

Impact of Cybersecurity, Artificial Intelligence, and Corruption on Money Laundering Risk: A Cross-National Quantitative Analysis of Financial Action Task Force Member States

Syed Maaz Ali

ssgroupmaaz@gmail.com

BS-Criminology, Shaheed Zulfiqar Ali Bhutto University of Law

Dr. Syed Khurram Mehdi

khuram.mehdi@szabul.edu.pk

Assistant Professor/Chairman Department of Criminology, Shaheed Zulfiqar Ali Bhutto University of Law

Shahzeb Imdad Ali

shahzaibsanjrani55@gmail.com

BS-Criminology, Shaheed Zulfiqar Ali Bhutto University of Law

Muhammad Maaz Khan

maazkhann090@gmail.com

BS-Criminology, Shaheed Zulfiqar Ali Bhutto University of Law

Corresponding Author: *Syed Maaz Ali ssgroupmaaz@gmail.com

Received: 17-07-2025

Revised: 24-08-2025

Accepted: 12-09-2025

Published: 27-09-2025

ABSTRACT

This study examines the impact of national-level cybersecurity capacity, AI readiness, and corruption on money laundering risk across member countries of the FATF. The study relies on secondary data from well-known sources: the Basel AML Index (for money laundering risk), the National Cyber Security Index (for cybersecurity), the Government AI Readiness Index (for AI readiness), and the Corruption Perceptions Index (for corruption). In total, 36 member states were analyzed. An ordinary least squares (OLS) multiple linear regression was used to test hypotheses. The analysis showed that higher cybersecurity capacity and lower perceived corruption, indicated by higher CPI scores, are significantly linked to lower money laundering risk. However, AI readiness did not show a statistically significant relationship, which goes against theoretical expectations. Together, the model accounted for 55.8% of the variation in money laundering risk among the sampled countries. The study relies on index-based proxy measures, which may not fully reflect the real-world conditions of AI use in AML practices. In addition, the cross-sectional design limits causal inference and temporal analysis. The findings highlight the important roles of strong cybersecurity infrastructure and anti-corruption efforts in reducing money laundering threats. While AI readiness seems statistically insignificant, its practical effect might still matter and calls for more focused metrics and longitudinal research. These insights can help guide FATF policymaking and capacity building by UNODC and inform cross-national AML strategies, especially in improving technological and governance frameworks.

Keywords: Money laundering, cybersecurity, artificial intelligence, corruption, FATF, anti-money laundering, regression analysis.

INTRODUCTION

On September 11, 2005, a notorious terrorist organization, Al-Qaeda, executed a terrorist attack on the World Trade Center in New York, just as the Colombian Medellín cartel was executing their large-scale trafficking of illicit drugs during the 70s to 90s. Regardless of their distinctive objectives, both criminal

organizations require operational funds. From organized criminality to terrorism, a sophisticated offense known as money laundering is a key facilitator to finance operational costs (Lombardo & El Khoury, 2023). The financial crime of dealing with illicit gains and concealing their source is known as money laundering (Jaffery & Mughal, 2020). In the context of money laundering, predicate offenses are those from which criminal proceeds are generated; the money laundering offense should be applied to all significant offenses. At the very least, it covers the 21 types of offenses listed in the FATF's vocabulary, which include tax offenses, fraud, drug trafficking, organized crime, corruption, and bribery (Korejo et al., 2021). In this regard, Wang & Yang (2007) suggest that criminal activities like bribery, smuggling, and drug trafficking often generate substantial profits; however, the obtained illicit proceeds need to appear legitimate before spending. Given the globalized nature of this offense, it has devastating consequences on political instability and economic progress (Alnasser Mohammed, 2021). In recent years, one of the top priorities in anti-crime policies is the fight against money laundering (Rusanov & Pudovochkin, 2021). Under the canvass of money laundering, it is essential to note that discussing anti-money laundering efforts is incomplete without considering the combating financing of terrorism and counter-proliferation financing aspects. In this regard, Terrorism financing refers to the methods that exploit weaknesses in the financial system and remain anonymous; it involves obtaining and providing proceeds to fund terrorist activities (International Monetary Fund, 2023). Similarly, proliferation financing refers to the provision of money or financial assistance for the development of WMD, such as CBRN weapons (ACCA, 2022). Despite many differences, proliferation, terrorism financing, and money laundering often uses similar defects in the financial system. One key difference that sets money laundering apart from terrorism financing and proliferation financing is that the money involved in money laundering must be illegally obtained; however, in terrorism financing and proliferation financing, it is not necessary but is often the case (International Monetary Fund, 2023).

For a better understanding, this sophisticated and complex crime of money laundering is demonstrated as a process. Regardless of the variety of available laundering schemes, the technique is generally divided into three stages: placement, layering, and integration (Unger & Ferwerda, 2011). These stages can be elaborated as follows: By accumulating the illicit proceeds through predicate offenses, proceeds are injected into the financial system in the placement stage, and then obscuring techniques are used in the layering stage through accounting, bookkeeping, offshore accounts, etc., depending on the scheme. In the last stage, integration takes place in which criminal proceeds, often called "black money," appear as legitimate funds for spending, often generally called "white money" (Levi & Reuter, 2006; Korejo et al., 2021). It is important to note that the process of money laundering can be cyclic to fund more criminal activities (Unger & Ferwerda, 2011).

Global trade is one of the many ways that money earned illegally can be laundered, and this technique is often called trade based money laundering, or TBML as an acronym. Basically, TBML is the process of concealing the proceeds of crime through the transfer of value through business dealings and the fabrication of information on the price, quantity, or quality of imports or exports in order to justify their illicit origins. Phantom shipments, over- or under-invoicing, and fabricating bills of lading, customs declarations, and invoices to misrepresent the type or grade of the product are some examples of this technique (Makkink et al., 2024). To further elaborate on the transnational nature of money laundering, it is essential to describe shell companies, UBOs, offshore accounts, tax havens, secrecy jurisdictions, and round-tripping. Shell companies are legally registered businesses with no real operations created to disguise ownership and execute money laundering schemes (Findley et al., 2014). A natural person who eventually owns or controls a business is known as the Ultimate Beneficial Owner or UBO. An explanation of what or who qualifies as a UBO, the definition of a UBO varies by jurisdiction, but generally speaking, a UBO is someone who owns at least 10–25% of the capital, stock, or voting rights in the underlying company (for example, 10% in India, 25% in the EU and the USA, etc.). To maintain

transparency and prevent money laundering, banks and regulators must detect Ultimate Beneficial Owners (Findley et al., 2014). Offshore accounts and tax havens, using jurisdictions with bank secrecy laws (i.e., the Cayman Islands, Myanmar, etc.) to hide illicit funds and to evade taxes, are commonly used for the layering stage of classic money laundering schemes (Garcia-Bernardo et al., 2017). Round-tripping is a cunning method of money laundering that is facilitated by shell companies. i.e., a US-based company "ABC" with ill-gotten gains, eager to clean their dirty money. In a tax haven, they set up a shell company "XYZ" and transferred their money there before reinvesting it in firm ABC through loans, share purchases, or other apparently legal means. Now disguising itself as legal capital, making the round-trip complete (Ledyaeva et al., 2013).

Statement of the Problem

Money laundering causes severe harm to a country's economy and impacts individuals worldwide (Aluko & Bagheri, 2012). According to several reports, the IMF estimates that the total amount of money laundering worldwide is US\$3.2 trillion, or 3% of the worldwide GDP (International Monetary Fund, 2023). It is crucial to note that money laundering is a complex crime that frequently involves multiple jurisdictions, making detection and prosecution challenging (Financial Action Task Force & Organisation for Economic Co-operation and Development, 2010; Levi & Reuter, 2006). Laundering illegal profits puts both national and international security at serious risk by enabling organized crime, financing terrorism, and the proliferation of WMD (International Monetary Fund, 2023; Soudijn, 2014; Malm & Bichler, 2013). It has been considered by several stakeholders that money laundering is a crime that requires collaborative efforts to combat (Shehu, 2004; Dobrowolski & Sułkowski, 2020), and to address this threat, cross-national studies are needed to identify factors that can help mitigate money laundering risk within countries, ultimately contributing to the global anti-money laundering ecosystem. Unfortunately, cross-national research in this field is rare, specifically in academics, although some studies have identified crucially associated variables that are not part of the AML Basel Index direct indicators but have been found to be predictors of money laundering risk. One such study is that of Amara et al. (2020), which examined the association between money laundering and the strength of reporting and auditing standards. Similarly, cyberspace and AI are taking charge, and it is well known that criminal groups are also using these resources to be more sophisticated in their execution (Financial Action Task Force et al., 2023). Therefore, the national infrastructure of these aspects must be strengthened in both cases if money launderers are benefiting or facing hindrances from such technological advancements. This dissertation aims to investigate these potential predictors (i.e., cybersecurity and AI) along with the traditional predictor, such as corruption, with money laundering risk among full member countries of the FATF. Selecting full member states as the universe is a strategic choice since they have an indirect but ultimate influence on AML policy recommendations of every country throughout the globe.

Conceptual Framework

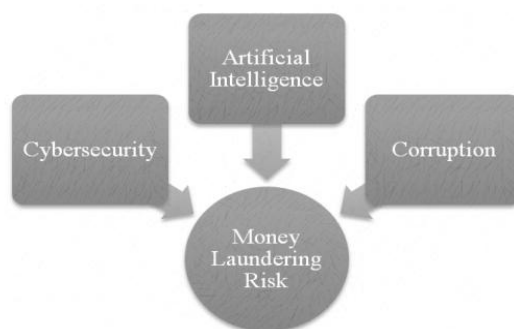


Figure 1. Factors Influencing Money Laundering Risk

Hypotheses

H₁: Higher national cybersecurity capacity is associated with lower money laundering risks.

H₂: Greater artificial intelligence readiness is associated with lower money laundering risks.

H₃: Lower perceived level of corruption (high CPI score) is associated with lower money laundering risks.

Research Objectives

- To analyze the impact of corruption on money laundering across FATF member nations.
- To investigate the association between national cybersecurity capacity with money laundering risk among FATF member countries.
- To assess the preparedness of FATF member countries in terms of artificial intelligence and its relationship with money laundering risk.
- To explain the combined impact of cybersecurity, artificial intelligence, and corruption on money laundering risk in FATF member states.

Research Questions

- To what extent does corruption play a role in influencing money laundering risks in FATF member states?
- What is the link between FATF member country's cybersecurity capacity and the risk of money laundering?
- How does the FATF nation's preparedness for AI technology affect its money laundering risk?
- How do cybersecurity measures, artificial intelligence, and corruption together shape variations in money laundering risks across FATF member countries?

Significance of Study

This study's practical implications target legislators, policymakers, and relevant international organizations. By identifying technology-based potential predictors of money laundering risk, stakeholders are equipped to make informed decisions with a risk-based approach or cost-benefit analysis. Its applicability is not only restricted to one nation since it is a cross-national study; thus, the expanded or regional significance is present, with the same rationale of UNODC that international cooperation should be promoted in various regions to counter money laundering. To be very specific, this study will also endorse the UNODC capacity-building programs with suggestions for tailored training on the identified areas concerning money laundering risk. Regardless of functional significance, this thesis also implies the work for academics and future research directions, offering a foundational econometric model and extending the geographical scope, adding omitted variables, or employing longitudinal data can bring more rigorous results. Lastly, by using established and trusted international indices as proxies, this research creates a replicable and scalable methodological precedent for future studies, especially for independent researchers seeking to examine similar crimes with transnational nature.

REVIEW OF LITERATURE

The act of hiding and purifying illegal gains so they seem like genuine or white money is known as money laundering. Monetary instability, economic vulnerability, and socioeconomic unrest are just a few of the negative effects this practice may have on the economy (Dowers & Palmreuther, 2003). The events of the 9/11 attacks brought to the attention of the globe how the act of money laundering facilitates or funds terrorism and criminal organizations, leading to devastating consequences (Ferwerda et al., 2013). Since its execution is possible on a transnational level, it has been recorded that money laundering is reduced across the globe if the capacity of regulation increases in one country (Chong & Lopez-de-Silanes, 2015). Thus, the concern emerges since money laundering enables terrorist groups and criminal organizations to finance their activities, and over the past few decades, money laundering has appeared as a major concern for policymakers (Norton, 2018). The two main purposes served by money laundering are, first, to reinject the washed proceeds into a legitimate economy so that they can be used without being caught for a predicate offense, and second, it is utilized to finance the proliferation of WMD, terrorism, and other illicit acts (Ketenci et al. 2021). Moreover, cross-border criminal investigations, especially those related to money laundering, encounter serious challenges because of the worldwide nature of digital evidence. The absence of uniform procedures in different jurisdictions makes it difficult to collect and share evidence (Casino et al., 2022). This lack of standardization not only hinders the effectiveness of law enforcement agencies but also allows criminals to exploit these gaps while operating across borders.

The Connection between Corruption and Illicit Financial Flows

Jurisdictions with lowered public sector corruption do have stricter AML regulations and lower money laundering risk; thus, the FATF has consistently emphasized this domain (Schneider & Buehn, 2018). Likewise, Reganati & Oliva (2018) also endorsed that strong law enforcement efforts along with effective education on anti-corruption have been associated with lower money laundering risk. Similarly, nations with more heightened corruption levels often experience a high risk of money laundering. Research has shown that higher corruption levels can be disrupted with strong AML measures, especially in developing countries where transparency and accountability of financial activities are overlooked (Ferwerda & Reuter, 2019).

Barone et al. (2019) emphasize the importance of increased transparency in systems made to prevent money laundering; by doing so, it will be hard for corrupt officials to exploit the system, ultimately reducing corruption. Moreover, they also claimed that corruption increases demand for money laundering operations, indicating that corruption is both a contributing factor to and a cause of money laundering. Additionally, Amara et al. (2020) also found that corruption has a positive association with money laundering, meaning that higher levels of corruption result in more heightened money laundering. Furthermore, Teichmann (2020) also investigated the connection between money laundering and corruption and proposed that in order to prevent money laundering, anti-corruption measures must be implemented. With the same spirit, research has shown that real instances of money laundering activities and the perceived level of corruption are correlated, making the corruption perception index a credible measure for evaluating corruption status within the scored region (Hope Sr, 2022).

The interlink of money laundering and corruption with the assistance of offshore financial infrastructure is necessary to broaden the understanding by exploring it on a transnational and collective level as a financially advanced phenomenon (Costa, 2022). It is commonly acknowledged that one of the main effects of lax AML regulation is corruption. Research has shown that corruption impacts AML measures, further highlighting an ineffective AML framework that enables criminal proceeds to flow through financial institutions (Lindasari, 2023). Further reinforcing this argument, Bartulovic et al. (2023) conducted a longitudinal study on corruption and money laundering. The research period was from 2011

to 2020, and Croatia, Germany, Italy, Slovakia, Slovenia, and Sweden were included in the research sample. The results of the study show a positive and statistically significant relationship between corruption and money laundering, which are also often closely linked and do have mutually reinforcing or reciprocal criminogenic relationship. Likewise, Ekwueme & Agu (2025) also examined the nexus of money laundering and corruption and found that these phenomena have domino implications on each other as well as on several other social problems, including organized criminality. These findings suggests the importance of implementing robust regulatory frameworks to combat both issues effectively. As countries continue to grapple with these challenges, understanding their interconnectedness will be critical for developing comprehensive anti-corruption and AML strategies.

Cybersecurity and Cyber Laundering

Transitioning to nature, cyber laundering techniques are way faster and more convenient as compared to traditional money laundering techniques; additionally, the entire cyberspace makes the whole process much cheaper in the digital era (Mabunda, 2018). According to Butler and O'Brien (2019), regulatory technology is a type of information technology that aids businesses in carrying out their regulatory obligations, which helps combat money laundering. This is in line with the current anti-money laundering (AML) regulations. A thorough analysis was carried out by Joveda et al. (2019) in order to design a cybersecurity system that detects money laundering. In the age of trade-based concealment, website hacking, ATM fraud, cyber laundering, and credit card fraud, the study highlights that classic AML techniques are no longer effective. Nevertheless, they can still be helpful when combined with contemporary technology. As a result, research suggests that financial institutions, regulators, and LEAs invest more in IT infrastructure. Furthermore, the emergence of e-commerce and its accessible nature unintentionally facilitates fraudulent actors to conceal and launder criminal proceeds through legitimate businesses; it is similar to trade-based money laundering but in a digital space (Alsaibai et al., 2020). Furthermore, cooperative efforts among law enforcement, academia, and the private sector can support research and development as well as the sharing of expertise and knowledge to combat rapidly evolving malicious actors in cyberspace (Lim & Thing, 2022). Traditional money laundering techniques are being replaced with the help of cybercrime, and it is more sophisticated and suave in execution because it could be committed in multiple jurisdictions without any barrier, and the threat posed by cybercrime money laundering schemes was aggravated during the Covid-19 pandemic (Bošković, 2022). However, Svitlychna (2022) evaluated the potential convergence of cybersecurity with AML efforts, suggesting results indicate that an integrated model will help to reduce cybercriminality and financial crimes and also strengthen the AML regime of the country. Likewise, the prevention of money laundering is positively and significantly impacted by transaction monitoring, which is facilitated by regulatory technology (Kurniawan, 2023). In a similar vein, there is a substantial negative correlation between money laundering and general digitization, indicating that lower rates of money laundering are typically associated with greater digitalization (Khelil et al., 2023). Furthermore, Khelil et al. (2023) also investigated how corruption moderates the effects of money laundering and digitization; however, results suggested whether the environment is characterized by low or high corruption doesn't impact the strong negative association of digitalization and money laundering.

Integration of AI in AML System

The emergence of artificial intelligence is revolutionizing AML systems. AI can reduce false positives, meet regulatory expectations with compliance, and optimize the productivity of operational resources (Han et al., 2020). It is important to note that artificial intelligence requires training for better results, and when it comes to transaction monitoring, the system detects suspicious transactions based on the provided detection scenarios and data patterns, and there is a high risk of labeling harmless transactions as suspicious. For example, red flags are raised by the system, but they are ultimately investigated by AML

analysts to find whether the flagged transaction is a true hit or not. From here the decision-making process of the AI system got refined since the analyst's decision is learning for a system for future predictions. A similar understanding can be applied to name screening as well (Eddin et al., 2021). Additionally, a study conducted by Ketenci et al. (2021) proposed a novel technique for transaction monitoring based on time-frequency analysis that uses machine learning and 2-D demonstrations to detect distinguishing factors of non-suspicious and suspicious transactions. This experimental model showed significant results by reducing the false positive rate to 14.9% as compared to a staggering 90%. To address spelling inconsistencies and partial matches during name screening, fuzzy matching uses probabilistic logic and tolerance thresholds to detect. The primary objective is to reduce the likelihood of false negatives, and innovative algorithms are employed to refine the name-screening process. Factors like known aliases, variations in names, and geographic locations are considered to improve due diligence efforts. Regardless of the algorithm's advantages, it may still produce false positives; however, continuous machine learning undoubtedly improves its efficiency (Eddin et al., 2021). In regards to trade-based money laundering, artificial intelligence can optimize the detection of anomalies such as over-invoicing tactics by analyzing transaction unit prices that deviate from established international thresholds price of goods through open-source intelligence; overstate or understate manipulation of the reported volume or price of a good can be detected more efficiently (Rouhollahi, 2021). The most common use of AI is to predict behavior based on probability-based analysis of past patterns employing AI in banking helps to keep track of financial transactions, customer behavior, market trends, and adverse media reports by the implementation of algorithms, open-source intelligence, and other techniques. By analyzing several aspects of data, AI can identify typical behavior and flag anomalies that might suggest fraudulent activity, such as money laundering (Alhajeri & Alhashem, 2023). Empirically, Google Cloud and HSBC have collaborated on a machine learning based money laundering detection trial. Google Cloud has released Anti-Money Laundering AI, or AML AI, for large-scale applications following a successful pilot test. This product's primary distinction is that it does not employ the conventional rule-based methodology (May, 2023). Instead, it employs machine learning and a comprehensive view of consumer data to identify instances of money laundering. It is an API that can be integrated into the bank's backend software (Brue, 2023; Eddin et al., 2021). To offer the compliance team a comprehensive risk score for reviewing high-risk situations, the model automatically learns from a variety of client data that the bank provides it, such as KYC, transactions history, etc., and integrates this with previously detected risk events. Through a feedback loop, the model is adjusted to become increasingly accurate based on the compliance team's actions. The risk score's explainability about the reasons behind a transaction's flagging and the factors taken into account when determining the risk score weightage is another crucial component. According to the HSBC trial, this technique led to a staggering 60% decrease in false negatives and two to four times more suspicious activity identification (Brue, 2023; May, 2023).

In addition, Al-Ababneh et al. (2024) Present a study that enables the creation of an accurate predictive model for detecting money laundering abnormalities using machine-learning algorithms, networks of neurons, and techniques for detecting anomalies (i.e., incorporating Benford law into the system) by employing both supervised and unsupervised learning methods for the model. This empirical investigation demonstrates that AI models reduced false positives by thirty percent and increased detection rate by twenty-five percent, highlighting that traditional rule-based systems have been outperformed by AI models.

AI and the Identification of Ultimate Beneficial Ownership

Legitimate businesses spanning multiple jurisdictions are commonly used to conceal criminal proceeds, making the money laundering network significantly complex. Detecting the ultimate beneficial owner is crucial for businesses, regulators, and LEAs to counter money laundering and terror financing (Meunier, 2018). In most jurisdictions natural person who owns 25% of a company is considered the ultimate

beneficial owner, but the layered nature of data and varying regulations make it difficult to identify the ultimate beneficial owner. Regardless of emerging legislation throughout the world on transparency in ownership, identification of the ultimate beneficial owner remained difficult due to complex and opaque ownership structures, shell companies, nominee shareholders, multiple investment layers, and unstructured data or handwritten notes obscuring true ownership (Alhajeri & Alhashem, 2023). From here, technology offers solutions. Machine learning and optical character recognition can help relevant stakeholders read shareholder documents provided as PDF files and change them into machine-readable texts that a machine learning system can examine. This process can make it easier to search and analyze these records, which helps with quick cross-border investigations (Subbagari, 2023). By leveraging these advanced technologies, regulatory bodies can enhance their ability to detect fraudulent activities and ensure compliance with financial regulations. Additionally, the integration of blockchain technology could further bolster transparency and traceability in ownership records, fostering a more robust financial ecosystem (Ramalingam, 2023).

RESEARCH METHODOLOGY

Research Design and Variables

This research investigates the empirically guided predictors, such as cybersecurity capacity, artificial intelligence readiness, and corruption concerning money laundering risk among member countries of the FATF, using a quantitative index-based cross-sectional approach. The research design is explanatory since it aims to test hypothesized associations using statistical analysis. Predicting variables are empirically grounded based on consistent validation of predictors by the literature. This study relies solely on secondary data sourced from publicly available international indices that act as proxy measures for the variables of interest. Gathering primary data on these subjects can be challenging and often impractical; therefore, this approach has been opted for instead. Data for money laundering risk was sourced from the Basel AML Index (Basel Institute on Governance, 2024), cybersecurity capacity from the National Cyber Security Index (e-Governance Academy, 2024), AI readiness from the Government AI Readiness Index (Oxford Insights, 2024), and corruption from the Corruption Perceptions Index (Transparency International, 2024). Furthermore, the indices that are part of the study are being selected based on their active and comprehensive reporting of variables, and consideration of two aspects: (1) the availability of data for the most recent year, 2024, and (2) the scores of all active FATF member nations must be recorded in the index, which makes them the best fit to be chosen as proxy measures for inferential analysis.

Sampling and Population

Regarding sampling, the FATF consists of 40 full members, including 38 countries or territories and 2 regional organizations. Since the study focuses on member countries of the FATF, a census approach was chosen to gather data from active member states of the FATF. This way, the research truly reflects the insights on the strategic nations. However, FATF suspended the membership of Russia due to the Ukraine war (Tassilo & Ingrid, 2023). Moreover, Argentina is also excluded from the analysis because the key proxy measure of the study, the AML Basel Index, does not rank Argentina in the latest edition, making 36 member states of FATF that have been studied as elements. The study aimed to address the whole population pertinent to its range since no sampling per se is necessary. Alternatively, given the study's strategic emphasis and policy relevance for global anti-money laundering efforts, the approach can also be characterized as purposive sampling from the larger universe of countries listed in the AML Basel Index, with intentional inclusion of FATF full members only.

Data Collection

The gathered data was extracted by a self-constructed tool that enabled the collection of country-level scores from various indices. Since the data is published and comes from trusted and recognized sources, it is inherently consistent and accurate, ultimately making the tool reliable. Moreover, our data extraction tool was reviewed and endorsed by academicians and experts in criminology and anti-money laundering for content validity.

Ethical Considerations

Lastly, This research has exclusively relied solely on publicly available secondary data, which means it does not require specific ethical approval as necessary if working with human subjects. Proper citations of all our sources are given throughout the study.

Table 1 – Proxy Measures and Sources

Variable	Proxy Measure	Source
Money Laundering Risk	AML Basel Index	Basel Institute on Governance
Cybersecurity Capacity	National Cyber Security Index	e-Governance Academy Foundation
AI Readiness	Government AI Readiness Index	Oxford Insights
Corruption	Corruption Perception Index	Transparency International

Data Presentation

This section presents a comprehensive description of global indices assessing money laundering risk, cybersecurity capacity, AI readiness, and perceived public sector corruption among FATF member states. The data is sourced from the Basel AML Index, National Cybersecurity Index (NCSI), Government AI Readiness Index, and Corruption Perception Index (CPI). Each subsection details the respective index, its methodology, and key findings, supported by tabular data for clarity.

Global AML Index by the Basel Institute on Governance

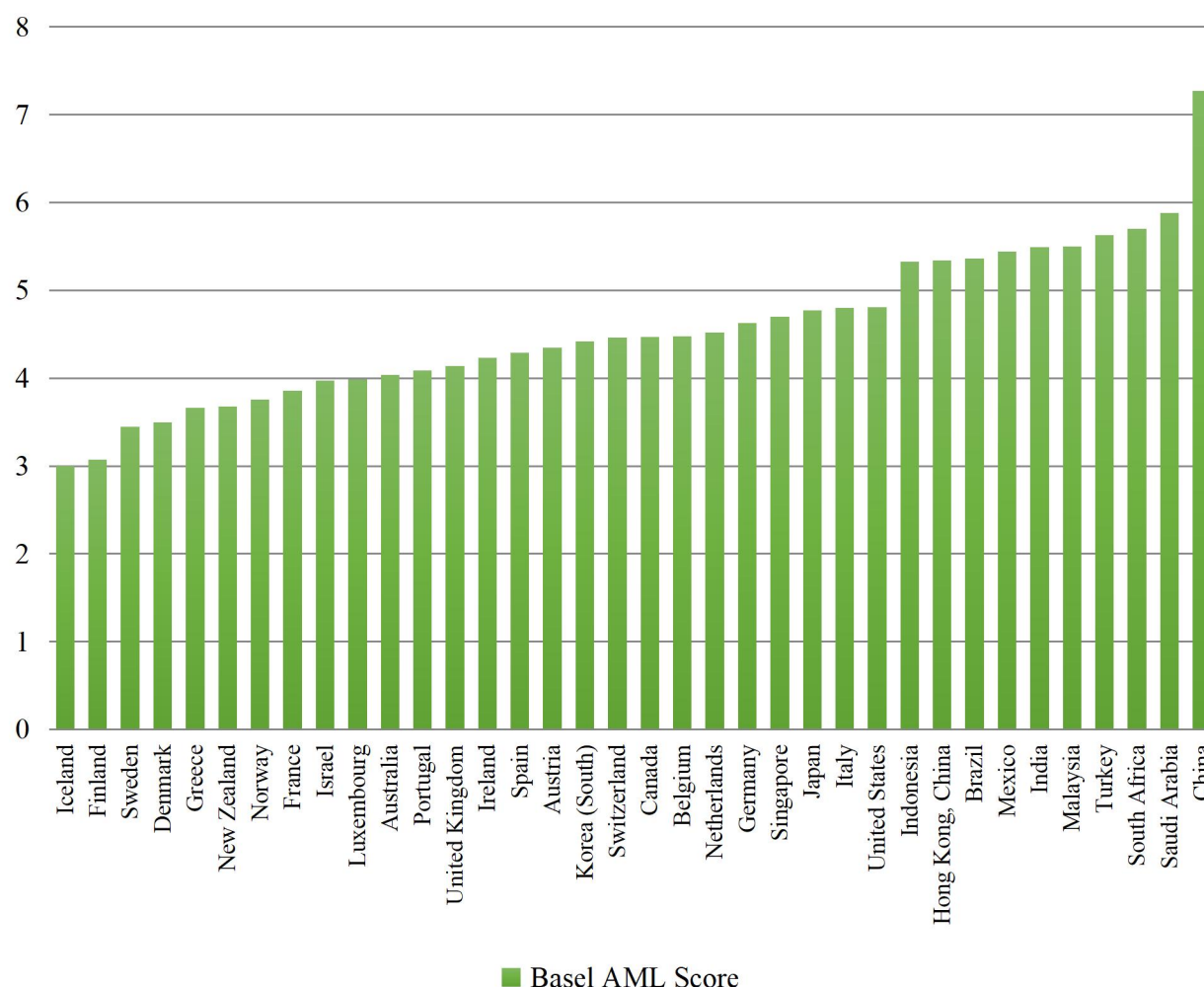
The Basel Institute on Governance is an independent nonprofit organization established in 2003 from the University of Basel, Switzerland. The Public Edition of the Global AML Index by the Basel Institute on Governance is a core product that publishes annually to assess money laundering risk around the world on a scale of 0 to 10. In total, 5 domains of jurisdiction are evaluated, including the AML/CFT/CPF framework, legal and political risk, government integrity, corruption and fraud risk, and financial transparency. To evaluate these domains, 17 different indicators are used. Table 2 lists the study's elements, the FATF member states, in which a Nordic nation, Iceland, scored the lowest, 3, suggesting Iceland has the lowest money laundering risk among the FATF member states. However, China scored highest with 7.27, suggesting it as a moderate-to-high-risk jurisdiction regarding money laundering. It is important to note that the average score, which is 4.56 (SD = 0.88) for FATF member nations, suggests a moderate to low risk of money laundering.

Table 2 – Country wise Basel AML Index Score (Low Risk: 0 – High Risk: 10)

S. No	Country	Money Laundering Risk
1	Iceland	3
2	Finland	3.07
3	Sweden	3.45
4	Denmark	3.5
5	Greece	3.66
6	New Zealand	3.68
7	Norway	3.76
8	France	3.86
9	Israel	3.97
10	Luxembourg	3.99
11	Australia	4.04
12	Portugal	4.09
13	United Kingdom	4.14
14	Ireland	4.23
15	Spain	4.29
16	Austria	4.35
17	Korea (South)	4.42
18	Switzerland	4.46
19	Canada	4.47
20	Belgium	4.48
21	Netherlands	4.52
22	Germany	4.63
23	Singapore	4.7
24	Japan	4.77
25	Italy	4.8
26	United States	4.81
27	Indonesia	5.33
28	Hong Kong, China	5.34
29	Brazil	5.36
30	Mexico	5.44
31	India	5.49
32	Malaysia	5.5
33	Turkey	5.63
34	South Africa	5.7
35	Saudi Arabia	5.88
36	China	7.27
Mean Score:		4.56
Standard Deviation:		0.88

Source: Basel AML Index (2024)

Figure 2. Basel AML Score



National Cybersecurity Index

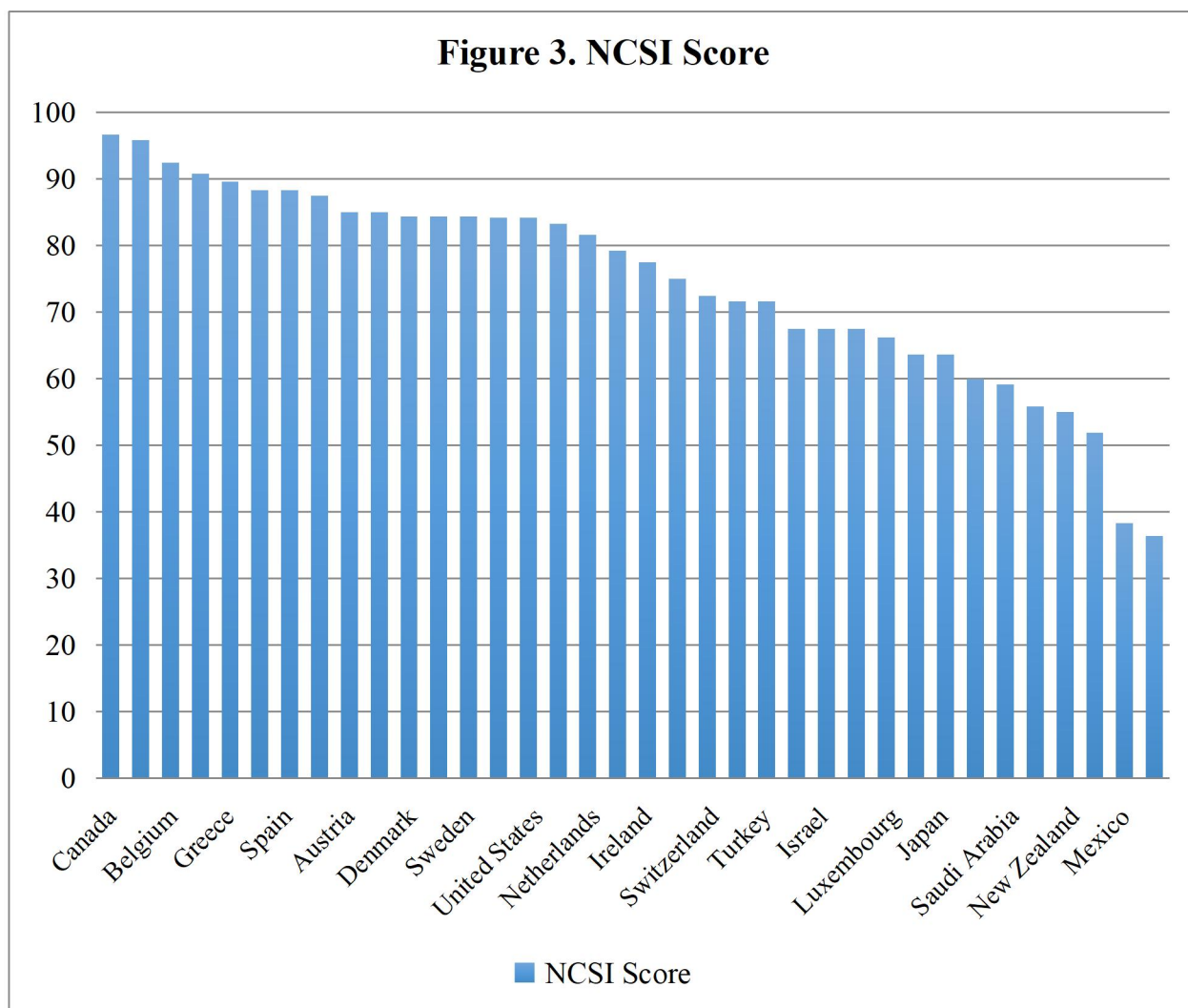
The NCSI scores jurisdictions based on their capacity and preparedness in cybersecurity. NCSI is published by a foundation named e-Governance Academy, which was established in 2002 as a collaborative effort of UNDP, the Estonian government, and the Open Society Institute (OSI) to encourage digital transformation around the world. NCSI measures countries' preparedness for cybersecurity on the basis of 3 categories, 12 capacities, and 49 indicators; fundamentally, the index is developed on strategic, preventive, and responsive domains, and country rating is based on public evidence, including legal acts, official documents, and official websites. Among the FATF member states, South Africa is listed as a state with the lowest cybersecurity capacity or preparedness, with an NCSI score of 36.36. On the other hand, Canada scored the highest, with a 96.67 NCSI score, indicating that it is the strongest nation for cybersecurity among FATF member states. The mean NCSI score for FATF member states, which is 74.62 (SD = 15.20), suggests a moderate to high capacity of cybersecurity for member nations of FATF. For every element's score, see Table 3.

Table 3 – Country wise NCSI Score (Low Capacity: 0 – High Capacity: 100)

S. No	Country	Cybersecurity
1	Canada	96.67
2	Finland	95.83
3	Belgium	92.5
4	Germany	90.83
5	Greece	89.61
6	Italy	88.33
7	Spain	88.31
8	Australia	87.5
9	Austria	85
10	Singapore	85
11	Denmark	84.42
12	France	84.42
13	Sweden	84.42
14	Portugal	84.17
15	United States	84.17
16	Korea (South)	83.33
17	Netherlands	81.67
18	Malaysia	79.22
19	Ireland	77.5
20	United Kingdom	75
21	Switzerland	72.5
22	Brazil	71.67
23	Turkey	71.67
24	India	67.53
25	Israel	67.53
26	Norway	67.53
27	Luxembourg	66.23
28	Indonesia	63.64
29	Japan	63.64
30	China	60
31	Saudi Arabia	59.17
32	Iceland	55.84
33	New Zealand	55
34	Hong Kong, China	51.95
35	Mexico	38.33
36	South Africa	36.36
Mean Score:		74.62
Standard Deviation:		15.20

Source: National Cybersecurity Index (2024)

Figure 3. NCSI Score



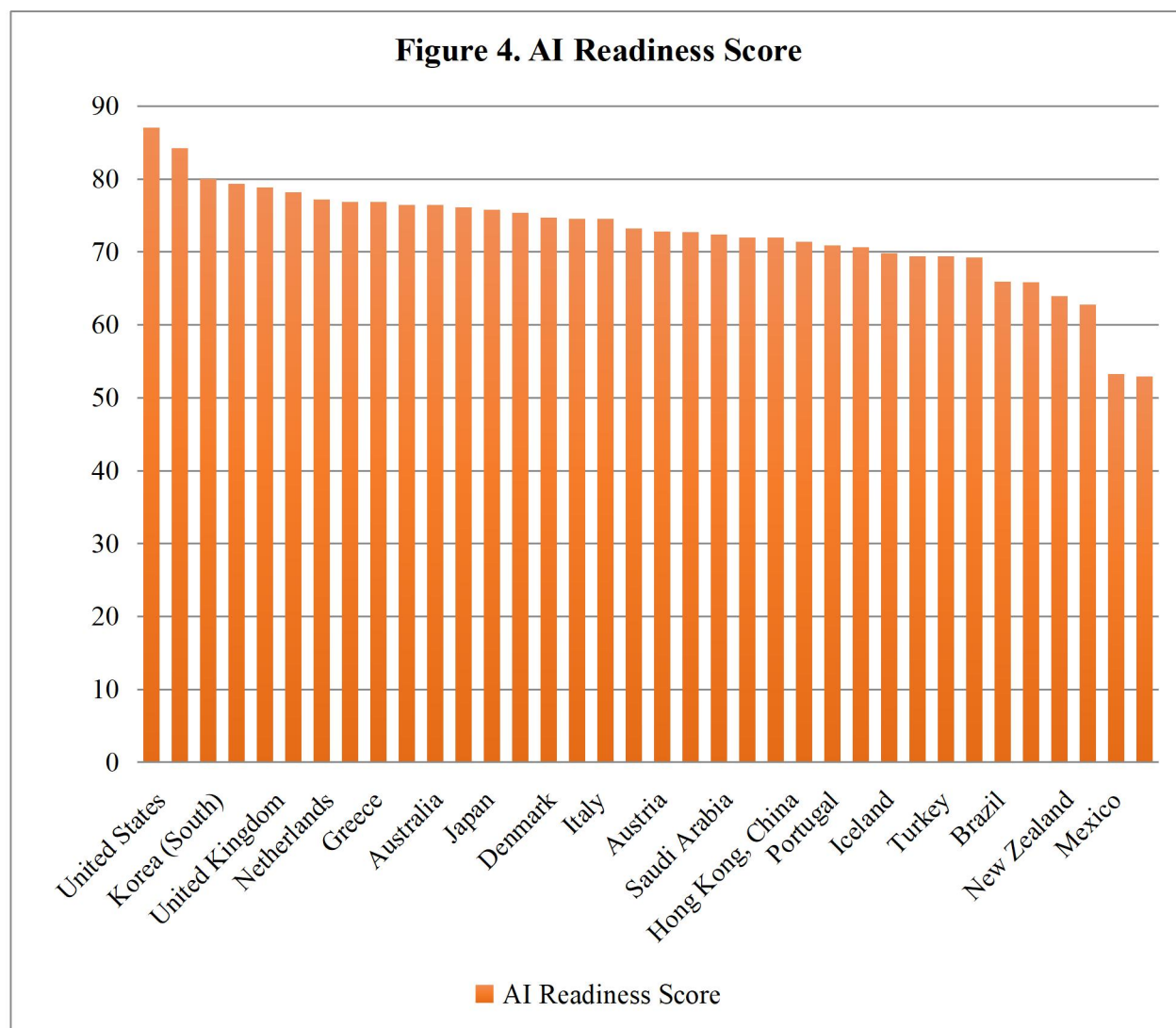
The Government AI Readiness Index

The government AI readiness index assesses and ranks nations according to their readiness for AI. To evaluate the countries, they have established 3 domains, including government, technology sector, and data & infrastructure, consisting of 10 dimensions assessed by 40 indicators in total. FATF member states score 72.60 on AI readiness on average with a standard deviation of 6.99, suggesting moderate to high readiness among member nations. Particularly, South Africa scores lowest among the member nations at 52.91 as an overall AI readiness score; on the other hand, the United States and Singapore are the leading jurisdictions, scoring 87.03 and 84.25 on overall AI readiness, respectively, followed by South Korea (79.98) and France (79.36). Notably, 20 countries score above the mean. To see the AI readiness ranking among FATF member states, refer to Table 4.

Table 4 – Country wise AI Readiness Score (Low Readiness: 0 – High Readiness: 100)

S. No	Country	Artificial Intelligence
1	United States	87.03
2	Singapore	84.25
3	Korea (South)	79.98
4	France	79.36
5	United Kingdom	78.88
6	Canada	78.18
7	Netherlands	77.23
8	Germany	76.9
9	Greece	76.9
10	Finland	76.48
11	Australia	76.45
12	Norway	76.12
13	Japan	75.75
14	Sweden	75.4
15	Denmark	74.71
16	Israel	74.52
17	Italy	74.52
18	Ireland	73.18
19	Austria	72.84
20	Belgium	72.69
21	Saudi Arabia	72.36
22	China	72.01
23	Hong Kong, China	72.01
24	Malaysia	71.4
25	Portugal	70.93
26	Luxembourg	70.63
27	Iceland	69.82
28	Switzerland	69.42
29	Turkey	69.42
30	Spain	69.25
31	Brazil	65.89
32	Indonesia	65.85
33	New Zealand	63.98
34	India	62.81
35	Mexico	53.29
36	South Africa	52.91
Mean Score:		72.60
Standard Deviation:		6.99

Source: Government AI Readiness Index (2024)



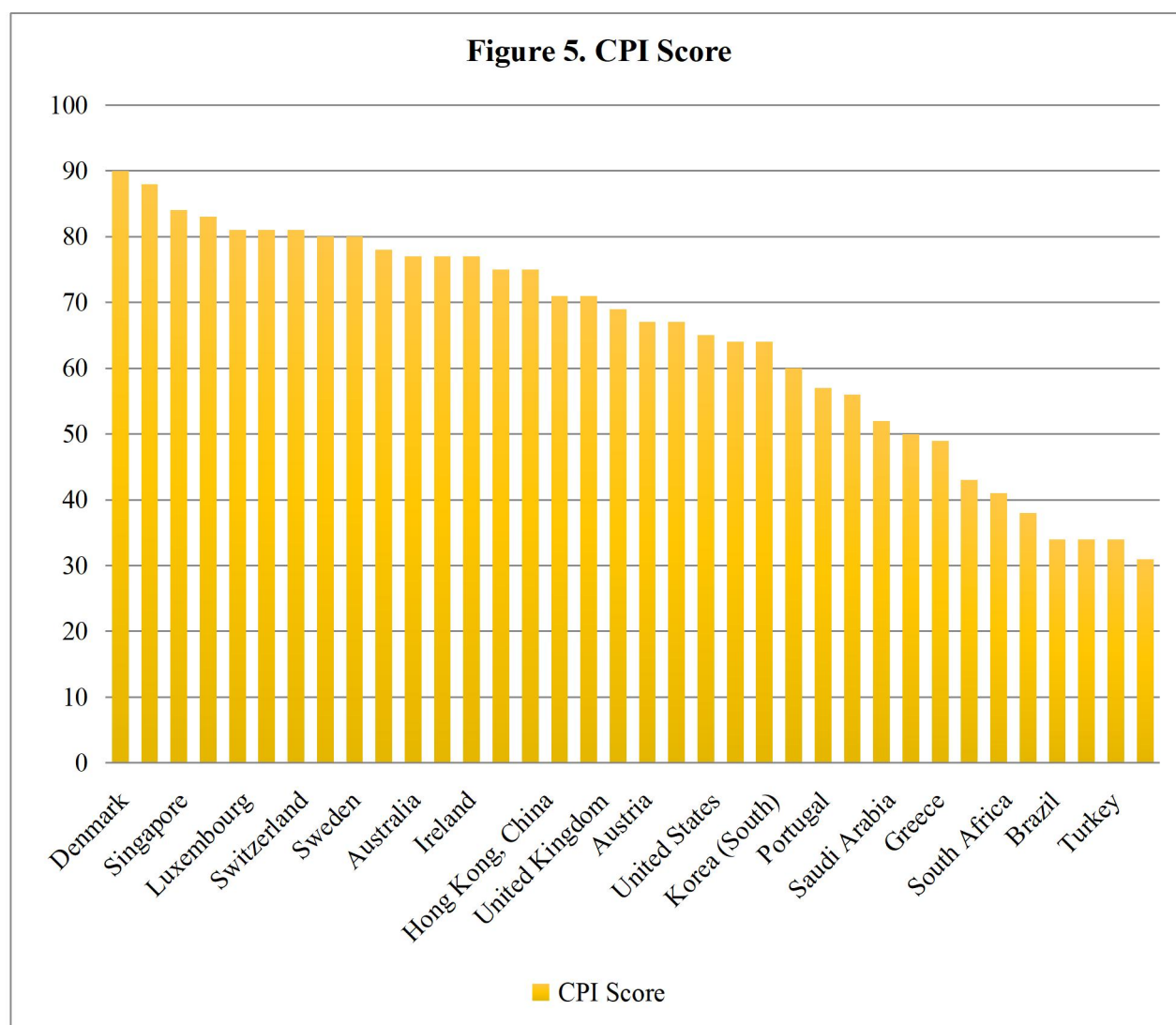
Corruption Perception Index

The Corruption Perception Index (CPI) evaluates perceptions of public sector corruption among experts and businesspeople, aggregating data from diverse, credible sources. Table 6 presents the CPI scores for FATF member states. Mexico records the lowest score, signaling a high likelihood of perceived corruption within its public sector. In contrast, Denmark achieves a score of 90, reflecting the lowest level of perceived corruption and positioning it as the leading jurisdiction among FATF members. The mean score of 64.55 (SD = 17.40) suggests that, on average, FATF member states exhibit moderate to low levels of perceived corruption. This variation underscores the need for targeted anti-corruption measures in jurisdictions with lower scores to enhance governance and align with global standards for public sector integrity.

Table 5 – Country wise CPI Score (Low Risk: 100 – High Risk: 0)

S. No	Country	Corruption
1	Denmark	90
2	Finland	88
3	Singapore	84
4	New Zealand	83
5	Luxembourg	81
6	Norway	81
7	Switzerland	81
8	Netherlands	80
9	Sweden	80
10	Germany	78
11	Australia	77
12	Iceland	77
13	Ireland	77
14	Canada	75
15	Hong Kong, China	75
16	Japan	71
17	United Kingdom	71
18	Belgium	69
19	Austria	67
20	France	67
21	United States	65
22	Israel	64
23	Korea (South)	64
24	Spain	60
25	Portugal	57
26	Italy	56
27	Saudi Arabia	52
28	Malaysia	50
29	Greece	49
30	China	43
31	South Africa	41
32	India	38
33	Brazil	34
34	Indonesia	34
35	Turkey	34
36	Mexico	31
Mean Score:		64.55
Standard Deviation:		17.40

Source: Corruption Perception Index (2024)



This section synthesizes the extracted data from global indices evaluating money laundering risk, cybersecurity. These findings reveal diverse performance across FATF jurisdictions, with Nordic countries excelling in risk mitigation and governance, while comparatively others face challenges in specific domains. Targeted policy measures are essential to address vulnerabilities and strengthen global standards in anti-money laundering, cybersecurity, AI integration, and public sector transparency.

DATA ANALYSIS

Descriptive statistic was employed on aforementioned dataset and to test the hypotheses Ordinary Least Squares (OLS) based multiple linear regression has been employed, and the following econometric model has been developed:

$$MLR_i = \beta_0 + \beta_1 (\text{Cybersecurity}_i) + \beta_2 (\text{Artificial Intelligence}_i) + \beta_3 (\text{Corruption}_i) + \varepsilon_i$$

- **Money Laundering Risk (MLR)** represents money laundering risk based on the Basel AML index score.
- β_0 represents the intercept of the model.
- β_i represents coefficients of corresponding variables.
- **Cybersecurity** denotes the NCSI score.
- **Artificial Intelligence** denotes the Government AI Readiness score.
- **Corruption** denotes the CPI score.
- ε refers to the error term.

Ordinary Least Squares Assumptions

- ✓ The residual errors in linear regression are assumed to be normal. P-value for Shapiro-Wilk = $0.312 > 0.05$ (level of significance). Therefore, the data is assumed to be normally distributed.
- ✓ To meet the OLS assumption of autocorrelation, the Durbin-Watson (DW) was applied; the result shows the test statistic is 1.872, and it suggests no autocorrelation. DW value ranges from 0 to 4, with an acceptable range from 1.5 to 2.5 (Draper & Smith, 1998).
- ✓ Multicollinearity is not present because every VIF value is less than 2.5.
- ✓ Homoscedasticity has been tested through the White test; the White test p-value equals 0.00000350943 ($F = 18.824473$). Assuming that the variance is not consistent, this indicates a violation of the assumption, suggesting heteroscedasticity in the data. To counter this violation, the remedy of robust standardized error, particularly HC3, has been employed to address the heteroscedasticity in the data.
- ✓ Lastly, to ensure linearity in data scatterplots for each combination are presented below:

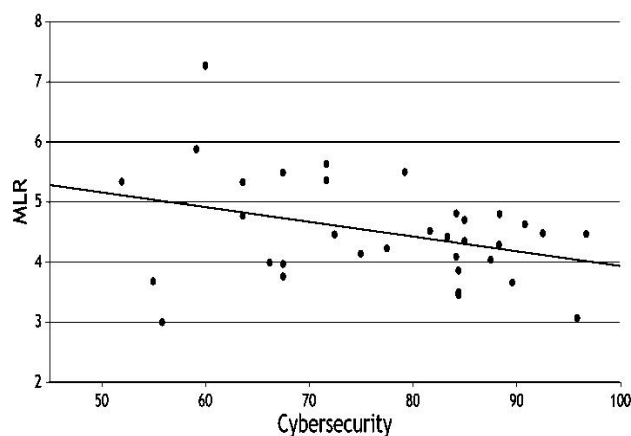


Figure 6. Scatterplot for Money Laundering Risk and Cybersecurity.

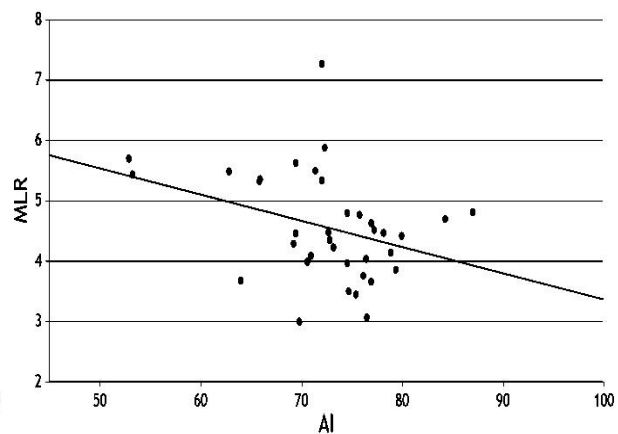


Figure 7. Scatterplot for Money Laundering Risk and AI.

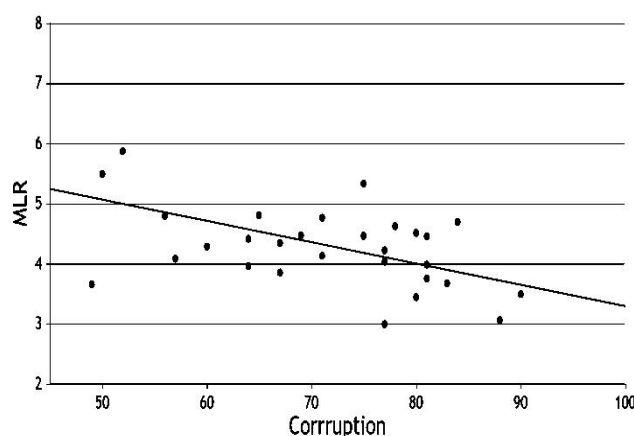


Figure 8. Scatterplot for Money Laundering Risk and Corruption.

RESULTS AND FINDINGS

Pearson Correlation Coefficient

Prior to using regression analysis to test hypotheses and assess and forecast the relationship between predictors and outcome variable, it is essential to establish a baseline and provide statistical support for more thorough investigation. Thus, the Pearson correlation coefficient between each predictor and the outcome variable is calculated using the dataset that was previously presented.

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2 \sum (y - \bar{y})^2}}$$

Table 6 – Correlation Results

		Money Laundering Risk	Cybersecurity	Artificial Intelligence	Corruption
Money Laundering Risk	<i>Pearson Correlation</i>	1	-0.421**	-0.343**	-0.698**

Note: **Significant at $p < 0.05$

The results reveal an inverse correlation between the predictors and the money laundering risk. Corruption, with a correlation coefficient of $r = -0.698$, is the leading variable, exhibiting a moderate to strong correlation with money laundering risk. The other two variables show a moderate to weak correlation with money laundering risk; cybersecurity was found to have -0.421 of Pearson r , while artificial intelligence scored $r = -0.343$. Corruption, cybersecurity, and artificial intelligence exhibit a negative linear relationship with money laundering risk. To further investigate the causal impact, the ordinary least squares (OLS) method with HC3 robust consistent standard error is employed.

Furthermore, the results of the multiple linear regression depicted in Table 6 showed that corruption, cybersecurity, and artificial intelligence, had a high collective significant influence on money laundering risk $\{F_{(3, 32)} = 12.914, p\text{-value} < .001, R^2 = 0.558, \text{adjusted } R^2 = 0.516\}$. Upon closer examination of the individual predictors, it was found that Corruption ($\beta_1 = -0.0375, p = 0.00003 < 0.05$) and Cybersecurity ($\beta_2 = -0.0215, p = 0.034 < 0.05$) were significant predictors in the model, and Artificial Intelligence ($\beta_3 = 0.0417, p = 0.085 > 0.05$) was insignificant predictor in the model.

Table 7 – Regression Results

<i>Regression Statistics</i>					
Multiple R	0.747				
R Square	0.558				
Adjusted R Square	0.516				
Standard Error	0.615				
Observations	36				

<i>ANOVA</i>					
	<i>df</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>Significance F</i>
Regression	3	15.301	5.100	12.914	0.000009
Residual	32	12.118	0.378		
Total	35	27.419			

<i>Model</i>	<i>Coefficients (β)</i>	<i>Std Error (HC3)</i>	<i>t Stat</i>	<i>P-value</i>	<i>VIF</i>
Intercept	5.563	1.210	4.598	0.00005	-
Cybersecurity	-0.0215	0.010	-2.150	0.039	2.024
Artificial Intelligence	0.0417	0.025	1.668	0.105	2.492
Corruption	-0.0375	0.008	-4.688	0.00003	1.446

Multiple Linear Regression with HC3 Robust Standard Errors

As per Table 7, overall regression: $F_{(3, 32)} = 12.914$, $p\text{-value} = 0.000009$, with a $p\text{-value} < \alpha (0.05)$, we reject the null hypothesis. The model without independent variables, $y = \beta_0 + \epsilon$, underperforms than the linear regression model, $y = \beta_0 + \beta_1x_1 + \dots + \beta_ix_i + \epsilon$. To pull inference from the analysis, it can be said that higher national cybersecurity capacity and higher CPI scores (lower perceived levels of corruption) do have an effective impact on reducing the money laundering risk within the state, aligning with the literature. However, the insignificant impact of artificial intelligence does not align with the past empirical and theoretical evidence. According to the results of the cross-sectional analysis, artificial intelligence is statistically insignificant; in other words, the observed sample did not validate the casual impact. It is important to note that failure to reject the null hypothesis for artificial intelligence as a predictor does not imply that artificial intelligence does not have any impact on money laundering, but it needs to be explored in future studies with other measures for this variable.

On the basis of data analysis and manual iterations, this study presents a statistically significant econometric model, which is depicted in the following equation:

$$MLR_i = 5.563 - 0.0215 (\text{Cybersecurity}_i) - 0.0375 (\text{Corruption}_i) + \epsilon_i$$

The regression equation suggests, if x_i (cybersecurity or corruption) is increased by one unit, then money laundering risk decreases by β_i (0.0215 or 0.0375) unit, keeping other factors constant or *ceteris paribus*.

Hypotheses Testing

The findings regarding the interplay between corruption, cybersecurity capacity, AI readiness, and money laundering risk within a framework of 36 FATF member countries have been quantitatively analyzed. The findings are organized in accordance with the hypotheses and research questions. They include pertinent statistical findings from multiple linear regression analyses with HC3 robust standard errors to address heteroscedasticity. The analysis provides critical insights into how the studied factors influence money laundering risk.

Hypothesis 1: Higher national cybersecurity capacity is associated with lower money laundering risks.

With a range of 36.36 (South Africa) to 96.67 (Canada), the average NCSI score was 74.62 (SD = 15.20) among studied elements. The regression coefficient for NCSI was $\beta_2 = -0.0215$ ($p = 0.034$). This supports Hypothesis 1 by showing a statistically significant negative association.

Hypothesis 2: Greater artificial intelligence readiness is associated with lower money laundering risks.

The average AI readiness score was 72.60, with a SD of 6.99 among FATF member states. The lowest score was 52.91 (South Africa), and the highest was 87.03 (United States). The regression coefficient for AI readiness was $\beta_3 = 0.0417$ ($p = 0.085$). This result is not statistically significant, so it does not support Hypothesis 2; hence, we failed to reject the null hypothesis.

Hypothesis 3: Lower perceived level of corruption (high CPI score) is associated with lower money laundering risks.

The regression analysis between the AML Index by the Basel Institute, which measures money laundering risk, and the CPI, which measures corruption, determined the slope of the regression for the

CPI to be $\beta_1 = -0.0375$ ($p = 0.00003$). This analysis confirms a significant negative relationship, thus affirming Hypothesis 3.

Research Question 4: Combined impact of cybersecurity, AI readiness, and corruption on money laundering risk.

To answer the combined impact, the multiple linear regression model yielded a significant overall effect, $F(3, 32) = 12.914$, $p < 0.001$, with $R^2 = 0.558$ and adjusted $R^2 = 0.516$, in response to the combined effect. This shows that the predictors account for 55.8% of the variation in money laundering risk, with cybersecurity and corruption being significant contributors.

DISCUSSION

The results are interpreted, placed within the body of existing literature, and their limitations and implications are examined in this section. As per the data analysis, AI readiness was found to be an insignificant predictor of reducing money laundering risk; however, this inference is unexpected because the impact of AI on money laundering has strong empirical evidence, so it is important to consider that the measure of AI in this study is a proxy variable, and due to consistent empirical support, there is a likelihood that the failure to reject the null hypothesis is due to the proxy measurement, and we cannot say at this moment that AI does not impact the overall paradigm of money laundering risk. On the other hand, the rest of the research questions are addressed by the findings. First, the regression coefficient indicates a strong relationship between lower perceived corruption (higher CPI scores) and lower risk of money laundering. This implies that nations with better governance are less vulnerable to money laundering. Second, strong digital defenses help prevent cyber-laundering, as evidenced by the fact that higher cybersecurity capacity (higher NCSI scores) also lowers money laundering risk. Lastly, the combined model explains more than half of the variation in money laundering risk across FATF member states, emphasizing the importance of cybersecurity and corruption as major drivers.

To align findings with existing literature, in this regard, anticipations were partially met. The strong role of corruption is in line with earlier research (Ekwueme & Agu, 2025; Bartulovic et al., 2023; Hope Sr., 2022; Amara et al., 2020; Barone et al., 2019; Ferwerda & Reuter, 2019) that says weak governance leads to more money laundering. The association of cybersecurity to reduce money laundering risk is also aligned with the findings of Joveda et al. (2019). However, the AI readiness result was surprising because studies like Han et al. (2020) show how AI could help with AML. The difference could be because the Government AI Readiness Index looks at general AI readiness instead of AML-focused uses or because of the fact that sophisticated criminals also utilize AI to counter its benefits. Another possible explanation is that AI has different effects depending on how it is used, as shown by the HSBC-Google Cloud trial (Brue, 2023), which showed strong AML results with targeted AI tools. This shows that while AI can improve AML efforts, its success depends a lot on the specific applications and strategies used. Future research should aim to optimize these tools to make the most impact against the ever-changing methods of criminals.

To further endorse the importance of digital security, consider the following case: AUSTRAC and SFCT conducted a joint investigation in Australia in 2018 that revealed a criminal syndicate involved in extensive cybercrimes. The syndicate opened 60 fictitious bank accounts at various Australian institutions using disposable SIM cards, phony email addresses, and identities stolen from darknet marketplaces. So the execution was so sophisticated that they stole credentials, gained access to victims' accounts, and took out more than \$3.3 million by building a phishing website that looked like a superannuation fund. The money trail was obscured by transferring \$2.5 million to a contact in Asia who bought luxury goods, sold them, and sent the money back to Australia in digital currencies. This case demonstrates how weak cybersecurity makes cyber-laundering possible as a facilitator of a fraudulent scheme because fraudulent

account creation was made possible by flaws in authentication systems (AUSTRAC, 2024). Similarly, emerging cyber-laundering schemes exploit vulnerabilities in digital platforms, as noted in the literature (Bošković, 2022). Simultaneously, criminals have also discovered a new method challenging cybersecurity domain, which involve bogus plays on music streaming platforms like Spotify or Deezer, in order to launder money. They make music, post it under fictitious names, and use bots or sponsored click farms to produce false streams. The funds seem like authentic artist royalties that are traceable, clean, and part of the official economy. And the best part is that it is inexpensive. By this method, \$4,000 can be laundered for as little as \$50 to \$300, or 7% to 12.5% of each dollar. In a well-known case, a gang that made money illegally purchased one million fake streams. The pure royalty money they received after that was approximately \$4,000. Monthly repetition of the plan results in a consistent cycle of low-risk money laundering that is concealed by entertainment revenue. With little initial examination, streaming rewards are scalable because they are tied to plays (Forestier, 2025).

Furthermore, the results from this study endorse several implications of past empirical evidence; for instance, as suggested by the work of Schneider & Buehn (2018), jurisdictions with stricter AML regulations tend to have less corrupt atmospheres. Similarly, the findings also align with Svitlychna's (2022) dissertation that emphasizes the importance of integrated cybersecurity and AML approaches. However, the AI-related insights in regard to money laundering risk present quite surprising and unexpected discoveries. To contrast with existing literature, our study suggests a complex relationship between AI and money laundering risk, differing from simpler perspectives. These findings indicate that a one-size-fits-all approach may not be effective for AI in this context. Instead, tailored AI tools are essential to combat money laundering effectively, as supported by several empirical studies (Ketenci et al., 2021; Eddin et al., 2021; Rouhollahi, 2021; Subbagari, 2023; Al-Ababneh et al., 2024). Regardless of misaligned findings related to AI and money laundering risk, this research has added new knowledge by countering the belief that simply being ready with AI will automatically help reduce risks related to money laundering. In order to draw implications from the study, it is crucial to keep in mind that, given the increase in cyber-laundering, it is obvious that enhancing public sector accountability and funding robust cybersecurity measures, such as digital forensics, penetration testing, vulnerability assessment, threat intelligence, and behavioral analytics, are critical to the success of cyber security integrated AML initiatives. Because the statistical information in this study is based on FATF member states, FATF can play a crucial role in addressing these shortcomings. With a mean score of 4.56, they are performing well, indicating a low to moderate risk of money laundering among FATF member states. To encourage the rest of the world to follow suit, these factors may be taken into consideration when evaluating a nation for money laundering risk.

CONCLUSION

In the shadowy underworld of global finance, money laundering works quietly, moving illegal funds through the arteries of legitimate economies. This quantitative study, based on 36 FATF members, has been useful in establishing determinants like corruption and cybersecurity capacity as significant in the fight against this complex crime. Based on our evidence, we establish that effective cybersecurity policy and lower perceived corruption (higher CPI scores) greatly lessen the threat of money laundering. Yet, the unexpected insignificance of AI readiness in our model challenges the narrative that technological advancement alone is a silver bullet. However, it can be inferred that the inefficient proxy measure could be the cause of insignificance, or it might be that the broad AI preparedness does not automatically curb money laundering risk. On the other hand, this contradiction can be justified, as technology is only as effective as its strategic deployment. This indicates that the battle against illicit finance is neither in a vacuum nor an isolated phenomenon but where technology and governance intersect. For the FATF member countries with an average Basel AML Index score of 4.56, this work is a clarion call to enhance cybersecurity, root out corruption, and adapt AI tools to cut off the financial lifelines of crime. These

results echo across borders, echoing the UNODC's vision of international cooperation to strangle illicit flows.

Additionally, this study creates a base for future research to dig deeper using a replicable index-based methodology. The future studies could involve longitudinal data, other potential factors to reduce money laundering risk, or AI measurements specific to AML that key players should create i.e., Napier AI AML Index. The fight against money laundering is a global game of chess where every move counts. This study is not the conclusion it just a beacon in a high-stake chess game. By improving governance with the right technology and collaborating across countries, we can shift the balance toward justice and prevent injurious effects that are ultimately associated with money laundering.

KEY RECOMMENDATIONS

- Improve national cybersecurity by investing in digital forensics and authentication systems.
- Supports public-private partnerships and cross-border harmonization by discussing tech-driven AML and international cooperation.
- Work with private sector experts to combine regulatory technology (RegTech) solutions.
- On a national level, foster the integration of anti-money laundering units with the mandate of cybercrime investigation within LEAs.
- Create specialized AI tools designed for AML.
- Set up a feedback loop with compliance teams to improve AI model accuracy.
- Use FATF's mutual evaluation process to share best practices among member states, especially with high-performing countries like Denmark (CPI: 90) and Canada (NCSI: 96.67), to raise global AML standards.
- Support UNODC capacity-building programs with specific training on cybersecurity, anti-corruption, and AI integration.
- Regularly update AML strategies to confront new cyber-laundering techniques, such as music streaming manipulation (Forestier, 2025). This can be done by incorporating real-time data analysis and cross-border investigative frameworks.

REFERENCES

- ACCA. (2022). Proliferation financing. What is it and why does it matter to my firm?
ACCA Global. <https://www.accaglobal.com/uk/en/technical-activities/uk-tech/in-practice/2022/october/proliferation-financing.html>
- Al-Ababneh, H. A., Nuralieva, C., Usmanalieva, G., Kovalenko, M., & Fedorovych, B. (2024). The use of artificial intelligence to detect suspicious transactions in the anti-money laundering system. *Theoretical and Practical Research in Economic Fields*, 15(4), 1039-1050. doi:10.14505/tpref.v15.4(32).19
- Alhajeri, R., & Alhashem, A. (2023). Using artificial intelligence to combat money laundering. *Intelligent Information Management*, 15(4), 284-315. doi: 10.4236/iim.2023.154014.

- Alnasser Mohammed, S. A. S. (2021). Money laundering in selected emerging economies: is there a role for banks? *Journal of Money Laundering Control*, 24(1), 102-110. doi:10.1108/JMLC-12-2019-0096
- Alsaibai, H., Waheed, S., Alaali, F., & Wadi, R. A. (2020). Online fraud and money laundry in Ecommerce. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security*(p.13). Academic Conferences and publishing limited. doi:10.34190/EWS.20.045
- Aluko, A., & Bagheri, M. (2012). The impact of money laundering on economic and financial stability and on political development in developing countries: The case of Nigeria. *Journal of Money Laundering Control*, 15(4), 442–457. doi:10.1108/13685201211266024
- Amara, I., Khelif, H., & Ammari, A. E. (2020). Strength of auditing and reporting standards, corruption and money laundering: a cross-country investigation. *Managerial Auditing Journal*, 35(9), 1243–1259. doi:10.1108/MAJ-10-2018-2026
- AUSTRAC (2024). *Case study: Money laundering through cybercrime*. <https://www.austrac.gov.au/case-study-money-laundering-through-cybercrime>
- Barone, R., Masciandaro, D., Schneider, F. (2019). Money laundering and corruption: birds of a feather flock together. *CESifo Working Paper*, No. 7687, Center for Economic Studies and ifo Institute (CESifo), Munich.
- Bartulovic, M., Aljinovic, N., & Piplica, D. (2023). Determining the Relationship Between Corruption and Money Laundering. *Montenegrin journal of economics*, 19(2), 109-118.
- Basel Institute on Governance. (2024). *Basel AML Index 2024 public edition*. <https://index.baselgovernance.org/ranking>
- Bošković, M. M. M. (2022). Cybercrime money laundering cases and digital evidence. *Strani pravni život*, 66(4), 451-46. doi:10.56461/SPZ_22406KJ
- Brue, M. (2023). Google Cloud Unleashes AI On Money Laundering Activities After Successful HSBC Trial. *Forbes*. <https://www.forbes.com/sites/moorinsights/2023/06/23/google-cloud-unleashes-ai-on-money-laundering-activities-after-successful-hsbc-trial/>
- Butler, T., & O'Brien, L. (2019). Understanding RegTech for digital regulatory compliance. *Disrupting finance: FinTech and strategy in the 21st century*, 85-102. doi:10.1007/978-3-030-02330-0_6
- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014. doi:10.1093/cybsec/tyac014
- Chong, A. and Lopez-de-Silanes, F. (2015), “Money laundering and its regulation”, *Economics and Politics*, Vol. 27 No. 1, pp. 78-123. doi:10.1111/ecpo.12051.
- Costa, J. (2022). The nexus between corruption and money laundering: deconstructing the Toledo-Odebrecht network in Peru. *Trends in Organized Crime*, pp. 1-22. doi:10.1007/s12117-022-09439-6
- Dobrowolski, Z., & Sułkowski, Ł. (2020). Implementing a sustainable model for anti-money laundering in the United Nations development goals. *Sustainability*, 12(1), 244. doi:10.3390/su12010244

- Dowers, K. and Palmreuther, S. (2003), "Developing an international consensus to combat money laundering and terrorism financing", *Infrastructure and Financial Markets Review*, Vol. 1, pp. 1-7.
- Draper, N. R., & Smith, H. (1998). Serial correlation in the residuals and the Durbin–Watson test. *Applied regression analysis*, 179-203. doi:10.1002/9781118625590.ch7
- Eddin, A. N., Bono, J., Aparício, D., Polido, D., Ascensão, J. T., Bizarro, P., & Ribeiro, P. (2021). Anti-money laundering alert optimization using machine learning with graphs. *arXiv preprint arXiv:2112.07508*. doi:10.48550/arXiv.2112.07508
- e-Governance Academy. (2024). *National Cyber Security Index (NCSI) ranking*. <https://ncsi.ega.ee/ncsi-index/?order=rank>
- Ekwueme, E., & Agu, O. B. (2025). Domino implications of corruption and money laundering in developing countries: a preliminary analysis on the way forward. *Northern Ireland Legal Quarterly*, 76(AD1), 1-23. doi:10.53386/nilq.v76iAD1.1159
- Ferwerda, J., & Reuter, P. (2019). Learning from money laundering National Risk Assessments: the case of Italy and Switzerland. *European Journal on Criminal Policy and Research*, 25, 5-20. doi:10.1007/s10610-018-9395-0
- Ferwerda, J., Kattenberg, M., Chang, H. H., Unger, B., Groot, L., & Bikker, J. A. (2013). Gravity models of trade-based money laundering. *Applied economics*, 45(22), 3170-3182. doi:10.1080/00036846.2012.699190
- Financial Action Task Force & Organisation for Economic Co-operation and Development. (2010). *Money laundering using new payment methods*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20using%20New%20Payment%20Methods.pdf>
- Financial Action Task Force, INTERPOL, & Egmont Group. (2023). *Illicit financial flows from cyber-enabled fraud*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf>
- Findley, M. G., Nielson, D. L., & Sharman, J. C. (2014). Global shell games: Experiments in transnational relations, crime, and terrorism (No. 128). *Cambridge University Press*. doi:10.1017/CBO9781107337848
- Forestier, B. (2025). Money Laundering Technique: Music Streaming Manipulation. *Linkedin*. <https://www.linkedin.com/feed/update/urn:li:activity:7335545791312248832/>
- Garcia-Bernardo, J., Fichtner, J., Takes, F. W., & Heemskerk, E. M. (2017). Uncovering offshore financial centers: Conduits and sinks in the global corporate ownership network. *Scientific reports*, 7(1), 6246.
- Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance*, 2(3), 211-239. doi:10.1007/s42521-020-00023-1
- Hope Sr, K. R. (2022). Reducing corruption and bribery in Africa as a target of the sustainable development goals: applying indicators for assessing performance. *Journal of Money Laundering Control*, 25(2), 313-329. doi:10.1108/JMLC-03-2021-0018
- International Monetary Fund. (2023). Anti-Money laundering and combating the financing of terrorism. *IMF*. <https://www.imf.org/en/Topics/Financial-Integrity/amlcft>

- International Monetary Fund. (2023). Financial crimes hurt economies and must be better understood and curbed. *IMF Blog*. <https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed>
- Jaffery, I. H., & Mughal, R. A. L. (2020). Money-laundering risk and preventive measures in Pakistan. *Journal of money laundering control*, 23(3), 699-714. doi:10.1108/JMLC-02-2020-0016
- Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information. *International Journal of Economics and Finance*, 11(10), 54-65. doi:10.5539/ijef.v11n10p54
- Ketenci, U. G., Kurt, T., Önal, S., Erbil, C., Aktürkoğlu, S., & İlhan, H. Ş. (2021). A time-frequency based suspicious activity detection for anti-money laundering. *IEEE Access*, 9, 59957-59967. doi:10.1109/ACCESS.2021.3072328
- Khelil, I., El Ammari, A., Bouraoui, M. A., & Khelif, H. (2023). Digitalization and money laundering: the moderating effects of ethical behaviour of firms and corruption. *Journal of Money Laundering Control*, 26(6), 1203-1220. doi:10.1108/JMLC-01-2023-0015
- Korejo, M. S., Rajamanickam, R., & Md. Said, M. H. (2021). The concept of money laundering: a quest for legal definition. *Journal of Money Laundering Control*, 24(4), 725-736. doi:10.1108/JMLC-05-2020-0045
- Kurniawan, V. (2023). The Role of Regulatory Technology & Bankers to Prevent Money Laundering in Bank. *JBMP (Jurnal Bisnis, Manajemen dan Perbankan)*, 9(1), 43-52. doi:10.21070/jbmp.v9i1.1660
- Ledyaeva, S., Karhunen, P., & Whalley, J. (2013). Offshore jurisdictions (including Cyprus), corruption money laundering and Russian round-trip investment (No. w19019). *National Bureau of Economic Research*. doi:10.3386/w19019
- Levi, M., & Reuter, P. (2006). Money laundering. *Crime and justice*, 34(1), 289-375. doi:10.1086/501508
- Lim, J. W., & Thing, V. L. (2022). Towards Effective Cybercrime Intervention. *arXiv preprint arXiv:2211.09524*. doi:10.48550/arXiv.2211.09524
- Lindasari, L. (2023). Implications of Money Laundering From Corruption Proceeds on The Application of Reverse Evidence in Corruption Crimes. *Corruptio*, 4(1), 61-72. doi:10.25041/corruptio.v4i1.3051
- Lombardo, G., & El Khoury, C. A. (2023). Investigating, Prosecuting, and Sanctioning Terrorist Financiers. In *Countering the Financing of Terrorism*. International Monetary Fund. doi:10.5089/9798400204654.071
- Mabunda, S. (2018). Cyberlaundering and the future of corruption in america. *JACL*, 2, 214. doi:10.14426/jacl.v2i1.1290
- Makkink, I. M., Steyn, B., & Bezuidenhout, H. C. (2024). The role of freight forwarding companies in detecting and investigating trade-based money laundering. *Journal of Money Laundering Control*, 27(7), 26-42. doi:10.1108/JMLC-04-2024-0069

- Malm, A., & Bichler, G. (2013). Using friends for money: The positional importance of money-launderers in organized crime. *Trends in Organized Crime*, 16(4), 365–381. doi:10.1007/s12117-013-9205-5
- May, R. D. (2023). How HSBC fights money launderers with artificial intelligence. *Google Cloud Blog*. <https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence>
- Meunier, D. (2018). Hidden beneficial ownership and control: Canada as a pawn in the global game of money laundering. *CD Howe Institute*, 519. doi:10.2139/ssrn.3246098
- Norton, S. (2018), “Suspicion of money laundering reporting obligations: auditor compliance, or sceptical failure to engage?” *Critical Perspectives on Accounting*, Vol. 50, pp. 56-66. doi:10.1016/j.cpa.2017.09.005
- Oxford Insights. (2024). *Government AI Readiness Index 2024*. <https://oxfordinsights.com/ai-readiness/ai-readiness-index/>
- Ramalingam, M., Selvi, G. C., Victor, N., Chengoden, R., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2023). A comprehensive analysis of blockchain applications for securing computer vision systems. *IEEE Access*, 11, 107309-107330. doi:10.1109/ACCESS.2023.3319089
- Reganati, F. and Oliva, M. (2018), “Determinants of money laundering: evidence from Italian regions”, *Journal of Money Laundering Control*, Vol. 21 No. 3, pp. 402-413. doi:10.1108/JMLC-09-2023-0150
- Rouhollahi, Z. (2021). Towards Artificial Intelligence Enabled Financial Crime Detection. *arXiv (Cornell University)*. doi:10.48550/arxiv.2105.10866
- Rusanov, G., & Pudovochkin, Y. (2021). Money laundering in the modern crime system. *Journal of money laundering control*, 24(4), 860-868. doi:10.1108/jmlc-08-2020-0085
- Schneider, F., & Buehn, A. (2018). Shadow economy: Estimation methods, problems, results and open questions. *Open Economics*, 1(1), 1-29. doi:10.1515/openec-2017-0001
- Shehu, A. Y. (2004). International initiatives against corruption and money laundering: An overview. *Journal of Money Laundering Control*, 8(1), 6–26. doi:10.1108/13685200510621181
- Soudijn, M. R. J. (2014). Using strangers for money: A discussion on money-launderers in organized crime. *Trends in Organized Crime*, 17(4), 255–270. doi:10.1007/s12117-014-9217-9
- Subbagari, S. (2023). Leveraging optical character recognition technology for enhanced anti-money laundering (AML) compliance. *SSRG International Journal of Computer Science and Engineering*, 10(5), 1-7. doi:10.14445/23488387/IJCSE-V10I5P102
- Svitlychna, A. O. (2022). Modelling the potential convergence of the cybersecurity system and combating money laundering. https://essuir.sumdu.edu.ua/bitstream-download/123456789/89735/1/Svitlychna_bac_rob.pdf
- Tassilo, H., & Ingrid, M. (2023). Financial crime watchdog FATF suspends Russia over Ukraine war. *Reuters*. <https://www.reuters.com/world/europe/financial-crime-watchdog-fatf-suspends-russias-membership-over-ukraine-war-2023-02-24/>

- Teichmann, F. M., J. (2020). How useful are anti-money laundering efforts in combating bribery? *Journal of Money Laundering Control*, Vol. 23, No. 2, pp. 309-314. doi:/10.1108/JMLC-03-2018-0025
- Transparency International. (2024). *Corruption Perceptions Index 2024*. <https://www.transparency.org/en/cpi/2024>
- Unger, B., & Ferwerda, J. (2011). Money laundering in the real estate sector: Suspicious properties. *Money Laundering in the Real Estate Sector*, Edward Elgar Publishing. doi:10.4337/9781781000915
- Wang, S. N., & Yang, J. G. (2007). A money laundering risk evaluation method based on decision tree. In *2007 international conference on machine learning and cybernetics* (Vol. 1, pp. 283-286). IEEE. doi:10.1109/ICMLC.2007.4370155