The Nexus of Cybercrime and Money Laundering: A Conceptual Paper

Mohd Afiq bin Azero[1], Sarah Nur Aisyah Kay Abdullah[1], Zailawati Zakaria[2],
Hasfaliza Haris[1] & Yusri Hazrol Yusoff[1]

[1] Faculty of Accountancy, Universiti Teknologi MARA (UiTM), Cawangan Selangor, Kampus Puncak Alam, 43200 Puncak Alam, Selangor, Malaysia

[2] Jabatan Kastam Diraja Malaysia, Kompleks Kementerian Kewangan No 3, Persiaran Perdana, Presint 2, 62596, Putrajaya, Malaysia

Correspondence: Mohd Afiq bin Azero, Faculty of Accountancy, Universiti Teknologi MARA (UiTM), Cawangan Selangor, Kampus Puncak Alam, 43200 Puncak Alam, Selangor, Malaysia. E-mail: mohdafiq816@uitm.edu.my

Received: March 3, 2024 Accepted: May 13, 2024 Online Published: May 22, 2024

doi:10.5430/afr.v13n2p167 URL: https://doi.org/10.5430/afr.v13n2p167

Abstract

The nexus between cybercrime and money laundering poses significant challenges that require a holistic understanding and strengthened global efforts to address. Cybercrimes provide financial motivation for criminals to engage in illicit activities. Techniques like cryptocurrency laundering and exploiting online payment systems allow criminals to disguise illegal proceeds. Investigating these modern financial crimes faces hurdles from rapid technological advancements, encryption, international jurisdiction issues, and lack of standardized information sharing between agencies and sectors. Gaps exist in current anti- money laundering legal frameworks in properly criminalizing emerging cyber threats and prosecuting related offenses effectively, as seen in the Malaysian context. Reforms are needed to enhance enforcement mechanisms, risk assessment practices, and the role of regulatory authorities like the Financial Intelligence Unit. A comprehensive approach combining updated laws, improved inter-agency coordination, public-private collaboration, andadaptive strategies is crucial to counter the evolving nexus between cybercrime and money laundering in today's digital landscape.

Keywords: Cybercrime, Money laundering, Cryptocurrency, Dark web, Regulatory framework

1. Introduction

The intersection between cybercrime and money laundering is a pressing issue in thedigital age. Cyber laundering, which involves the laundering of money through online transactions in cyberspace, has emerged as a significant concern (Nizovtsev et al., 2021). Cybercrimes, which encompass offenses where computers or communication tools are involved as targets, commission instruments, or incidental elements, are closely linked to the prevalence of computer technology (Al-Khater et al., 2020). Empirical studies have underscored the interconnection between the threat of cybercrimes and the prevention of money laundering, emphasizing the necessity for a comprehensive understanding of this relationship (Mugarura & Sali, 2020).

Money laundering, defined as the illegal act of concealing the nature, source, location,or movement of money derived from criminal activities, has adapted to exploit digital advancements, including the use of cryptocurrencies like Bitcoin for laundering proceeds fromcybercrimes (Bolgorian & Mayeli, 2020; Wegberg et al., 2018). The rise in money laundering levels is associated with the digitalization and technification of society, the globalization of financial markets, and the repercussions of quarantine measures due to the COVID-19 pandemic (Vitvitskiy et al., 2021). Furthermore, the impact of money laundering extends to theloss of state revenues, investor reluctance, and the erosion of trust in the international market(Adilah et al, 2022).

2. Background of the Study

The relationship between money laundering and cybercrime is intricate, with cybercriminals leveraging advanced technological solutions to illegally transfer money, posing a global threat with funds sourced from illegal and fraudulent activities (Vedamanikam & Chethiyar, 2020). The transition of the digital economy has given rise to new methods and schemes for money laundering, necessitating the identification of contemporary risks and the enhancement of counteracting strategies (Reznik et al., 2020). Additionally, the role of committee like National Coordination Committee to Counter Money Laundering (NCC) in coordinating, implementing and monitoring

Malaysia's anti-money laundering and counter financing of terrorism (AML/CFT) is crucial in preventing and eradicating the crime of money laundering (BNM, 2022).

The nexus between cybercrime and money laundering has given rise to "cyber-laundering," a criminal practice conducted in cyberspace through online transactions. The investigation and combat of cyber-related money laundering are of paramount importance due to the evolving landscape of financial crimes. This has necessitated the promotion of international standards in combating money laundering, particularly through an analysis of the mechanisms of money laundering obtained from cybercrime. Furthermore, the current emphasis on "risk-based" strategies in AML regulation underscores the need for regulatory, law enforcement and reporting agencies to respond to money laundering threats proportionately to the risks involved. Additionally, dynamic and bibliometric analyses of terms identifying the combating financial and cyber fraud system can provide valuable insights for improving the strategy of combating financial and cybercrimes, forming an analytical basis for the scientific community and practitioners.

The significance of investigating and combating cyber-related money laundering extends beyond financial realms. It is crucial for preserving the integrity of financial systems, protecting against illegal activities, and ensuring the safety and soundness of financial institutions. Moreover, the evolving nature of financial crimes, particularly in the digital age, necessitates a comprehensive understanding of the mechanisms and dynamics of money laundering obtained from cybercrime. Therefore, efforts to combat cyber-related money laundering are essential for maintaining the stability and security of financial systems, both domestically and internationally.

3. Purpose and Scope of the Paper

The purpose of this paper is to thoroughly examines the interconnected issues of cybercrime and money laundering. It begins by defining and emphasizing the significance of investigating and combating cyber-related money laundering. The paper aims to provide a comprehensive understanding of these issues, especially in the context of Malaysian environment of those SMEs covering the types of cybercrimes, the financial motivations behind them, and the techniques cybercriminals employ for money laundering. It delves into the challenges faced in investigating cyber- related money laundering cases, including technological advancements, international jurisdictional issues, and the lack of standardized information sharing.

The legal and regulatory frameworks surrounding these issues are explored, encompassing existing laws and regulations, identifying gaps in the current framework, and proposing reforms. This paper then concludes by summarizing key findings, underlining the importance of addressing the nexus between cybercrime and money laundering, and issuing a call to action for strengthened global efforts. Ultimately, the paper seeks to contribute insights, raise awareness, and advocate for measures to tackle the complex challenges arising from the convergence of cybercrime and money laundering in the modern digital landscape.

4. Literature Review

4.1 Understanding Cyber-Related Money Laundering

Cybercrime poses significant challenges to individuals, businesses, and governments, as it can result in financial losses, data breaches and damage to reputation. Understanding the nature and scope of cybercrime is essential for developing effective strategies to prevent and combat these activities. One of the key aspects of cybercrime is the use of technology to perpetrate illegal activities. This can include exploiting vulnerabilities in computer systems and networks, using malicious software to gain unauthorized access to sensitive information, or using the internet to deceive individuals into providing personal or financial information. Understanding the nature of cybercrime and its impact is crucial for developing effective strategies to prevent and combat these activities. By staying informed about the latest trends in cybercrime and implementing robust security measures, individuals and organizations can better protect themselves from this growing threat.

4.2 Cybercrime: The 3 Distinct Types

Cybercrime is defined as an unlawful act perpetrated through information and communication technology (ICT), targeting networks, systems, data, websites, and/or facilitating a crime. It distinguishes itself from traditional crime by transcending physical and geographic boundaries, being executed with less effort, greater ease, and increased speed. Europol classifies cybercrime into cyber-dependent crimes, which exclusively rely on computers or ICT, and cyber-enabled crimes, where traditional crimes are facilitated by the internet and digital technologies. The key distinction lies in whether ICT is the target or part of the modus operandi (method of operation). Cybercrime can be committed by individuals, groups, businesses, or nation-states, each with distinct motives. (UNODC, n.d).

Cybercrimes represent an existential threat to e-commerce, emphasizing the urgency of controlling their growth (Shah et al., 2019). Various types of cybercrime, such as online shopping fraud, online fraud banking/payment, cyber threats/harassment, malware, and hacking, have been distinguished (Yadav et al., 2021). The UNODC classifies cybercrime into three categories. First, offences against the confidentiality, integrity and availability of computer data or systems. Second, computer-related acts for personal or financial gain or harm and third, computer-content related acts (UNODC, n.d).

The first category is offenses against the confidentiality, integrity, and availability of computer data and systems reveals various cybercrimes. Hacking, characterized by unauthorized access to systems and data, may aim at gaining or maintaining access beyond authorization. Cybercriminals engage in intercepting data during transmission, compromising its confidentiality. Data interference involves intentionally damaging, deleting, or altering computer data without proper authorization. System interference, hindering a computer system's functioning without right, includes activities like denial of service (DoS) attacks that disrupt legitimate user access. Distributed denial of service (DDoS) attacks, executed with multiple computers, further obstruct access. Website defacement, a form of online vandalism, targets the content of websites. The illegal interception of data is emphasized, stressing the importance of confidentiality. Additionally, the module discusses malware-related offenses, covering the creation, possession, and distribution of various malicious software types, such as worms, viruses, Trojan horses, spyware, ransomware, crypto ransomware and doxware. Lastly, the production, possession, and distribution of computer misuse tools are outlined, encompassing tools designed for committing cybercrimes.

The second category of computer-related offenses, as outlined by the UNODC, encompasses crimes committed "for personal or financial gain or harm," inherently involving the use of computer systems or digital devices. One prominent offense within this category is computer-related fraud or forgery, which involves the intentional manipulation of computer data to create inauthentic information. This includes the impersonation of legitimate entities online for fraudulent purposes, often executed through tactics like phishing. Another facet is computer-related identity offenses, which entail the unlawful acquisition and use of personal information for various online schemes, including bank fraud, email fraud, and debit/credit card fraud. Additionally, offenses like sending or controlling the sending of spam focus on the deceptive dissemination of unsolicited emails or messages to mislead users. The category also extends to computer-related copyright or trademark offenses, addressing infringements such as digital piracy and unauthorized distribution of copyrighted material. Furthermore, computer-related acts causing personal harm encompass activities like cyberstalking, cyber harassment, and cyberbullying. In these instances, computer systems are utilized to harass, threaten, or intimidate individuals. Lastly, the category includes solicitation or "grooming" of children, where information and communication technologies are exploited to foster emotional relationships with victims, often leading to manipulative tactics, threats, or intimidation.

The third category is content-related offenses in cybercrimes, advocating for the use of the term "child sexual abuse material" to underscore the gravity of offenses related to child pornography. Emphasizing global legal variations, it details the criminalization of these offenses, including production, distribution, and possession of explicit content involving minors under the Council of Europe Cybercrime Convention. The UNODC explores commercial sexual exploitation of children, contentious content such as "racist and xenophobic material" and the criminalization of false information publication in certain countries. Delving into incitement to terrorism, it notes diverse global legal approaches, with examples from the United States and the United Kingdom. Recognizing the complex balance between counter-terrorism efforts and human rights, particularly freedom of expression, the UNODC underscores ongoing challenges in achieving a universally agreed approach, suggesting further exploration in related modules on legal frameworks, human rights, privacy, and data protection.

4.3 Financial Motivations behind Cybercrimes

The motivations behind cyberattacks, particularly in the context of financial gain, have been a subject of extensive research. Various studies have highlighted the prevalence of financial incentives as a primary driver for cybercriminal activities (Khan et al., 2021, Wegberg et al., 2017). These motivations range from financial frauds, phishing attacks, and money mule schemes to espionage, data breaches, and the retrieval of trade secrets and sensitive information. The financial benefits derived from cybercrimes provide a positive economic feedback to cybercriminals, making it a lucrative endeavor (Kshetri, 2009). Additionally, the transformation of the cybercrime industry from low-tech cyber-enabled crimes to high-tech sophisticated and organized attacks, such as hacking, reflects the evolving financial motivations behind cybercriminal activities (Wang et al., 2020).

Understanding the financial motivations behind cyberattacks is crucial for developing effective cybersecurity strategies and mitigating the impact of cybercrimes on individuals, organizations, and critical infrastructure. The

prevalence of financial gain as a primary motivator underscores the need for robust cybersecurity measures, including leadership in financial organizations, to prevent and combat cyberattacks (Khan et al., 2021). Furthermore, the impact of cybercrimes on financial inclusion and the healthcare industry emphasizes the urgency of addressing these threats to safeguard sensitive financial and medical information (Khan et al., 2021, McGowan et al, 2021).

4.4 Money Laundering Techniques Employed by Cybercriminals

Money laundering is a critical aspect of cybercrime, enabling criminals to disguise the illicit origins of their funds. Cybercriminals deploy sophisticated techniques to launder money effectively by encompass a range of sophisticated methods. Understanding money laundering techniques is crucial for developing effective countermeasures to combat financial crimes in the digital age.

4.5 Layering through Cryptocurrencies

In the realm of money laundering, the layering stage stands as a sophisticated tactic employed by cybercriminals to distance illicit funds from their origins. Cryptocurrencies, with their pseudonymous attributes and decentralized structure, have become a preferred tool for this purpose. The process of layering through cryptocurrencies involves a meticulous sequence of transactions designed to obscure the source of illegitimate funds. Initially, these funds are converted into cryptocurrencies like Bitcoin or Monero, often utilizing unregulated exchanges or mixing services for added obfuscation. A series of transactions within the cryptocurrency network ensues, where funds traverse multiple wallets and addresses in a seemingly haphazard manner.

The deployment of privacy-centric cryptocurrencies, particularly those employing advanced cryptographic techniques, adds an extra layer of complexity, making it arduous to trace these transactions. Integrating illicit funds with legitimate cryptocurrency transactions further masks their origin. Finally, the laundered funds are converted back into traditional fiat currency or other assets, completing the process.

The study by Wegberg et al. (2018) provides insights into the complexities of money laundering of cybercrime proceeds using Bitcoin, shedding light on the challenges and mixed results associated with this process. Additionally, the work by Desmond et al. explores the laundering of cryptocurrencies, including the layering stage, and provides a comprehensive understanding of the complexities involved in this process. Furthermore, the study by Teichmann and Falker (2021) discusses the use of cryptocurrencies to conceal criminal proceeds and foster an increase in money laundering platforms, shedding light on the challenges posed by cryptocurrencies in combating financial crimes.

4.6 Virtual Currencies in Online Transactions

The use of virtual currencies in online transactions has indeed provided cybercriminals with a fertile ground for money laundering activities. Virtual currencies, such as Bitcoin and Ethereum, offer pseudonymity and decentralization, enabling illicit financial activities to be conducted with a veil of anonymity (Böhme et al. 2015). Criminals integrate laundered funds into seemingly legitimate online transactions, leveraging the borderless nature of virtual currency transactions, making it challenging for authorities to track and regulate (Ho, 2020). Online platforms, including e-commerce websites and digital marketplaces, serve as conduits for money laundering schemes, allowing illicit funds to intertwine with legitimate financial flows, obscuring their origin (Farrugia et al., 2020).

The integration of virtual currencies into mainstream financial activities adds complexity to the detection process, posing significant challenges for anti-money laundering efforts (Leuprecht et al., 2022). The stateless and intangible nature of virtual currencies further complicates regulatory and legal frameworks, requiring active efforts from many countries to address the associated challenges (Leuprecht et al., 2022). Moreover, the use of machine learning techniques and blockchain technology has been explored for anomaly detection and tracking illicit financial flows in virtual currency transactions (Liu et al., 2023; Kamišalić et al., 2021).

The regulatory dialectic predicts an impeding cycle of innovation in the use of virtual money for laundering purposes, followed by an expected reactive behavior by governments (Dupuis & Gleason, 2020). Additionally, the potential use of virtual currencies in money laundering and terrorism funding has been a subject of analysis, emphasizing the need for effective regulatory measures (Sapoan et al., 2018). Furthermore, the widespread use of virtual currencies has raised concerns about their vulnerability to illicit financial flows, necessitating comprehensive research and regulatory responses (Rysin & Rysin, 2021).

The use of virtual currencies in online transactions has also been associated with risks to national security and has prompted discussions about their potential impact on the global economic development (Bobric, 2021; Dumitru, 2021). The potential of virtual currencies to contribute to the welfare of individuals and global economic development has been a topic of exploration, highlighting the need for a balanced approach to harnessing the benefits

while mitigating the risks (Dumitru, 2021).

4.7 Exploitation of Online Payment Systems

In the intricate landscape of money laundering cybercriminals exploit online payment systems to obscure the origins of illicit funds, integrating them into seemingly legitimate transactions across various platforms (Leonov et al., 2019). The speed, convenience, and global reach of these systems facilitate illicit financial activities while evading traditional regulatory scrutiny (Demetis, 2018). By funneling funds through multiple transactions, often across international borders, criminals create a complex trail that is challenging for authorities to trace (Walker & Unger, 2009). The inherent anonymity and accessibility of online payment systems provide a convenient veil for money launderers, allowing them to blend illicit proceeds with lawful financial flows (Johari et al., 2020).

Furthermore, the integration of emerging payment technologies and digital wallets further complicates detection efforts (Wang & Ou, 2015). The exploitation of online payment systems by cybercriminals for money laundering purposes poses significant challenges to traditional regulatory efforts. The integration of emerging payment technologies further complicates detection, emphasizing the need for enhanced cooperation, improved supervision mechanisms, and advanced detection techniques to combat this evolving threat.

4.8 Challenges in Investigating Cyber-Related Money Laundering Case

The surge in cybercrimes has led to the emergence of cyber-related money laundering as a significant challenge for law enforcement. Rapid technological advancements and the evolving tactics of cybercriminals make investigating these cases increasingly complex. This section explores the hurdles faced by investigators, from the swift evolution of criminal tools to international jurisdictional complexities. From encryption challenges to the covert realm of the dark web, this exploration emphasizes the crucial need for global cooperation and streamlined information sharing. The complexities inherent in investigating cyber-related money laundering cases underscore the urgency of developing adaptive strategies to counter the evolving nature of this modern-day criminal nexus.

4.9 Rapid Technological Advancements

In the ever-evolving landscape of cybercrimes, the pace of technological advancements presents both opportunities and challenges for law enforcement. This section delves into the dynamic realm of rapid technological progress, exploring the hurdles posed by the continuous evolution of cyber techniques. From sophisticated hacking methodologies to emerging attack vectors, we examine the need for constant adaptation and proactive measures to stay ahead in the face of these technological shifts.

4.10 Difficulty in Keeping Pace with Evolving Cyber Techniques

The inexorable march of technological advancements in the realm of cybercrimes presents an ever-growing challenge for law enforcement agencies worldwide. The rapid evolution of cyber techniques, including the development of novel malware, sophisticated hacking methodologies, and emerging attack vectors, necessitates an ongoing and dynamic effort to upgrade the skills and technological infrastructure of investigators (Wronka, 2021).

To address this perpetual challenge, continuous training programs for cybercrime investigators must be implemented (Sultan & Mohamed, 2022). These programs should focus on the latest cyber threats, advancements in digital forensics techniques, and emerging trends in cybersecurity (Perkins, 2021). Collaborative initiatives involving law enforcement agencies, academia, and the private sector can facilitate the timely exchange of knowledge and expertise, fostering a collective ability to stay ahead of malicious actors in the rapidly evolving cyber landscape (Tiwari et al., 2022).

4.11 Encryption Challenges and Anonymity on the Dark Web

The widespread use of encryption technologies, coupled with the cloak of anonymity provided by the dark web, poses a formidable obstacle in the investigation of cyber-related money laundering cases (Nuryanto, 2019). While encryption is essential for securing legitimate communications, it becomes a double-edged sword when exploited by cybercriminals seeking to conceal their illicit activities (Nizovtsev et al., 2021).

The dark web, with its encrypted communication channels and untraceable transactions, serves as a haven for various forms of illicit financial activities (Zolkaflil et al., 2019). Investigating transactions and communications conducted on the dark web presents substantial challenges due to the sophisticated concealment techniques employed by cybercriminals (Mniwasa, 2021). Overcoming these challenges requires a multi-faceted approach, including advancements in decryption technologies, international collaboration to dismantle dark web networks, and the development of innovative strategies to track and trace transactions even within encrypted environments (Nazri et al., 2019).

In parallel, a concerted effort must be made to enhance the investigative capabilities of law enforcement personnel. Training programs should encompass specialized courses on decrypting technologies, dark web investigations, and the nuances of tracking financial transactions in encrypted environments. Additionally, fostering partnerships with cybersecurity firms specializing in encryption can provide law enforcement with valuable insights and tools.

Tackling the encryption challenges associated with cyber-related money laundering demands a holistic and collaborative approach that combines technological innovation, international cooperation, and continuous education for law enforcement agencies. This multifaceted strategy is essential to navigate the intricate landscape of encrypted cyber activities and safeguard financial systems from illicit practices.

4.12 International Jurisdictional Issues

As cyber-related money laundering transcends geographical borders, navigating international jurisdictional challenges becomes paramount. In this section, we explore the cross-border nature of cybercrimes, emphasizing the urgent need for enhanced global cooperation and coordination among law enforcement agencies.

4.13 Cross-Border Nature of Cybercrimes

The borderless nature of cyberspace adds layers of complexity to the investigation and prosecution of cyber-related money laundering cases (Mniwasa, 2020). Cybercriminals operate without regard for geographical boundaries, orchestrating attacks and laundering money across multiple jurisdictions (Naheem, 2018). This cross-border nature of cybercrimes necessitates enhanced international cooperation and coordination among law enforcement agencies to effectively combat these illicit activities (Yeh, 2022).

Establishing international norms and frameworks that facilitate seamless collaboration is paramount (Akhtar et al., 2023). Mutual legal assistance treaties (MLATs), extradition agreements, and standardized protocols for sharing evidence and intelligence can streamline the process of pursuing cybercriminals across borders (Bošković, 2023). Developing a shared understanding of the global nature of cyber threats is essential for fostering stronger alliances and promoting collective action (Alshantti & Rasheed, 2021).

To enhance the effectiveness of international collaboration, it is imperative to evolve the existing legal frameworks and mechanisms. Strengthening international organizations dedicated to combating cybercrime, such as INTERPOL, and fostering open channels of communication between nations can contribute to a more cohesive global response. Additionally, regular forums and conferences focused on cybercrime should be established to encourage dialogue, share best practices, and address emerging challenges in a collaborative manner.

4.14 Coordination and Cooperation among Law Enforcement Agencies

Despite the acknowledged importance of international cooperation, challenges persist in fostering effective collaboration among diverse law enforcement agencies with varying mandates, resources, and legal frameworks (Yulianti et al., 2021). The inherent differences in organizational structures, communication protocols, and resource allocations often hinder the efficiency of joint efforts against cyber-related money laundering (Yeh, 2022).

To overcome these challenges, a critical need exists for enhanced inter-agency coordination mechanisms at both national and international levels (Ariyani & Junaidi, 2022). This involves establishing dedicated cybercrime units within law enforcement agencies, equipped with specialized knowledge and resources to address the unique challenges posed by cyber-related financial crimes. Fostering a culture of information sharing through the creation of secure platforms can help build trust and collaboration among law enforcement agencies globally (Šurković, 2021).

Joint training exercises, both domestically and internationally, are instrumental in aligning the methodologies and skill sets of investigators across borders. These exercises not only enhance the technical capabilities of law enforcement personnel but also cultivate a shared understanding of the evolving tactics employed by cybercriminals. Additionally, the development of standardized communication platforms and protocols is vital for facilitating real-time information exchange, enabling a more coordinated and agile response to cyber threats (Rahmadan, 2021).

Fostering a culture of collaboration necessitates systemic changes within law enforcement agencies, encompassing structural adaptations and procedural refinements. Dedicated task forces focused on international cybercrime investigations should be constituted, comprising experts from various agencies and jurisdictions. Furthermore, the establishment of shared databases and analytical tools can augment information sharing and analysis capabilities among these agencies, enabling more efficient cross-border investigations.

In essence, resolving international jurisdictional challenges in combating cyber- related money laundering demands a comprehensive overhaul of collaborative frameworks, legal structures, and operational methodologies among law enforcement agencies at both domestic and international levels. Embracing innovative strategies and fostering a

culture of cooperation are indispensable in confronting the globalized nature of cybercrimes.

4.15 Lack of Standardized Reporting and Information Sharing

Within the realm of combating cyber-related money laundering, a significant obstacle arises from the absence of standardized reporting and information-sharing. This section explores the challenges posed by this lack of coordination and emphasizes the urgent need for a global initiative to establish standardized mechanisms and enhance collaboration between public and private sectors.

4.16 Barriers to Information Exchange

The absence of standardized reporting mechanisms and information-sharing platforms represents a formidable impediment in facilitating the timely exchange of crucial data related to cyber-related money laundering cases (Jade et al., 2020). This lack of coordination not only undermines the effectiveness of law enforcement agencies in detecting and preventing cyber threats but also hampers their ability to respond promptly to the evolving nature of these illicit activities.

To tackle this pervasive challenge, a comprehensive global initiative is warranted to establish standardized reporting mechanisms and information-sharing platforms. Such an initiative must be prioritized to create a cohesive and interconnected global network. Encouraging collaboration between the public and private sectors is paramount in this endeavor. The establishment of secure and accessible databases and the implementation of protocols for responsible sharing of threat intelligence can significantly amplify the collective ability to detect and counter cyber-related money laundering activities.

Developing standardized reporting mechanisms involves crafting international agreements and protocols that facilitate the consistent and secure exchange of information across borders. This necessitates the involvement of international organizations, governmental bodies, and regulatory agencies to create a framework that ensures the confidentiality, integrity, and availability of shared information.

Furthermore, technology plays a pivotal role in enabling efficient information exchange. Investing in advanced data-sharing platforms, utilizing blockchain for secure transactions, and employing artificial intelligence for pattern recognition can enhance the speed and accuracy of cross-border information sharing. Regular audits and assessments should be conducted to ensure the robustness and compliance of these platforms with global standards.

4.17 Need for Improved Collaboration between Public and Private Sectors

Effective collaboration between the public and private sectors is indispensable for a comprehensive and proactive approach to combat cyber-related money laundering. Private sector entities, including financial institutions, technology companies, and cybersecurity firms, possess invaluable insights and data that can significantly contribute to law enforcement agencies' investigative efforts (Pontes et al., 2021).

Encouraging information sharing between these sectors requires the establishment of trusted partnerships and the development of clear frameworks for collaboration (Murray, 2011). Initiatives such as public-private information-sharing forums, joint task forces, and the creation of sector-specific threat intelligence sharing platforms can foster a more symbiotic relationship. These platforms should facilitate seamless communication, allowing for the swift exchange of information between public and private entities.

Moreover, incentivizing private sector entities to actively report suspicious activities is crucial. Establishing legal protections for such disclosures can alleviate concerns about potential repercussions and encourage a more open and transparent exchange of information. Governments and regulatory bodies should work collaboratively to establish frameworks that not only protect whistleblowers but also ensure that shared information is used responsibly and within the bounds of the law.

In conclusion, addressing the lack of standardized reporting and information sharing in the realm of cyber-related money laundering requires a multifaceted approach. The development of international agreements, investment in advanced technologies, and the cultivation of a collaborative culture between public and private sectors are pivotal steps in building a resilient and interconnected global defense against the evolving landscape of cyber threats.

The Proposed Conceptual Framework of the nexus of cybercrime and money laundering:

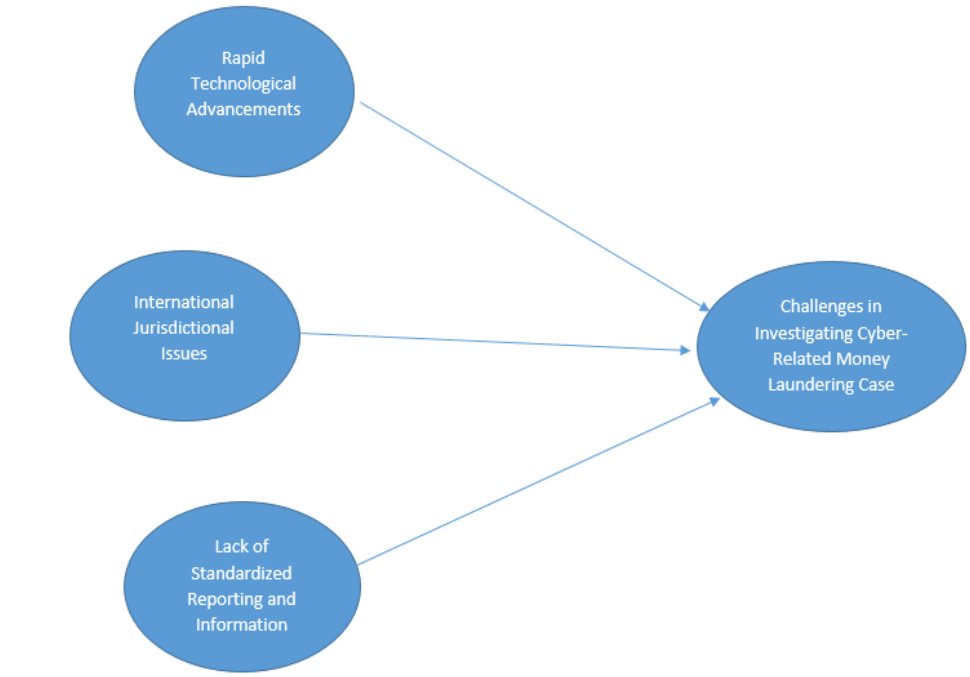

Figure 1. The Proposed Conceptual Framework of the nexus of cybercrime and money laundering

A conceptual framework is needed to address the challenges of cyber – related money laundering. The above conceptual framework is developed for the study in order to properly cybercrimes and money laundering. This conceptual framework emphasizes how the nexus could help better understanding in money laundering. Rapid technological advancements, International jurisdictional issues and lack of standardized reporting and information sharing contribute to detecting illegal activities.

4.18 Legal and Regulatory Framework

In the dynamic landscape of cybercrimes, cyber laundering stands out as a complex and elusive financial threat. This form of illicit financial activity leverages digital technologies to obscure the origins of funds, exploiting online vulnerabilities. As traditional legal frameworks struggle to keep pace with the rapid evolution of cyber techniques, there is an urgent need for adaptive and comprehensive regulations. This section delves into the legal and regulatory frameworks essential for combating cyber laundering, addressing the unique challenges posed by the intersection of technology, finance, and criminal enterprise.

4.19 Overview of Existing Laws and Regulations of National and InternationalAnti-Money Laundering Laws

The legal and regulatory framework for combating cybercrime money laundering in Malaysia is a critical aspect of the country's efforts to address financial crimes. Malaysia has established the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act (AMLATFA) to combat money laundering (Dhillon et al., 2013) aside from Computer Crimes Act 1997, Copyright (Amendment) Act 1997, Communications and Multimedia Act 1998, Personal Data Protection Act 2010, and Malaysian Penal Code, form the basis for addressing cybercrimes in the country Singh et al. (2021). However, there are calls for a more comprehensive legislative approach to effectively prosecute cybercrimes, as the current legislation is seen as fragmented and not fully equipped to address the evolving nature of cybercrimes (Mohamed, 2013). Additionally, the Computer Crimes Act 1997 is utilized to combat cybercrime attacks in Malaysia, highlighting the significance of existing legislation in addressing cyber threats (Rosli et al., 2021).

Efforts to combat cybercrimes in Malaysia involve a combination of cyber laws and traditional laws, reflecting the multifaceted approach taken by the country to address cyber threats. However, there is a need for a more cohesive and robust legislative framework to effectively combat cybercrimes and prosecute offenders. The absence of specific criminalization of cyberstalking within Malaysian cyber laws or traditional legal frameworks underscores the need

for more targeted legislation to address emerging cyber threats. There are also concerns about the effectiveness of the enforcement mechanisms under AMLATFA, indicating a need for more robust enforcement (Dhillon et al., 2013). Strengthening cooperation, coordination, and capacity among Law Enforcement Agencies (LEAs) is suggested to ensure effective targeting, investigation, and prosecution of money laundering (Nazri et al., 2019).

In addition to legal and legislative frameworks, the regulatory and supervisory framework is equally important in combating money laundering (Ige, 2021). The role of auditors is also highlighted in reducing the effects of money laundering, emphasizing the need for a comprehensive approach involving various stakeholders (Yusoff et al., 2023). Furthermore, the effectiveness of the Financial Intelligence Unit (FIU) and reporting mechanisms are crucial in combating money laundering (Ahmed et al., 2021).

5. Recommendation of the Study

The existing legal framework for combating cybercrime money laundering in Malaysia exhibits certain gaps and limitations, necessitating proposed reforms and enhancements. The proposed reforms can draw insights from various studies and scholarly works to address the deficiencies and inadequacies addressing cyber-related money laundering in the current legal framework. The regulatory framework in Malaysia, as required by the Financial Action Task Force (FATF), plays a significant role in addressing money laundering issues (Yusoff et al., 2023). However, variations in governance frameworks and regulatory mechanisms between states can pose challenges in combating money laundering effectively (Alshaer et al., 2021). The weaknesses in the investigation and prosecution of money laundering cases in Malaysia, particularly the limitations in prosecuting cases by Bank Negara Malaysia, indicate a gap in the legal framework's ability to effectively address and prosecute money laundering offenses (Mohamed & Ahmad, 2012).

The gaps in the legal framework for combating money laundering in Malaysia also extend to the role and effectiveness of the Financial Intelligence Unit (FIU). The lack of a legal framework and effective role of the FIU in combating money laundering activities in Malaysia suggests a need for strengthening the institutional and regulatory mechanisms to enhance the effectiveness of the legal framework (Ahmed et al., 2021). Furthermore, there are instrumental and normative deficiencies in the Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) law in Malaysia, indicating the need for comprehensive reforms to address the remaining deficiencies and ensure the legal framework's sufficiency in preventing and regulating money laundering and terrorist financing within the country (Hamin, 2017).

Furthermore, the role of technology should also be considered important especially in offering various tools, techniques, and advancements aimed at detecting, preventing and prosecuting financial crimes. Incorporating technologies such like data analytics and machine learning, cryptocurrency forensic tools, blockchain analysis, and the use of Artificial Intelligence (AI) in risk assessment could be among the options that can be used to combat any possibilities of money laundering activities to happen. The right approach is necessary for such counter measures to even be adopted.

The existing legal framework for combating cybercrime money laundering in Malaysia exhibits certain gaps and limitations, necessitating proposed reforms and enhancements. The proposed reforms can draw insights from various studies and scholarly works to address the deficiencies in the current legal framework.

6. Conclusion

One potential area for reform is the enhancement of the enforcement mechanisms under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act (AMLATFA) in Malaysia. The viability of enforcement mechanisms under money laundering and anti-terrorism offenses in Malaysia has been questioned, indicating a need for more effective enforcement (Shanmugam & Thanasegaran, 2008). Strengthening the enforcement mechanisms can significantly contribute to combating cybercrime money laundering. Additionally, the gaps in banking risk assessment related to trade-based money laundering (TBML) within the banking sector highlight the need for reforms in risk assessment practices to address financial crimes effectively (Zolkaflil et al., 2019). Reforms in risk assessment methodologies can enhance the legal framework's ability to combat money laundering activities.

Furthermore, the regulatory and supervisory framework for combating money laundering in Malaysia requires appraisal and potential enhancement to ensure the stability, productivity, and integrity of the financial system (Shehu, 2010). Effective implementation of the core and key Financial Action Task Force (FATF) Recommendations is crucial and can be a focus area for reforms. The weaknesses in the investigation and prosecution of money laundering cases in Malaysia, particularly the limitations in prosecuting cases by Bank Negara Malaysia, indicate a

need for reforms to enhance the legal framework's effectiveness in addressing and prosecuting money laundering offenses (Ho, 2010). Exploring other predicate offenses and concepts such as "irresistible inference" can be considered to increase efforts in prosecuting money laundering activities in the country (Sharman, 2008).

Moreover, the role and effectiveness of the Financial Intelligence Unit (FIU) in combating money laundering activities in Malaysia require attention and potential reforms to strengthen institutional and regulatory mechanisms (Holt, 2012). Reforms in the legal framework can focus on enhancing the role and effectiveness of the FIU in combating money laundering.

In conclusion, the nexus between cybercrime and money laundering poses significant challenges that require a holistic and coordinated global response. While countries like Malaysia have established legal frameworks and regulatory bodies to combat money laundering, gaps remain in addressing the evolving nature of cyber- related financial crimes. Issues like technological advances enabling new money laundering techniques, international jurisdictional complexities, and lack of standardized information sharing impede effective investigations. Proposed reforms focus on strengthening enforcement mechanisms, risk assessment practices, and the role of institutions like the FIU. Overall, a multi-pronged approach encompassing legal reforms, regulatory enhancements, technological solutions, and robust international cooperation is needed to navigate this complex issue impacting financial systems worldwide.

Acknowledgement

The authors would like to express their gratitude to the Faculty of Accountancy, University Teknologi MARA, Malaysia for funding and facilitating this research project.

References

Adilah, Fahmi, mohd zahir, Mohd, Ali, Hasani, & Hassan, Muhamad. (2022). A study of Malaysian anti-money laundering law and the impact on public and private sector. *Journal of Money Laundering Control, 26*. https://doi.org/10.1108/JMLC-02-2022-0035

Agbor, A. (2022). A delineation of the impact of illicit financial flows on the right to development: details from cameroon's special criminal court. *Journal of Financial Crime, 30*(4), 877-890. https://doi.org/10.1108/JFC-03-2022-0071

Ahmed, J., Nazri, S., Zolkaflil, S., Omar, N., & Shafie, N. (2021). The effectiveness of maldives' financial intelligence unit in combating money laundering. *Asia-Pacific Management Accounting Journal, 16*(3), 409-435. https://doi.org/10.24191/APMAJ.v16i3-16

Akhtar, N., Khan, A., & Raza, M. (2023). Technological advancements and legal challenges to combat money laundering: evidence from pakistan. *Pakistan Journal of Humanities and Social Sciences, 11*(1), 473-483. https://doi.org/10.52131/pjhss.2023.1101.0365

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access, 8,* 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Alshaer, H., Said, M., & Rajamanickam, R. (2021). The role of the palestine monetary authority in combating money laundering. *Journal of Money Laundering Control, 24*(4), 762-774. https://doi.org/10.1108/JMLC-09-2020-0106

Alshantti, A., & Rasheed, A. (2021). Self-organising map based framework for investigating accounts suspected of money laundering. *Frontiers in Artificial Intelligence, 4*. https://doi.org/10.3389/frai.2021.761925

Ampratwum, G., Osei-Kyei, R., & Tam, V. (2022). A scientometric review of public-private partnership in critical infrastructure resilience. *Iop Conference Series Earth and Environmental Science, 1101*(5), 052007. https://doi.org/10.1088/1755-1315/1101/5/052007

Ariyani, E., & Junaidi, J. (2022). *Position and evidence of predicate crime in the crime of money laundering,* 108-116. https://doi.org/10.2991/978-2-494069-81-7_13

Biagioli, A. (2008). Financial crime as a threat to the wealth of nations. *Journal of Money Laundering Control, 11*(1), 88-95. https://doi.org/10.1108/13685200810844523

BNM. (2022). *National Coordination Committee to Counter Money Laundering (NCC)*. BNM (n.d) Human Verification. (n.d.). https://amlcft.bnm.gov.my/web/amlcft/domestic- coordination.

Bobric, G. (2021). Risks to the national security generated by the widespread use of cryptocurrency. *Scientific Bulletin, 26*(2), 87-97. https://doi.org/10.2478/bsaft-2021-0011

Bolgorian, M., & Mayeli, A. (2020). Accounting conservatism and money laundering risk. *Accounting Research Journal, 33*(2), 343-361. https://doi.org/10.1108/ARJ-12-2018-0221

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-238. https://doi.org/10.1257/jep.29.2.213

Boonkrong, S., Prompunjai, K., Watcharawongbodee, S., & Chueachantuek, S. (2022). The evolution of cyberattack motives. *International Journal on Advanced Science Engineering and Information Technology, 12*(5), 1956. https://doi.org/10.18517/ijaseit.12.5.16431

Bošković, M. (2023). Cybercrime money laundering cases and digital evidence. *Strani Pravni Zivot, 66*(4), 451-167. https://doi.org/10.56461/SPZ_22406KJ

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk. *European Societies, 23*(sup1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Chen, Z., Le, D., Teoh, E., Nazir, A., Karuppiah, E., & Lam, K. (2018). Machine learning techniques for anti-money laundering (aml) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems, 57*(2), 245-285. https://doi.org/10.1007/s10115-017-1144-z

Chitimira, H., & Munedzi, S. (2023). An evaluation of customer due diligence and related anti-money laundering measures in the united kingdom. *Journal of Money Laundering Control, 26*(7), 127-137. https://doi.org/10.1108/JMLC-01-2023-0004

Chitimira, H., & Munedzi, S. (2023). Historical aspects of customer due diligence and related anti-money laundering measures in south africa. *Journal of Money Laundering Control, 26*(7), 138-154. https://doi.org/10.1108/JMLC-01-2023-0016

Demetis, D. (2018). Fighting money laundering with technology: a case study of bank x in the UK. *Decision Support Systems, 105*, 96-107. https://doi.org/10.1016/j.dss.2017.11.005

Dhillon, G., Ahmad, R., Rahman, A., & Miin, N. (2013). The viability of enforcement mechanisms under money laundering and anti-terrorism offences in Malaysia. *Journal of Money Laundering Control, 16*(2), 171-192. https://doi.org/10.1108/13685201311318511

Dumitru, A. (2021). The potential of virtual currencies to contribute to the welfare of individuals and the global economic development. *Land Forces Academy Review, 26*(4), 401-405. https://doi.org/10.2478/raft-2021-0052

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime, 28*(1), 60-74. https://doi.org/10.1108/JFC-06-2020-0113

Ekwueme, E. (2021). The dichotomisation fallacy of public and private corruption and the quantification dilemma. *Journal of Financial Crime, 28*(4), 1179-1192. https://doi.org/10.1108/JFC-10-2020-0215

Farrugia, S., Ellul, J., & Azzopardi, G. (2020). Detection of illicit accounts over the ethereum block chain. *Expert Systems With Applications, 150*, 113318. https://doi.org/10.1016/j.eswa.2020.113318

Ferwerda, J. (2009). The economics of crime and money laundering: does anti-money laundering policy reduce crime? *Review of Law & Economics, 5*(2), 903-929. https://doi.org/10.2202/1555-5879.1421

Gilmour, N., & Ridley, N. (2015). Everyday vulnerabilities – money laundering through cash intensive businesses. *Journal of Money Laundering Control, 18*(3), 293-303. https://doi.org/10.1108/JMLC-06-2014-0019

Hataley, T. (2020). Trade-based money laundering: organized crime, learning and international trade. *Journal of Money Laundering Control, 23*(3), 651-661. https://doi.org/10.1108/JMLC-01-2020-0004

Ho, C. (2020). Does virtual currency development harm financial stocks' value? comparing Taiwan and China markets. *Economic Research-Ekonomska Istraživanja, 33*(1), 361-378. https://doi.org/10.1080/1331677X.2019.1702076

Holt, T., Lee, J., & Smirnova, O. (2022). Exploring risk avoidance practices among on-demand cybercrime-as-service operations. *Crime & Delinquency, 69*(2), 415-438. https://doi.org/10.1177/00111287221103753

Ige, A. (2021). Appraisal of the regulatory frameworks for combatting money laundering in nigeria. *Journal of Money Laundering Control, 25*(2), 345-357. https://doi.org/10.1108/JMLC-02-2021-0013

Irwin, A., Choo, K., & Liu, L. (2012). Modelling of money laundering and terrorism financing typologies. *Journal of Money Laundering Control, 15*(3), 316-335. https://doi.org/10.1108/13685201211238061

Jade, A., Fajrin, Y., Putri, D., & Nugraha, A. (2020). The reverse burden of proof in indonesia's money laundering: a review. *Lentera Hukum, 7*(3), 355. https://doi.org/10.19184/ejlh.v7i3.18680

Johari, R., Zul, N., Talib, N., & Hussin, S. (2020). *Money laundering: customer due diligence in the Era of cryptocurrencies*. https://doi.org/10.2991/aebmr.k.200305.033

Joveda, N., Khan, M., & Pathak, A. (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. https://doi.org/10.5539/ijef.v11n10p54

Kamišalić, A., Kramberger, R., & Fister, I. (2021). Synergy of blockchain technology and data mining techniques for anomaly detection. *Applied Sciences, 11*(17), 7987. https://doi.org/10.3390/app11177987

Kemsley, D., Kemsley, S., & Morgan, F. (2021). Tax evasion and money laundering: a complete framework. *Journal of Financial Crime, 29*(2), 589-602. https://doi.org/10.1108/JFC-09-2020-0175

Khan, A., Mubarik, M., & Naghavi, N. (2021). What matters for financial inclusions? evidence from emerging economy. *International Journal of Finance & Economics, 28*(1), 821-838. https://doi.org/10.1002/ijfe.2451

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O., & Vergara, R. (2022). A systematic literature review on cybercrime legislation. *F1000research, 11*, 971. https://doi.org/10.12688/f1000research.123098.1

Khan, H., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2022). *Role of authentication factors in fin-tech mobile transaction security*. https://doi.org/10.21203/rs.3.rs-2365318/v1

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the Acm, 52*(12), 141-144. https://doi.org/10.1145/1610252.1610288

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime, 30*(4), 1036-1054. https://doi.org/10.1108/JFC-07-2022-0161

Li, Z., Zhang, Y., Wang, Q., & Chen, S. (2022). Transactional network analysis and money laundering behavior identification of central bank digital currency of china. *Journal of Social Computing, 3*(3), 219-230. https://doi.org/10.23919/JSC.2022.0011

Liu, J., Yin, C., Wang, H., Wu, X., Lan, D., Zhou, L., …Ge, C. (2023). Graph embedding- based money laundering detection for ethereum. *Electronics, 12*(14), 3180. https://doi.org/10.3390/electronics12143180

McGowan, A., Sittig, S., & Andel, T. (2021). *Medical internet of things: a survey of the current threat and vulnerability landscape*. https://doi.org/10.24251/HICSS.2021.466

Mekpor, E., Aboagye, A., & Welbeck, J. (2018). The determinants of anti-money laundering compliance among the financial action task force (fatf) member states. *Journal of Financial Regulation and Compliance, 26*(3), 442-459. https://doi.org/10.1108/JFRC-11-2017-0103

Mniwasa, E. (2020). Tackling money laundering in tanzania: are private legal practitioners crime enablers or ineffectual and reluctant gatekeepers? *Journal of Money Laundering Control, 24*(2), 291-324. https://doi.org/10.1108/JMLC-03-2020-0028

Mniwasa, E. (2021). Institutionalizing the fight against money laundering in tanzania: the potential, limitations and challenges. *Journal of Money Laundering Control, 25*(4), 792-832. https://doi.org/10.1108/JMLC-07-2021-0083

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control, 24*(1), 10-28. https://doi.org/10.1108/JMLC-11-2019-0092

Murray, K. (2011). The uses of irresistible inference. *Journal of Money Laundering Control, 14*(1), 7-15. https://doi.org/10.1108/13685201111098842

Naheem, M. (2018). Tbml suspicious activity reports – a financial intelligence unit perspective. *Journal of Financial Crime, 25*(3), 721-733. https://doi.org/10.1108/JFC-10-2016-0064

Nazri, S., Zolkaflil, S., & Omar, N. (2019). Mitigating financial leakages through effective money laundering investigation. *Managerial Auditing Journal, 34*(2), 189-207. https://doi.org/10.1108/MAJ-03-2018-1830

Nizovtsev, Y. Y., Parfylo, O., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2021). Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control, 25*(2), 297-305. https://doi.org/10.1108/JMLC-02-2021-0015

Nuryanto, A. (2019). Problem penyidikan tindak pidana pencucian uang yang berasal dari predicate crime perbankan. *Bestuur, 7*(1), 54. https://doi.org/10.20961/bestuur.v7i1.43437

Parida, D., & Kumar, D. (2020). A framework to score the risk associated with suspicious money laundering activity and social media profile. *Indian Journal of Finance and Banking, 4*(2), 1-10. https://doi.org/10.46281/ijfb.v4i2.662

Perkins, A. (2021). Does holding offshore jurisdictions to higher aml standards really assist in preventing money laundering?. *Journal of Money Laundering Control, 25*(4), 742-756. https://doi.org/10.1108/JMLC-10-2021-0116

Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2021). Anti-money laundering in the united kingdom: new directions for a more effective regime. *Journal of Money Laundering Control, 25*(2), 401-413. https://doi.org/10.1108/JMLC-04-2021-0041

Rahmadan, D. (2021). The development of the crime of money laundering in the industrial revolution 4.0. *Melayunesia Law, 5*(1), 85. https://doi.org/10.30652/ml.v5i1.7840

Reznik, O., Danylevska, Y., Стеблянко, A. B., Chekmarova, I. M., & Karelin, V. V. (2020). Current status and prospects of anti-money laundering in digital economy. *REICE: Revista Electrónica De Investigación en Ciencias Económicas, 8*(15), 314-327. https://doi.org/10.5377/reice.v8i15.9962

Rose, K. (2020). Disclosing anti-money launderers through csr regulation – a new way to combat money laundering. *Journal of Money Laundering Control, 23*(1), 11-25. https://doi.org/10.1108/JMLC-07-2019-0062

Rysin, V., & Rysin, N. (2021). Vulnerability of virtual assets to illicit financial flows. *Economics Entrepreneurship Management, 8*(1), 35-42. https://doi.org/10.23939/eem2021.01.035

Shah, M., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organizational practices. *Information Technology and People, 32*(5), 1125-1129. https://doi.org/10.1108/ITP-10-2019-564

Sultan, N., & Mohamed, N. (2022). Financial intelligence unit of pakistan: an evaluation of its performance and role in combating money laundering and terrorist financing. *Journal of Money Laundering Control, 26*(4), 862-876. https://doi.org/10.1108/JMLC-04-2022-0060

Šurković, A. (2021). Criminal investigation of money laundering in the practice of the financial intelligence unit of the state investigation and protection agency. *Praxis International Journal of Social Science and Literature, 4*(2), 42-52. https://doi.org/10.51879/PIJSSL/4.2.10

Sapoan, H., & Hamdani, H. (2018). Potential use of virtual currencies in money laundering and terrorism funding in indonesia. *Russian Journal of Agricultural and Socio-Economic Sciences, 77*(5), 5-11. https://doi.org/10.18551/rjoas.2018-05.01

Souto, M. (2013). Money laundering, new technologies and Spanish penal reform. *Journal of Money Laundering Control, 16*(3), 266-284. https://doi.org/10.1108/JMLC-01-2013-0002

Walker, J., & Unger, B. (2009). Measuring global money laundering: "the walker gravity model". *Review of Law & Economics, 5*(2), 821-853. https://doi.org/10.2202/1555-5879.1418

Teichmann, F. M. J., & Falker, M. C. (2021). Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Control, 24*(4), 775-788. https://doi.org/10.1108/JMLC-05-2020-0060

Tiwari, M., Ferrill, J., & Mehrotra, V. (2022). Using graph database platforms to fight money laundering: advocating large scale adoption. *Journal of Money Laundering Control, 26*(3), 474-487. https://doi.org/10.1108/JMLC-03-2022-0047

UNODC. (n.d.). *Univesity Module Series-Cybercrime*. United Nations on Drugs and Crime. https://www.unodc.org/e4j/en/tertiary/cybercrime.html

Varelas, E. (2017). Is bank lending corruption self-regulatory?. *Journal of Economic & Financial Studies, 5*(3), 31. https://doi.org/10.18533/jefs.v5i3.285

Vedamanikam, M., & Chethiyar, S. D. M. (2020). Money mule recruitment among university students in malaysia: awareness perspective. *PUPIL: International Journal of Teaching, Education and Learning*, *4*(1), 19-37. https://doi.org/10.20319/pijtel.2020.41.1937

Vitvitskiy, S. S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. B. (2021). Formation of a new paradigm of anti-money laundering: the experience of ukraine. *Problems and Perspectives in Management*, *19*(1), 354-363. https://doi.org/10.21511/ppm.19(1).2021.30

Walker, J., & Unger, B. (2009). Measuring global money laundering: "the walker gravity model". *Review of Law & Economics*, *5*(2), 821-853. https://doi.org/10.2202/1555-5879.1418

Wang, Y., & Ou, Y. (2015). Anti-money laundering regulation of china's mobile payment and settlement industry. *Open Journal of Social Sciences*, *03*(11), 276-281. https://doi.org/10.4236/jss.2015.311033

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in nigeria: cyber security breaches, practices and capability. *International Journal of Law Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

Wegberg, R. v., Oerlemans, J., & Deventer, O. v. (2018). Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 00-00. https://doi.org/10.1108/JFC-11-2016-0067

Wegberg, R., Klievink, B., & Eeten, M. (2017). Discerning novel value chains in financial malware. *European Journal on Criminal Policy and Research*, *23*(4), 575-594. https://doi.org/10.1007/s10610-017-9336-3

Wronka, C. (2021). "cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330-344. https://doi.org/10.1108/JMLC-04-2021-0035

Yaacob*, N., & Harun, A. (2019). The effectiveness of money-laundering regulations: evidence from money-services-business industry in Malaysia. *International Journal of Recent Technology and Engineering*, *8*(3), 8643-8648. https://doi.org/10.35940/ijrte.C6454.098319

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). *Various types of cybercrime and its affected area.*, 305-315. https://doi.org/10.1007/978-981-15-9774-9_30

Yeh, S. (2022). New financial action task force recommendations to fight corruption and money laundering. *Laws*, *11*(1), 8. https://doi.org/10.3390/laws11010008

Yeh, S. (2022). New osce recommendations to combat corruption, money laundering, and the financing of terrorism. *Laws*, *11*(2), 23. https://doi.org/10.3390/laws11020023

Yulianti, S., Wiwoho, J., & Rustamaji, M. (2021). *Criminal law enforcement of money laundering as a community protection effort against economic crime in indonesia*. https://doi.org/10.2991/assehr.k.211014.019

Yusoff, Y., Hamidi, A., Ali, N., Zaidi, N., Isa, N., & Paharazi, M. (2023). Role of auditors in reducing effects of money laundering: concept paper. *International Journal of Academic Research in Economics and Management Sciences*, *12*(1). https://doi.org/10.6007/IJAREMS/v12-i1/16585

Zolkaflil, S., Omar, N., & Nazri, S. (2019). Implementation evaluation: a future direction in money laundering investigation. *Journal of Money Laundering Control*, *22*(2), 318- 326. https://doi.org/10.1108/JMLC-03-2018-0024