be exploited by state-linked actors to facilitate transnational corruption. From a legal standpoint, 1MDB highlights the weaknesses of cross-border enforcement and beneficial-ownership transparency, while ENI-Saipem reveals how public-private structures can blur accountability and enable illicit financial flows under the guise of legitimate investment. Analysing both

together allows for a comparative understanding of how similar legal vulnerabilities operate across different jurisdictions and governance models, providing insight into the limits and evolution of international anti-corruption and AML regimes.

The structure of the scheme relied heavily on beneficial ownership secrecy and jurisdictional arbitrage. Each intermediary company was legally registered, but its real ownership was hidden behind layers of nominee shareholders and trusts. The financial institutions involved processed transactions that, while legally documented, exhibited all the indicators of money laundering: complex transfers, rapid movement of large sums, and apparent lack of economic rationale (FATF, 2024). The absence of timely cross-border data-sharing allowed these transactions to proceed undetected for years, underscoring the structural weaknesses of the global AML regime.

From a legal standpoint, 1MDB exemplifies the limitations of fragmented jurisdictional enforcement, where national legal systems operate with varying transparency standards and procedural frameworks. The scandal demonstrated that even in the presence of comprehensive AML frameworks, the absence of timely information-sharing and consistent enforcement can allow criminal networks to exploit systemic blind spots.

A comparable example within the Italian legal and economic context is the ENI-Saipem “OPL 245” affair - a transnational corruption and money-laundering scandal that emerged from a sovereign framework rather than a purely corporate one.

As in the 1MDB case, the episode illustrates how state-linked entities, acting under the guise of legitimate development or resource-management initiatives, can be used to channel public funds into opaque international transactions. The affair centres on the 2011 acquisition of Oil Prospecting Licence 245 (OPL 245), a highly valuable offshore oil block in Nigeria, by ENI S.p.A. The transaction involved the payment of approximately USD 1.1 billion, nominally intended for the Nigerian government. The structure of the deal relied on offshore vehicles and consultancy contracts to disguise the true destination of funds, reproducing the same beneficial-ownership opacity and jurisdictional layering observed in the 1MDB network (Eboh & Jones, 2021). Legally, the OPL 245 transaction exposed the grey area that often exists when state-controlled enterprises act with commercial autonomy abroad. ENI operated as a listed corporation, yet the Italian State retained a controlling stake through the Ministry of Economy and Finance. This hybrid status blurred accountability: the transaction’s due diligence processes were governed by private law standards, while the underlying resources and risks were sovereign. Italian prosecutors argued that this structure

created a de facto laundering mechanism, permitting illicit transfers to appear as state-sanctioned investment flows.

The affair came under judicial scrutiny in Milan's Criminal Court, leading to a multi-year trial (2018-2021) in which ENI, its executives, and several intermediaries were charged with international corruption and aggravated money laundering. Although the defendants were ultimately acquitted in 2021, the proceedings revealed systemic weaknesses in cross-border legal cooperation, particularly concerning evidence gathering, beneficial-ownership verification, and the extraterritorial application of Italian AML norms (ENI S.p.A., n.d.). Parallel investigations by the UK Serious Fraud Office (SFO) and Nigerian authorities confirmed that over USD 800 million of the payment was transferred through offshore escrow accounts in Switzerland and the Netherlands, before being redistributed among private beneficiaries.

From a legal-comparative perspective, the ENI-Saipem and 1MDB cases converge on a central insight: when state-affiliated entities manage vast financial resources through transnational structures, the distinction between sovereign policy and private enrichment becomes blurred. Both reveal the limits of current international AML frameworks in supervising hybrid actors that operate at the intersection of public mandate and private corporate form.

5 Digital Infrastructures of Money Laundering

5.1 Introduction and the Dual Nature of Technology in Modern Money Laundering

Digital infrastructures have transformed the mechanism of global finance, creating new efficiencies and new opportunities while simultaneously deepening the shadows in which illicit capital circulates. However, these systems never imply a state of perfect security, as observed by cybersecurity expert Gene Spafford, who noted "the only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts" (Dewdney, 1989, p. 110). This paradox defines the modern financial landscape: the technologies that enable secure and rapid transactions also create vulnerabilities that criminal networks can exploit.

Simultaneously, digitisation has strengthened traceability. The reliance on extensive data flows across payment systems, communication platforms, and distributed ledgers allows investigators to reconstruct increasingly complex networks of transfers and ownership.

Within this dual dynamic, the cyber dimension of money laundering has become central to understanding how illicit finance operates today. Blockchain technologies, encrypted communication channels, and anonymity-enhancing tools provide criminals with powerful methods to disguise transactions and coordinate across borders. However, these same systems also enable investigators to conduct blockchain tracing, integrate open-source intelligence, and deploy AI-based anomaly-detection models to uncover hidden financial flows.

For these reasons, analysing the cyber dimension is integral to a comprehensive understanding of contemporary money-laundering mechanisms. This section examines the principal technological models involved, ranging from encryption and anonymity systems to blockchain-based obfuscation and digital-forensic tracing, in order to demonstrate how cyberspace simultaneously enables and constrains modern laundering practices.

5.2 Cyber Vulnerabilities in Compliance Systems

Within the money-laundering lifecycle, numerous layers and scenarios create opportunities for cyber-enabled criminal activity. Weak due diligence systems, compromised credentials, inadequate cross-system controls, and the lack of integration between cybersecurity functions, compliance teams, and AML risk assessments represent only a fraction of the vulnerabilities embedded in banking compliance architectures - vulnerabilities that are routinely exploited in sophisticated fraud and laundering schemes.

Some of the most prominent challenges are those related to regulations and compliance. Constant updates and increasing complexity in global AML regulations make it progressively more challenging for institutions to remain compliant across multiple jurisdictions while simultaneously supporting robust cybersecurity measures and maintaining effective compliance processes that meet all regulatory requirements. Furthermore, these adjustments can delay the implementation of new cybersecurity safeguards, providing cybercriminals with temporary opportunities to perform complex criminal processes such as routing funds through intricate chains: creating multiple accounts, navigating through different jurisdictions, and mixing services. Since most monitoring systems rely on established, “known” patterns, their ability to detect new criminal schemes is already limited. When these systems are simultaneously constrained by technological and global coordination barriers, identifying emerging cross-asset or cross-platform laundering patterns becomes even more challenging.

Technological barriers also pose a challenge to actively preventing fraud, with emerging markets and legacy systems contributing to the challenges of integrating cybersecurity measures. Many institutions rely on outdated technology and equipment, or their infrastructure lacks the level of cybersecurity needed to actively integrate and support modern AML technologies, providing criminals with even more opportunities to exploit these vulnerabilities.

Lastly, coordination and collaboration issues impede the effective implementation of necessary measures. As briefly noted above, differing regulatory frameworks and cooperation practices among financial institutions, regulatory bodies, and law enforcement complicate cross-border AML efforts. They also underscore the need for stronger collaboration and timely information-sharing to counter increasingly complex financial crime methods, particularly those facilitated by digital platforms and AI (Kendra et al., 2024).

5.3 Criminal Use of Encryption, Anonymity Tools, and Communication Technologies

Criminals use a variety of technologies to conceal and encrypt data from law enforcement. Encryption tools, remote data-storage (often supported by keyloggers, memory-capture software, or hardware interception devices), and anonymous digital payment systems are frequently exploited and continually refined to support increasingly sophisticated schemes. As a result, forensic investigators are left with little or no recoverable evidence in approximately 60% of cases (Balogun & Zhu, 2013).

While the main purpose of encryption was to enable people to protect their confidentiality and block out criminal activity, it is also used by criminals themselves, keeping them out of reach of law enforcement and judicial authorities. The most accessible methods, such as end-to-end encryption (E2EE) and user-only access, guarantee that only the communicating parties can decrypt and access the content of the conversations, thus allowing criminals to “go dark” and restrict law enforcement’s ability to obtain crucial evidence and information from messengers, even with warrants or court orders. Moreover, in recent years, the development of quantum computers is expected to have a profound impact on cryptography. Through quantum algorithms, law enforcement will be able to access previously heavily protected and encrypted information, such as databases, protected files, and communications data, by breaking cryptographic protocols, guessing complex passwords and deciphering digital keys (EU Innovation Hub for Internal Security, 2024). From a law enforcement perspective, quantum computers can open up a completely new side for forensic

investigations, providing access to relevant electronic evidence previously unattainable due to different forms of encryption.

Among other anonymity tools used, the most complex and multifaceted are cryptocurrencies and virtual assets. With few current laws and regulations on cryptocurrency markets, the main peculiarities of cryptocurrencies are decentralisation, highly speculative nature, and self-regulation, thus providing the perfect environment for fraud with identity concealment (Nizzoli et al., 2020). Virtual assets are entirely digitalised, making them easily transferable, with no strict requirement for true identification information (Koutsoupia, 2023). These technical characteristics make it very difficult to use traditional AML mechanisms in an attempt to combat money laundering, with challenges arising, such as the mode of confiscation of the crypto-assets and tracing of the whole chain of transactions, with many cross-account and cross-platform transaction flows used to conceal true identities.

With schemes becoming more complex and multi-layered, involving different forms of digital identity concealment and transaction encryptions through E2EE and anonymous digital cash flows, authorities need to employ more elaborate mechanisms to identify these frauds while avoiding exposure of sensitive information about individuals not directly involved in the schemes, and remaining consistent with legal and ethical standards.

5.4 Cyber Models Used to Facilitate Money Laundering

Digital transformation has expanded the architecture of money laundering beyond traditional banking channels. In cyberspace, illicit actors no longer depend solely on intermediaries or physical transfers; instead, they manipulate technological infrastructures to conceal the origin, ownership, and destination of funds. The same innovations that power legitimate digital finance have been strategically repurposed to create opacity by design (Dogan, 2024). The models examined represent the main technological frameworks that enable concealment, each illustrating a distinct layer of the laundering process within the cyber ecosystem.

1. **Encryption Models**

The proliferation of encrypted communication technologies has profoundly reshaped the conditions for privacy in the digital environment. While essential to safeguard privacy and freedom of expression, such tools are increasingly exploited by organised criminal networks to coordinate seamlessly across geographical boundaries. Encrypted messaging apps, including *SkyECC*, *EncroChat* and *Telegram,* offer secure channels for criminal entities

to plan and execute operations without the immediate threat of interception. In addition, when encrypted communications are combined with other digital infrastructures, such as cryptocurrencies, the resulting information asymmetries further obscure illicit financial flows (Bardet, 2025). Investigations into platforms such as *EncroChat* have shown that dedicated devices were often modified to maximise operational security. These typically lacked cameras, microphones, GPS modules, USB ports and included features such as automatic message deletion.

Regulatory arbitrage, the deliberate structuring of activities to exploit inconsistencies across jurisdictions, becomes particularly salient within the fragmented legal landscape surrounding cross-border responsibilities. Cross-border cooperation is often slow and inefficient, a particularly problematic topic due to the transient nature of the data that allows remote deletion or manipulation. For instance, *Telegram* is incorporated in the British Virgin Islands while maintaining an operational headquarters in Dubai, illustrating the complexities of multi-jurisdictional oversight (Bardet, 2025). *Operation BULUT* exemplifies a successful data-driven operation: coordinated action by European authorities and Türkiye dismantled four major criminal networks that facilitated drug flows into the EU and Türkiye, the operation built on intelligence extracted from *SkyECC* and *ANOM*. French authorities shared decrypted *SkyECC* data with Türkiye to support the development of local investigations, and according to Europol's estimates, over €300 million worth of assets were seized across Türkiye and Europe (Europol, 2019).

2. Anonymity Models

The primary function of anonymity tools is to safeguard users' identities through the application of advanced encryption and obfuscation techniques, providing a digital refuge for those seeking to conceal their activities. The dark net represents a concealed stratum below the deep web within the internet protocol hierarchy, inaccessible to conventional search engines such as *Google* or *Yahoo*, but requiring specialised software, most notably *The Onion Router* (*Tor*). Accounting for approximately 95% of total web content, the dark net's scale underscores its significance; according to a recent Cloudflare report, roughly 94% of requests originating from the *Tor* network display patterns consistent with cybersecurity threats (Saleem et al. 2023). Anonymity systems within the dark net are generally classified into two categories. High-latency systems, such as the *Mixmaster protocol*, offer superior protection against traffic analysis by employing mixing, reordering, and batching techniques to obscure data origins and destinations. On the other hand, low-latency systems, such as *Tor*, minimise delays to support real-time applications like HTTP browsing, balancing usability with

reduced privacy protection (Gaballah et al., 2024). To illustrate how anonymity is maintained in practice, the *Tor* network serves as a representative model. Founded upon the Transmission Control Protocol (TCP), *Tor* employs a multi-hop technique to establish communication links: within preexisting communication pathways, *Tor* will employ a stochastic process to designate a set of relay nodes, no less than three. Individual nodes possess knowledge only of their immediate predecessor and successor, and the network's topology is continuously reshuffled to prevent correlation attacks. Data transmitted through this pathway is simultaneously enveloped in multiple layers of encryption, ensuring that even if one node is compromised, the remaining layers preserve confidentiality; this approach commonly referred to as onion routing (Saleem et al. 2023). Beyond the dark net, anonymity may also be achieved through Virtual Private Networks (VPNs) and Domain Name System (DNS) masking, which conceal user identities and locations across the broader web.

3. Blockchain Obfuscation Models

Blockchain obfuscation refers to a collection of techniques and tools designed to conceal transaction trails, ownership, or transferred amounts within blockchain networks. Cryptocurrencies serve as the primary medium through which blockchain obfuscation operates. Although each blockchain transaction leaves a permanent public record, these obfuscation techniques have emerged as a countermeasure to restore privacy.

While cryptocurrencies have revolutionised the efficiency of traditional financial transactions and decentralised them, they have simultaneously exposed regulatory and legal gaps that criminal actors readily exploit. The decentralised and pseudonymous character of cryptocurrencies makes them a pivotal tool for money laundering. Within this bodywork, "privacy coins" constitute a distinctive class of cryptocurrencies with enhanced anonymity. The two most popular examples, *Monero* and *Zcash,* employ cryptographic protocols that effectively sever traceability: *Monero* uses Ring Signatures, which obscure a transaction by merging multiple users' signatures, while *Zcash* employs Zero-Knowledge Proofs that allow transactions to be verified without disclosing the parties' identities or the amount of money exchanged (Longa, 2025).

Beyond privacy coins, cryptocurrencies utilise a suite of Privacy-Enhancing Technologies (PETs) to further complicate the tracking process, such as shielded transactions and stealth addresses (Longa, 2025). These features collectively enable the creation of an opaque environment resistant to forensic scrutiny. A historical precedent for such practices emerged with the *Silk Road* darknet marketplace, which relied extensively on Bitcoin to facilitate illegal commerce and launder proceeds. Given Bitcoin's inherently transparent

ledger, *Silk Road* operators employed tumblers and mixers - services that mix cryptoassets from a multitude of users into centralised utility pools to break the trace between the origin and the destination. In this way, *Silk Road* effectively fragmented transactional links, making the tracing of illicit financial flows extremely difficult. Modern analogues of these services, such as *Tornado Cash*, have expanded the scale and sophistication of obfuscation. *Tornado Cash* alone has reportedly mixed over USD7.1 billion in cryptoassets, demonstrating the persistence and magnitude of such laundering mechanisms (Manning et al., 2024).

Related practices include chain and asset hopping, which involve the transfer of funds across different cryptocurrencies or blockchains. The most common method is to use multiple wallets, engaging in a series of transactions across several intermediaries, referred to as "hops". The second, namely "Peel chains", involves the siphoning of small amounts of cryptocurrencies into a new wallet at every iteration, structuring funds into micro-transactions (Manning et al., 2024). The use of cold wallets, which operate outside of custodial exchanges and therefore lack Know-Your-Customer (KYC) oversight, further enhances anonymity. These methods are frequently facilitated through intermediaries or "mules", who conduct transactions on behalf of primary offenders to obscure direct involvement.

A more recent and rapidly expanding frontier of digital laundering involves Non-Fungible Tokens (NFTs). NFTs represent digital ownership of assets such as art, music, and gaming items, and can serve as conduits for transforming illicit funds into ostensibly legitimate crypto holdings. In simple schemes, NFTs are purchased with illicit funds and sold to unknowing buyers for "clean" crypto. More sophisticated methods include trace-based money laundering (TBML), in which fabricated NFT transactions simulate commercial activity. The rapidly fluctuating NFT prices are used to cover the creation of worthless NFTs, which are subsequently traded between criminals at inflated prices, disguising TBML as trading profits (Manning et al., 2024).

5.5 Cyber Models Used to Combat Money Laundering

As financial crime has migrated into digital environments, enforcement agencies, regulators, and private institutions have developed their own technological architectures to adapt to this change. The following frameworks aim not merely to trace single transactions but to reconstruct entire laundering networks across jurisdictions and digital platforms.

1. **Blockchain Tracing Models**

Blockchain tracing models represent distributed ledgers as graphs, in which addresses and clusters are nodes, and value transfers are directed edges. Analysts apply clustering heuristics, path and community detection, taint/flow propagation, and temporal motif analysis to reveal layering patterns such as peel chains, mixer usage, and cross-chain "hops". Recent surveys synthesise these techniques, catalogue their assumptions, and identify open challenges around address clustering reliability, entity labelling, cross-asset tracing, and privacy-enhancing technologies (Kumar & Thing, 2025; Azad & Lallie, 2024). In practice, tracing is an iterative process: parse ledgers, construct transaction graphs, cluster likely co-controlled addresses, score paths by probabilistic heuristics, and generate human-auditable evidence. The operational value of tracing increases when results are explainable (rule-based heuristics with confidence metrics), scalable (to multi-year, multi-chain corpora), and reproducible (stable parsing, versioned labels). The literature stresses that graph outputs are probabilistic and must be treated as investigative leads rather than definitive proof absent verification (Azad & Lallie, 2024). Policy-relevant observations include persistent observability gaps for privacy coins and obfuscation services, emphasising the need to combine on-chain models with off-chain evidence (Kumar & Thing, 2025).

2. OSINT-Fusion Models

Since legal identity and beneficial ownership are established off-chain, on-chain analytics must be combined with external data to support attribution and legal action. Open-source intelligence (OSINT) models integrate registry data, beneficial-ownership disclosures, sanctions, and politically exposed persons (PEP) lists, corporate filings, and investigative records with transaction graphs. Methodologies typically proceed as follows: (i) derive clusters and transaction motifs from the ledger; (ii) extract candidate identifiers; (iii) enrich with open records; and (iv) iterate through analyst review and hypothesis testing. At scale, this workflow benefits from standardised schemas and resolvable identifiers, enabling robust entity resolution and cross-jurisdictional comparisons. OSINT-fusion is particularly effective in multi-episode investigations, where separate data releases or records, such as leak-derived documents and sanctions updates, can be co-indexed and time-aligned to reveal networks rather than isolated transactions (Gertenbach et al., 2024).

3. AI-driven anomaly detection

Financial institutions increasingly deploy machine-learning models to complement rules-based monitoring. In cryptocurrency contexts, graph-based learning has emerged as a baseline, with studies demonstrating that graph convolutional networks and related architectures improve the detection of illicit patterns on transaction networks relative to

flat-feature models (Mousavian & Miah, 2025). In fiat and mixed-asset settings, comparative analyses show that ensembles (e.g., gradient-boosted trees) perform well when high-quality labels exist, while unsupervised or semi-supervised approaches (e.g., isolation-based methods, community-aware scoring) are advantageous under severe label scarcity and extreme class imbalance (Ajagbe et al., 2025). Two implementation themes recur. First, data realism: institutions often rely on simulators and synthetic corpora to prototype models because production labels are sparse and protected; model validation must therefore include careful performance transfer checks (Mousavian & Miah, 2025). Second, operational lift: beyond AUC/precision-recall metrics, programs should measure analyst workload effects (e.g., alerts per case resolved, time-to-decision), false-positive reduction, and the stability of explanations under drift (Ajagbe et al., 2025). Model outputs should be routed into case-management systems with feedback loops so that investigator dispositions improve future training data.

4. Model Limitations

Across these models, several limits persist. Attribution uncertainty, especially for clustering heuristics and third-party label imports, requires conservative interpretation and corroboration (Azad & Lallie, 2024). Coverage gaps, such as privacy coins, mixers/bridges, and cross-chain protocols, reduce observability and motivate hybrid investigations that join on-chain and OSINT evidence (Kumar & Thing, 2025). Data drift and adversarial adaptation demand periodic re-tuning, red-teaming, and post-deployment monitoring (Mousavian & Miah, 2025). Finally, evaluation remains uneven: public benchmarks rarely reflect production alert bases; future work should prioritise shared, privacy-respecting evaluation frameworks and reporting standards that capture operational impact (Ajagbe et al., 2025).

5.6 The Panama Papers and FinCEN Cases - Cyber Dimension

In this subsection, two real-world cases are examined to illustrate how cybersecurity methods, digital forensics, and open-source intelligence (OSINT) have been deployed to uncover hidden laundering networks. The leak of the Panama Papers is one of the clearest demonstrations of how digital evidence, when processed through forensic and cyber-analytical pipelines, can expose global financial misconduct. The data ingestion phase relied on large-scale extraction and indexing tools such as *Apache Tika* and *Solr*, enabling collaborators to search across names, addresses, company numbers, and dates. The investigative team then performed entity resolution, creating a unified schema representing

officers, corporate entities, intermediaries, and addresses; duplicates across languages and formats were consolidated into canonical nodes (Cabra, 2016; Hunger & Lyon, 2016). The normalised data was stored in a *Neo4j* graph database and interrogated using Cypher queries to identify beneficial-ownership proxies, nominee structures, and multi-layered offshore chains. Linkurious facilitated visual exploration, allowing investigators to detect hubs, cross-jurisdictional connections, and recurring structural motifs (Linkurious, 2016). Finally, a curated subset of the leak was released through the ICIJ's Offshore Leaks database, enabling public scrutiny and further enrichment through OSINT sources.

Another example of the use of cybersecurity tools and methods to combat money laundering is the FinCEN Files. After another whistleblower leaked thousands of U.S. Suspicious Activity Reports (SARs), a global consortium of investigative journalists applied a digital-forensics workflow similar to that used in the Panama Papers. The SARs were first ingested and indexed through secure platforms such as ICIJ Datashare. More than four hundred spreadsheets and tens of thousands of narrative descriptions were normalised to harmonise counterparties, account numbers, routing identifiers, and jurisdictions (Hunger, Lyon, & Van Bruggen, 2020). Using *Neo4j* for storage and querying, and *Linkurious* for visual analytics, the team constructed a transaction-centred knowledge graph that linked banks, correspondents, shell structures, wire transfers, and transaction timestamps. Additional features extracted from SAR narratives, such as references to shell companies, oligarch networks, and high-risk geographies, were layered onto the graph to identify high-priority pathways and suspicious communities. Temporal and network-analytic techniques were applied to reveal delays between suspicious transactions and SAR filings, as well as routing patterns that exposed systemic deficiencies in monitoring and enforcement (Díaz-Struck et al., 2020). Finally, the entities identified in the graph were cross-referenced with sanctions lists, court filings, corporate registries, and prior leaks through OSINT platforms, including ICIJ Datashare and OCCRP Aleph, which strengthened attribution and produced detailed investigative chronologies.

These cases demonstrate how the same digital infrastructures that afford opacity also generate analyzable data exhaust, which, when processed with cybersecurity tools, can expose and disrupt laundering networks. Yet these investigations also demonstrate the considerable analytical, technical, and collaborative effort required to transform fragmented digital evidence into actionable intelligence, underscoring both the promise and the difficulty of cyber-enabled financial investigations.

6 The Four-Pillar Money Laundering Model: An Integrated Framework

6.1 Model Overview

The *Four-Pillar Money Laundering Model* put forward in this paper conceptualises global money laundering as a system maintained and reproduced through the interaction of four self-reinforcing dimensions: the behavioural, legal, cyber, and financial pillars. Each pillar captures one particular but interdependent set of mechanisms in view of which illicit capital can circulate, mask its origin, and eventually be legitimised within the formal economy. The model illustrates that laundering is not a single-process crime but rather a complex adaptive system shaped by human behaviour, institutional design, technological infrastructures, and global economic structures all at once.

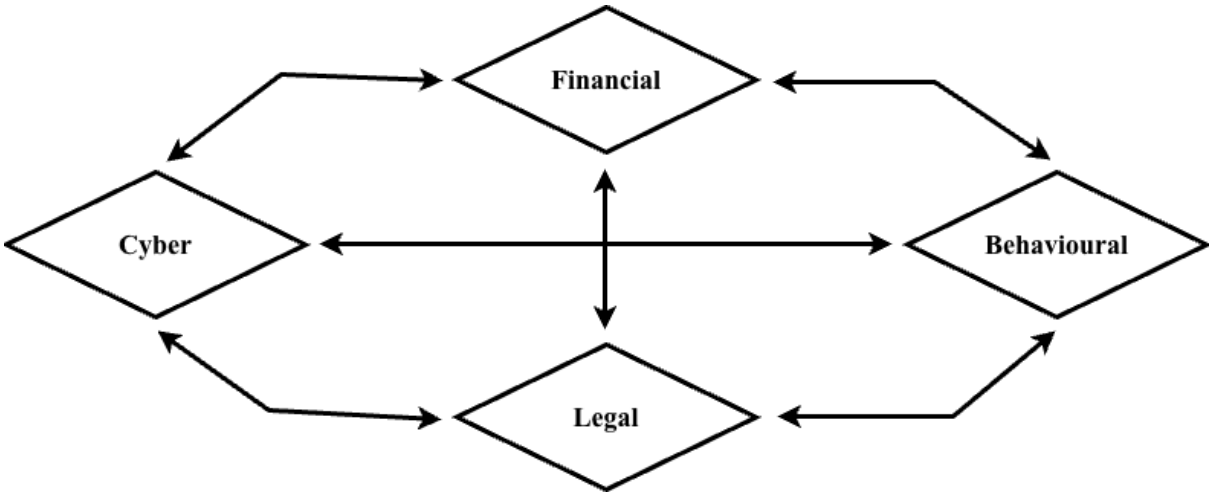

Figure 1: *Four-Pillar Money Laundering Model*

6.2 Financial Pillar

The *Financial Pillar* represents economic and banking structures that enable illicit funds to be moved, transformed, and ultimately integrated into the legitimate economy. It is driven by several core mechanisms, such as corresponding banking networks that facilitate cross-border transfers; shell companies and trusts which obscure beneficial ownership; offshore financial centres that provide secrecy and lenient regulations; and real estate markets which absorb illicit proceeds.

While other pillars explain the motivations, enablers and technological support of laundering, the financial dimension is where illicit value is formally reintroduced into the legal economy. It completes the laundering cycle and allows the capital to circulate, accumulate and sustain long-term crime.

The *Financial Pillar* is necessarily connected with the model's other components. Behavioural dynamics influence how actors select financial instruments. The legal structure shapes the opportunities that are available within financial systems, as regulatory gaps or inconsistent oversight offer exploitable entry points. Finally, the cyber pillar amplifies the operations by accelerating transfers, increasing anonymity, and enabling complex layering. This reinforces why financial infrastructure works as an integral part of the system rather than a freestanding mechanism.

6.3 Behavioural Pillar

The *Behavioural Pillar* reflects the psychological, cognitive, social, and cultural mechanisms by which people and institutions rationalise and normalise money laundering. It demonstrates how human-driven processes, such as institutional culture, moral disengagement, and rationalisation, turn illegal financial conduct into an everyday organisational routine. This pillar highlights that money laundering persists not only due to defective processes, but also because people interpret illegal behaviour as acceptable, legitimate, or the proper way of doing business.

Within this framework, the human dimension can be analysed through five distinct components: greed and self-interest driving the actions of politicians, entrepreneurs, and executives; offenders constructing an elaborate armour of justifications to preserve their psychological integrity; moral disengagement, which transforms fraud into a cognitive habit through collective dynamics; institutional complicity normalising immoral behaviour through implicit norms and established practices; and justification, employees believing they are doing right by the company, or seeing it as a means of career advancement. These factors make laundering psychologically sustainable inside institutions, allowing financial complexity, legal fragmentation, and cyber opacity to work together as a durable global architecture of illicit finance.

The same psychological drivers that sustain this behaviour internally also extend outward, shaping the other three dimensions of the model. Moral disengagement allows fraudsters to aggressively exploit financial loopholes, thus resulting in a rationalisation of the

use of shell companies. Skills encompassed within "capability" mentioned in the *Fraud Diamond* (manipulation and ability to deceive) allow for evasion of compliance systems and forged documentation. Human psychology is intertwined with the legal pillar, as evidenced by self-serving lobbyists pushing for regulations that enable financial crime, as seen in Enron's exploitation of deregulation passed in California (Clark & Demirag, 2002). The behavioural pillar also influences the cyber dimension: cognitive biases towards anonymity facilitate the adoption of cyber-enabled money laundering. These individuals share a belief that blockchain mixers, darknet markets or privacy tools ensure invulnerability. Moral restraint online is also greatly reduced: distance from victims makes digital finance crime feel more acceptable. Ultimately, human factors persist despite technological or legal safeguards: money laundering remains fundamentally enabled by people, such as operators, facilitators and regulators.

6.4 Legal Pillar

The *Legal Pillar* encompasses all the regulatory frameworks, institutional structures, and jurisdictional dynamics which either impede or facilitate money laundering. Whereas legal systems establish the formal obligations of prevention, detection, and repression, their actual effectiveness hinges upon coherence, enforcement, and the capacity to adapt to evolving financial and technological landscapes. Where there is fragmentation, obsolescence, or inconsistent enforcement of legal structures, they inadvertently provide the space in which other pillars will operate. Key vulnerabilities include beneficial ownership secrecy and opaque corporate structures; regulatory capture, political influence, and institutional weakness; cross-border enforcement failures and jurisdictional conflicts; and over-reliance on professional enablers, such as lawyers, notaries, and accountants.

The *Legal Pillar* interacts closely with all other components of the model by shaping the structural environment in which laundering occurs. Legal loopholes and fragmented enforcement reduce the perceived risk of detection, enabling rationalisation, moral disengagement, and institutional complicity to flourish. Weak or inconsistent regulations create the psychological space in which illicit behaviour becomes normalised within professional and corporate cultures. Technicalities such as beneficial ownership secrecy, inconsistent due diligence requirements, and uneven cross-border supervision directly enable the creation of shell companies, offshore entities, and complex ownership chains. The financial mechanisms depend on legal ambiguity to function, making the legal system an

essential enabler of layering and integration processes. Lastly, the slow pace of regulatory adaptation allows criminals to exploit emerging technologies, privacy tools, and digital assets before legislation can respond. Legal blind spots regarding virtual assets and encrypted communication create fertile ground for cyber-enabled laundering. The *Legal Pillar* influences both the boundaries of opportunity within a financial and cyber system, and shapes behavioural choice by increasing or reducing the perceived risk of detection.

6.5 Cyber Pillar

The *Cyber Pillar* illustrates the main digital infrastructures, tools, and models used in the money-laundering landscape, through which criminals conceal their financial transactions and digital traces and, on the other hand, through which legal authorities are able to identify and expose them.

At its core, the *Cyber Pillar* examines two opposing sets of technological models. The first includes cyber tools used *for* laundering: end-to-end encrypted messaging systems; dark-net anonymity networks such as *Tor*; blockchain obfuscation techniques, including mixers, privacy coins, chain-hopping and peel chains; and the misuse of virtual assets and NFTs to disguise the origin of value.

The second group comprises tools used *against* laundering: blockchain-tracing models that turn ledgers into analyzable transaction graphs, OSINT-fusion workflows combining off-chain records with on-chain patterns, AI-driven anomaly-detection systems that highlight suspicious flows at scale, and leak-forensics pipelines such as those employed in the Panama Papers and FinCEN Files investigations. These techniques demonstrate how digital opacity always produces a data exhaust that can be indexed, modelled, and ultimately leveraged to disrupt laundering networks.

Cyber tools enable money launderers to exploit legal blind spots and loopholes, overcoming vulnerabilities in compliance systems. With legislation taking more time to update and evolve than digital tools, criminals gain time to exploit virtual assets, new forms of cryptocurrencies and inconsistent standards for virtual asset service providers. Cyber systems also allow the financial area to expand rapidly, by increasing the number of virtual wallets one person can manage and providing flexibility in geographical and temporal terms, since the system becomes more digitalised and not fixed to a certain location or timezone. Cyber tools also facilitate the creation of new laundering channels by facilitating transactions, allowing fast cross-asset and cross-account operations and exploiting new cryptocurrencies.

Moreover, cyber anonymity lowers the perceived risk of having your digital traces and operations detected or your assets frozen. With digital dashboards, encrypted messages, and virtual wallets, a person feels that they are in control and can fully oversee all operations and processes. This affects the people's behaviour, engaging in riskier and more serious money-laundering schemes, and feeling a false sense of certainty about remaining undetected.

7 Conclusion

This paper set out to understand how global laundering networks operate as resilient transnational systems by analysing their financial, behavioural, legal, and cyber dimensions. Across all four perspectives, the findings consistently reveal that money laundering persists not because of isolated failures, but because of the systemic interaction of mechanisms that enable illicit capital to circulate, conceal itself, and ultimately enter the legitimate economy.

The findings carry several policy implications. Stronger and more harmonised beneficial-ownership transparency, improved cross-border supervisory cooperation, and clearer alignment between privacy protections and enforcement needs would help close identified legal and institutional loopholes. Expanding cyber-forensic capacity would help counter the increased complexity of technologically enabled laundering. Within organisations, reforms aimed at strengthening compliance cultures and reducing behavioural enablers such as motivated blindness and diffusion of responsibility are crucial for preventing internal facilitation of criminal networks.

These results also hold broader implications for forensic finance and global governance. The persistence of laundering networks highlights the limits of current detection paradigms and underscores the importance of integrating behavioural, legal, and cyber evidence into financial investigations. At the societal level, the findings show how illicit finance reinforces global inequality by diverting public resources and weakening state institutions, while also eroding democratic governance through opacity and corruption. Digital transparency initiatives have the potential to mitigate some of these effects, but only if implemented with adequate safeguards and coordinated oversight.

Future technological and AI-driven developments could transform the laundering landscape in both ways. Advanced automation, privacy-enhancing technologies, and rapidly evolving digital assets may increase opportunities for concealment and cross-platform mobility of illicit funds. At the same time, AI-supported anomaly detection, network analysis,

and large-scale data integration could strengthen investigative capacity. Whether crime or enforcement ultimately benefits will depend on the speed at which regulatory frameworks and investigative tools adapt relative to technological innovation.

In summary, this paper introduces a unified framework that accounts for the persistence of global laundering networks and underscores that effective reform must operate simultaneously across financial, legal, behavioural, and cyber domains. By articulating the interconnected mechanisms that sustain illicit finance, the *Four-Pillar Money Laundering Model* provides a conceptual basis for advancing interdisciplinary research and guiding the development of more coherent, system-oriented policy strategies.

8 Bibliography

Ajagbe, S. A., Majola, S., & Mudali, P. (2025). *Comparative analysis of machine learning algorithms for money laundering detection*. *Discover Artificial Intelligence, 5*, 144.

Aliprandi, G., Busschots, T., & Oliveira, C. (2023, December). Mapping the global geography of shell companies. *EU Tax Observatory*.

American Institute of Certified Public Accountants. (2002). *Statement on Auditing Standards No. 99: Consideration of fraud in a financial statement audit*.

AML Network. (2025, September 12). *What is currency smuggling in anti-money laundering?*

AML Network. *(2025, October 25). Shell company money laundering: Identification and regulatory overview.*

Ashforth, B. E., & Anand, V. (2003). The normalization of corruption in organizations. *Research in Organizational Behavior, 25*, 1-52.

Azad, M. A., & Lallie, H. S. (2024). *Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions*. *Electronics, 13*(17), 3568.

Bahaj, W., Adekola, P., Voso, M. T., & Johnson Mary, B. (2025). The political economy of AML scandals: Investigating how corruption, state capture and weak institutions enabled laundering at a national scale. ResearchGate.

Balogun, A. M., & Zhu, S. Y. (2013). *Privacy impacts of data encryption on the efficiency of digital forensics technology*. *International Journal of Advanced Computer Science and Applications, 4*(5).

Banca d'Italia. (n.d.). *Ruolo e funzioni della Banca d'Italia*.

Bandura, A. (2011). Moral disengagement. In *The encyclopedia of peace psychology*. Wiley.

Bank for International Settlements. (2019). Compliance and financial stability (BIS Working Paper No. 811).

Barnett, N., & Sloan, A. (2018). Democracy in the crosshairs: How political money laundering threatens the democratic process. *Atlantic Council*.

Bardet, L. (2025). *From shield to sword: Encryption, organized crime, and transnational legal gaps*. London School of Economics.

Berry, M., & Gundur, R. V. (2025). Money laundering plays a key role in every part of the illegal drugs industry - here's how it works. *The Conversation*.

Bjerregaard, E., & Kirchmaier, T. (2019). *The Danske Bank money laundering scandal: A case study*. *SSRN Electronic Journal*.

Cabra, M. (2016, May 12). *How the ICIJ used Neo4j to unravel the Panama Papers*. Neo4j.

Carabaña, C. (2025). Mexican cartels' new money laundering businesses: Cryptocurrencies, concerts and timeshares. *El País English*.

Cassella, S. D. (2018). *Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete? Journal of Money Laundering Control, 21*(4), 494-497.

Charlopova, I., Andon, P., & Free, C. (2020). How fraud offenders rationalize financial crime. In *Corporate fraud* exposed (pp. 39-59). Emerald Publishing.

Clark, W. W., & Demirag, I. (2002). Enron: the failure of corporate governance. *Journal of Corporate Citizenship*, (8), 105-122.

Consiglio Nazionale del Notariato. (n.d.). *Responsibilities of the notary*.

Consilium of the European Union. (2024). *Lotta al riciclaggio e al finanziamento del terrorismo nell'UE*.

Cressey, D. (1973). Other people's money: A study in the social psychology of embezzlement. *Patterson Smith*.

Dani, A., & Kollwitz, E. (2025). Fraud justification and the psychology of convicted financial criminals.

Denetro Fragoso, E. (2012). From cash to cards: How the 2012 Anti-Money Laundering Law moved money laundering to debit cards in Mexico.

Dewdney, A. K. (1989, March). *Computer recreations: Of worms, viruses and Core War. Scientific American, 260*(3), 110.

Dipartimento per le Politiche Antidroga. (n.d.). *Homepage*. www.politicheantidroga.gov.it

Díaz-Struck, E., Armendariz, A., Reuter, D., Cosic, J., Kehoe, K., Torres, M., Williams, M., & Fiandor Gutiérrez, M. (2020, September 20). *From a jumble of secret reports,*

damning data on big banks and dirty money. International Consortium of Investigative Journalists (ICIJ).

Dogan, K. H. (2024). *Corruption, bribery, and money laundering: Global issues*.

Dupire, C. (2025, September 26). Waking up to the AML challenges presented by correspondent banking - how the EU Global Facility is working with partner countries. EU AML/CFT Global Facility.

Dupuy, K., & Neset, S. (2018). The cognitive psychology of corruption: Micro-level explanations for unethical behaviour. *CHR. Michelsen Institute - U4 Anti-Corruption Resource Centre*.

Eboh, C., & Jones, M. (2021, March 17). *Nigeria's OPL 245 oilfield licence at heart of bribery cases*. Reuters.

ENI S.p.A. (n.d.). *The OPL 245 case: Legal proceedings in Nigeria*.

EU Innovation Hub for Internal Security. (2024, June 10). *First report on the use of encrypted communications in criminal investigations*.

European Bank for Reconstruction and Development. (2024). Correspondent banking: Factsheet.

Europol. (2019). *Encrypted app intelligence exposes sprawling criminal networks across Europe: Over 230 arrested as authorities dismantle drug pipelines and logistical structures*. Europol.

Europol. (2021). Shadow money: The international networks of illicit finance (Europol Spotlight). *Publications Office of the European Union*.

Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020, September). Electronic money laundering, the dark side of fintech: An overview of the most recent cases. In *Proceedings of the 2020 12th International Conference on Information Management and Engineering* (pp. 29-34).

Federal Bureau of Investigation. (2019). *Crime in the United States 2019: Table 43 — Arrests by race and ethnicity, 2019*.

Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations.*

Financial Action Task Force. (2023). *Guidance on beneficial ownership transparency for legal arrangements*.

Financial Action Task Force. (2024, March). *Guidance on beneficial ownership and transparency of legal arrangements (Recommendation 25)*. FATF/OECD.

FATF, Egmont Group, Interpol, UNODC. (2025, September 5). International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook.

Financial Crime Academy. (2025, September 15). Shell company, shelf company and front company.

Financial Crime Academy. (2025, October 20). The 1MDB money laundering scandal and corrupt politicians.

Financial Crime Academy. (2025, September 23). The artful deception: Understanding money laundering in art auctions.

Financial Secrecy Index. (n.d.). Financial secrecy index.

Fuller, J., & Jensen, M. (2002). Just say no to Wall Street: Putting a stop to the earnings game. *Journal of Applied Corporate Finance, 14*(4), 41-46.

Gaballah, S. A., Abdullah, L., Mühlhäuser, M., & Marky, K. (2024). *Let the users choose: Low latency or strong anonymity? Investigating mix nodes with paired mixing techniques* (pp. 1-11). TUbilio, Technical University of Darmstadt.

Gertenbach, W., Botha, J., & Leenen, L. (2024). *A proposed high-level methodology on how OSINT is applied in blockchain investigations*. *International Conference on Cyber Warfare and Security, 19*(1), 75–83.

Gilmour, P., Omondi, B., Alkaç, H. F., Han, B., Carre, A., Kapardis, D., & Halfpenny, C. (2024). Reexamining the “placement-layering-integration” model of money laundering.

Gross, E. (1978). Organizational crime: A theoretical perspective. In *N. K. Denzin (Ed.), Studies in symbolic interaction* (Vol. 1, pp. 55-85). JAI Press.

Huber, W. D. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. ResearchGate, 12(2), 28-49.

Hunger, M., & Lyon, W. (2016, April 8). *Analyzing the Panama Papers with Neo4j: Data models, queries & more*. Neo4j.

Hunger, M., Lyon, W., & Van Bruggen, R. (2020, September 22). *Analyzing the FinCEN Files with Neo4j*. Neo4j.

International Consortium of Investigative Journalists. (2016, April 3). Giant leak of offshore financial records exposes global array of crime and corruption.

International Consortium of Investigative Journalists. (2016). New Panama Papers leak reveals Mossack Fonseca’s chaotic scramble.

International Monetary Fund. (2023). 2023 review of the Fund's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) strategy (*Policy Paper No. 2023/052*).

Isolauri, E. A., & Ameer, I. (2023). Money laundering as a transnational business phenomenon: A systematic review and future agenda. *Critical Perspectives on International Business, 19*(3), 426–468.

Jávor, I., & Jancsics, D. (2016). The role of power in organizational corruption: An empirical study. *Administration & Society*, 48.

Jones, D. S. (2020). 1MDB corruption scandal in Malaysia: a study of failings in control and accountability. *Public Administration and Policy*, *23*(1), 59-72.

Judijanto, L., Mihardianto, M., Herlina, H., Wijaya, I., & Wang, Y. (2024). The Role of Accountants in Sustainable Business Practices. *Journal Markcount Finance*, *2*(2), 240-251.

Kavakli, K. C., Marcolongo, G., & Zambiasi, D. (2023). Sanction evasion through tax havens. *BAFFI CAREFIN Centre* Research Paper No. 212.

Kendra, J., Olabiyi, W., & Ibrahim, A. (2024, October). *Strengthening anti-money laundering and counter-terrorist financing efforts through integrated cybersecurity and compliance measures: A comprehensive framework for financial integrity.*

Klitgaard, R. (2011). *Fighting corruption*. *CESifo DICE Report, 9*(2), 31–35.

Kouchaki, M., & Smith, I. H. (2025). Moral decision-making in organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, 12, 45-72.

Koutsoupia, V. (2023). *Challenges of the use of virtual assets in money laundering*. *Nordic Journal of European Law, 6*(4), 53–78.

Kumar, A., & Thing, V. L. L. (2025). *A survey of transaction tracing techniques for blockchain systems*. arXiv.

LaBrie, R. (2022). White-collar crime: Diversity and discrimination in sentencing. *Seattle Pacific University*.

Liang, W., Mary, B. J., Hamzah, F., Taofeek, A., Mathew, B., & Blessing, M. (2025). The role of cryptocurrency in money laundering: Techniques, typologies, and detection challenges.

Linkurious. (2016, April 5). *Panama Papers: How ICIJ investigated the massive leak with Linkurious*.

Longa, F. E. A. (2025). *Cryptocurrency and money laundering*. *American Journal of Industrial and Business Management, 15*(2), 362-371.

Manning, M., Akartuna, E. A., & Johnson, S. (2024). *Opportunities to future crime: Scoping the future of money laundering and terrorist financing through cryptoassets*. *Technological Forecasting and Social Change, 210*, 123894.

McConnell, P. (2020). Danske Bank - a smorgasbord of risks. *Journal of Business Accounting and Finance Perspectives, 2*(3), 1–35.

MEF Dipartimento del Tesoro. (n.d.). *FATF - GAFI*. https://www.dt.mef.gov.it/it/attivita_istituzionali/prevenzione_reati_finanziari/area_internazionale/fatf_gafi.html

Mousavian, S., & Miah, S. J. (2025). *Review of artificial intelligence-based applications for money laundering detection*. *Intelligent Systems with Applications, 27*, 200572.

Nick Tabor. (2025, October 23). 1Malaysia Development Berhad scandal: Scheme, Jho Low, Najib Razak, exposure, & legacy. *Encyclopedia Britannica*.

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., & Ferrara, E. (2020). *Charting the landscape of online cryptocurrency manipulation*.

Obermayer, B., Obermaier, F., Wormer, V., & Jaschensky, W. (n.d.). *The Panama Papers: Exposing the rogue offshore finance industry*. Süddeutsche Zeitung.

O'Donovan, J., Wagner, H. F., & Zeume, S. (2019). The value of offshore secrets: Evidence from the Panama Papers. *The Review of Financial Studies, 32*(11), 4117-4155.

OMNIO. (2024, May 14). *3 stages of money laundering*.

Organisation for Economic Co-operation and Development. (2024). Beneficial ownership and tax transparency: Implementation and remaining challenges. *OECD & Global Forum*.

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education, 23*(4), 521-533.

Red Flag Alert. (2023). A guide to shell companies. https://www.redflagalert.com/articles/a-guide-to-shell-companies

Remeur, C. (2019, February). Understanding money laundering through real estate transactions. *European Parliament Think Tank*.

Riccardi, M., & Reuter, P. (2024). The varieties of money laundering and the determinants of offender choices. *European Journal on Criminal Policy and Research, 30*(3), 333-358.

Sabatino, M. (2020). Crime treasure islands: Tax havens, tax evasion and money laundering. *Journal of Economics and Business*, 3(1).

Saleem, J., Islam, R., & Islam, Z. (2023). *Darknet traffic analysis: A systematic literature review*. arXiv.

Saliya, C. A. (2025). Combating money laundering: Global challenges, mechanisms, and strategic solutions.

Terrill, J. A. (2014). The Role of Lawyers in Combating Money Laundering and Terrorist Financing: Lessons from the English Approach. *NYL Sch. L. Rev.*, *59*, 433.

Transparency International. (2021). G20 position paper: Transnational corruption and economic organized crime.

Transparency International. (n.d.). Dirty money - Our priorities.

UK Government. (2025, July 31). Guidance on the exemptions from the money laundering obligations and money laundering reporting obligations in the *Proceeds of Crime Act 2002*.

Unità di Informazione Finanziaria per l'Italia. (n.d.). *La UIF nel sistema antiriciclaggio*.

United Nations. (1988). *United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances*.

United Nations Office on Drugs and Crime. (n.d.). Money laundering overview. https://www.unodc.org/unodc/en/money-laundering/overview.html

United Nations Office on Drugs and Crime. (2013). Corruption and integrity challenges in the public sector of Iraq.

United Nations Office on Drugs and Crime. (2025). *World Drug Report 2025: Booklet 1 - Key findings*.

Winkler, C. (2024, April 10). Danske Bank scandal: Turning point for AML compliance of banking sector. *Pythagoras Solutions*.

Wolfe, D., & Hermanson, D. (2004). The fraud diamond: Considering the four elements of fraud.