Cyber-Laundering and Its Impacts on Auditors: A Conceptual Paper

Nur Afiqah Md Amin[1], Nurul Iffah Ghazali[1], Nurul Najihah Hassan[1], Nur Aisyah Ramlan[1],
Nur Maisara Sofea Abdul Rahman[1] & Sarah Lailatulhuda Sharifudin[1]

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

Correspondence: Nur Afiqah Md Amin, Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia. E-mail: afiqahamin@uitm.edu.my

Received: March 2, 2024 Accepted: March 27, 2024 Online Published: April 3, 2024

doi:10.5430/afr.v13n2p24 URL: https://doi.org/10.5430/afr.v13n2p24

Abstract

This concept paper explores how cyber-laundering affects auditors and the difficulties they encounter in identifying and preventing this emerging form of financial crime. Cyber-laundering is the act of utilizing digital currencies and online platforms to facilitate money laundering activities, which complicates the tracking of illegal financial transactions by auditors. The study emphasizes that cyber-laundering attracts money launderers due to the anonymity, lack of face-to-face interaction, as well as rapid transaction speed. It also discusses the placement, layering, and integration process of cyber-laundering, which makes it harder for auditors to detect and prevent fraud. Risks associated with cyber-laundering, including reputation, regulatory, and geographical are also identified. The literature review part analyzes the impact on auditors, various elements of cyber-laundering, and the process involved. The study highlights a research gap in understanding the effects of cyber-laundering on auditors and suggests the necessity for thorough research in this area. The paper ends with recommendations for enhancing public awareness and education on cyber-laundering. To effectively tackle cyber-laundering, a multidisciplinary strategy is necessary, along with continuous attempts to improve auditors' skills in dealing with this complex financial crime.

Keywords: cyber-laundering, money-laundering, cybercrime

1. Introduction

Money laundering has long been a concern due to criminals' attempts to normalize and incorporate the proceeds of their illegal operations into the legal financial system. The term “money laundering” was first used at the beginning of the twentieth century to label the operations that in some way intended to hide or disguise the origin of the money obtained from the proceeds of the crime (Harahap, 2020).

Cyber-laundering is a specific type of money laundering, so it is important to have a clear understanding of the broader concept of money laundering (Handa, & Ansari, 2022). In recent years, the rapid advancement of technology and the widespread use of the Internet have given rise to a new form of financial crime known as cyber-laundering. Cyber-laundering refers to the process of engaging in money laundering activities through the Internet and online exchanges (Irina, 2018). These exchanges provide a wide variety of options, quick transactions, and low fees, making them attractive for facilitating money laundering. The fight against cyber-laundering requires a multidisciplinary approach that includes expertise from the areas of criminology, cybersecurity, economics, and law as perpetrators take advantage of the complexity of the online world.

While the concept of money laundering is not new, the advent of cyber-laundering presents unique complexities and risks for auditors. The placing, layering, and integrating processes involved in money laundering allow for the transfer and conversion of illegal fiat cash into lawful assets. To conceal the trail and the original source of the illicit cash, the process frequently relies on a large number of local and remote actors who employ a wide variety of financial institutions and complicated instruments (Calafos & Dimitoglou., 2022). Online money laundering has expanded into the digital realm with the advent of cryptocurrencies and blockchain technology.

According to global cybercrime statistics in 2019, more than 60% of businesses encountered instances of phishing and social engineering attacks. The rise in these types of attacks during that year resulted in studies indicating that approximately 63.8% of businesses fell victim to cybercrime. (Lazic, 2023). More companies started using newly developed IT systems and exploring advanced technology. Thus, there is an increasing trend of cyber-laundering in

Malaysia. These systems frequently contain confidential information, such as customer information and financial records.

The increase in cybercrime has caused major problems for people, organizations, and nations alike in a world that is becoming more digitally linked and interconnected. Cyber-laundering is a sneaky method that allows criminals to pass off monies they have gained illegally as legitimate through the complicated network of the digital world. This type of cybercrime is one of the most dangerous types of crime. Understanding the complexity of cyber-laundering has become crucial for researchers, politicians, and law enforcement organizations as traditional money laundering techniques become more and more outdated in the face of technological developments.

The impact of cyber-laundering on auditors is multifaceted and requires thorough investigation. Cyber-laundering can increase the difficulty of tracking funds, the risk of being tricked, the difficulty of obtaining evidence, and the workload and stress levels of auditors. Auditors must utilize fraud prevention techniques by making fraud less likely to occur, increasing the difficulty of committing fraud by improving detection methods, reducing fraud losses, and identifying sufficient appropriate audit evidence to sentence fraud perpetrators for white-collar crimes. This will also have an impact on auditors' work since they need to learn new skills and comply with new regulations on cyber-laundering (Seetharaman et al., 2017).

Criminals who engage in money laundering are constantly looking for new ways to evade detection by the authorities and the internet has given them a wide range of options (Sampson, 2023). Authorities have a difficult time identifying and investigating crimes because criminals use encryption, decentralized systems, and complex money flow patterns to conceal the source and destination of illicit monies. As a result, the dangers of cyber-laundering include serious social, economic, and security effects in addition to financial losses.

There is a growing body of literature on money laundering and its implications for auditors, however, there is a significant research gap concerning the specific impacts of cyber-laundering on auditors. Existing literature primarily focuses on traditional forms of money laundering, with limited attention given to cyber-laundering. For instance, the studies on money laundering in the modern crime system (Rusanov & Pudovokochkin, 2020), studies on qualifying and raising anti-money laundering alarms with deep learning (Jensen & Iosifidis, 2023), and studies on fraud detection and prevention in e-commerce (Rodrigues et al., 2022). These studies lack comprehensive specific addresses of unique characteristics of cyber-laundering. As cybercrimes continue to evolve, there is a lack of comprehensive studies that specifically address the unique characteristics and implications of cyber-laundering for auditors. There is also an inadequate examination of the auditor's response to cybercrimes. While some studies touch upon the impacts of cyber-laundering on auditors, there is a need for more extensive research that explores the specific challenges faced by auditors in detecting and preventing cyber-laundering activities.

This concept paper aims to explore how cyber-laundering affects auditors, highlighting the difficulties they encounter in addressing cyber-laundering and identifying the potential strategies to enhance their capabilities in combating this evolving form of financial crime.

2. Literature Review

2.1 Impacts on Auditor

The accounting and auditing industries are susceptible to numerous impacts from cyber-laundering. Due to the difficulty in detecting and preventing cyber-laundering, the inherent risk of financial statement misstatement and, consequently, the audit risk assessment may be increased. Criminals frequently employ complex financial transactions as a means to obscure the origin of their illicit funds. This can make it difficult for auditors to monitor the movement of funds and discover suspicious transactions. Furthermore, auditors encounter challenges in identifying and investigating cyber-laundering schemes due to the criminals' reliance on digital technology to execute their illicit activities. For instance, employing advanced hacking techniques to steal financial data and utilizing anonymizing software to conceal their identities. Cyber-laundering also can occur in an organization due to a deficiency in internal controls (Samuel, Pelumi & Fasilat, 2021). Many organizations are unaware of the risks of cyber-laundering, resulting in a lack of awareness. This can make it easier for criminals to launder money.

Cybercriminals are always finding new ways to exploit vulnerabilities in computer systems, and auditors may not be aware of all of these risks. The normal audit procedures can detect some cybercrimes, but they are not always effective. Auditors may not have the necessary technical expertise to detect smooth cybercrimes. Thus, auditors need to improve their ability to detect cybercrimes. Auditors need to work closely with IT professionals to understand the risks of cybercrime and to design appropriate audit procedures. Auditors can use computer-assisted audit tools (CAATs) to automate some of the audit procedures and to identify suspicious activity (Samagaio & Diogo, 2022).

Auditors should also stay up-to-date on the latest cybercrime trends and techniques to better understand and be able to trace their activities.

Other than that, the cost of cybercrime detection software can be quite expensive. It depends on the size and complexity of the firm, the features and functionality of the software, and the number of users. However, the cost of cybercrime detection software is not the only factor that audit firms need to consider, they also need to consider the cost of training the staff on how to use the software. Therefore, audit firms should carefully consider their needs and budget when selecting cybercrime detection software.

Another impact of cyber-laundering on auditors is it requires auditors to undergo training and enhance their skills to combat cyber-laundering (Wayo, 2023). Auditors need to attend training courses on cyber-laundering which can help auditors learn about the latest cyber-laundering techniques and how to detect them. Auditors also need to understand the landscape of cybercrime and stay up-to-date on the latest trends. This can be done by reading industry publications, attending conferences, and networking with other professionals in the industry.

Lastly, cyber-laundering impacts the cyber security assurance process. Gaining insight into an organization is a continuous process undertaken by auditors to acquire fundamental information. Analytical procedures can aid in identifying abnormal transactions that impact both the financial statement and audit process. When auditors notice the possibility of fraudulent activity that could impact the accuracy of the financial statement, they are obligated to perform further audit procedures. If the doubts are not resolved, the auditor, in collaboration with the management, must ascertain if the impact of the fraud has been rectified in the financial statements and how this will impact the auditor's report. Therefore, cyber-laundering can make it more difficult for auditors to assess the risks of financial statement misstatement, design and implement appropriate audit procedures, identify and investigate suspicious transactions, and form an opinion on the fairness of the financial statements.

2.2 Aspects of Cyber-laundering

Three aspects of cyber transactions that can attract money launderers which are anonymity, no face-to-face contact, and speed of transactions (Wronka, 2022). All of these aspects provide a possibility for money launderers to conduct a crime because they may all be accomplished through the use of the internet considering the internet is a vast network of connected computers and devices that allows for the sharing of information and communication between users around the world. It is a global network of networks that uses standardized communication protocols to transmit data, voice, and video across the world (BasuMallick, 2023).

First and foremost is anonymity. Anonymity refers to the state of being unknown or unidentified, particularly concerning personal identity (Rodriguez, 2015). It means that a person's identity is concealed or kept private, often intentionally, to avoid being identified, traced, or targeted. The internet grants users the capability to conceal their identity amidst a vast number of other users, allowing them to mimic individuals without being easily identified. Money launderers can exploit various technologies such as virtual private networks (VPNs), anonymous browsers, and cryptocurrencies to conceal their digital traces and hide their true whereabouts (Mudditt, 2021). These tools allow them to establish numerous online identities, operate under false names, and obscure their financial records.

Another aspect is no face-to-face contact. The internet has revolutionized the way people connect and communicate, eliminating the necessity for in-person interactions (Nimma, 2022). It serves as a global platform that enables individuals to engage with others worldwide, disregarding geographical constraints and time differences. Financial institutions' servers typically rely on two elements which are login credentials and passwords for user authentication to log into an online account making it simpler for cybercriminals to conceal their true identities. If the provided information matches the data stored in the server’s memory, access would be granted. Consequently, detecting and preventing transactions associated with money laundering activities becomes more challenging.

Speed of transactions is another feature of cyber-laundering that can attract money launderers (Wronka, 2022). Conventional money-laundering practices are significantly costly and slower in comparison to modern cyber-laundering techniques. The internet empowers criminals to swiftly and covertly transfer funds or data, often with just a few clicks. This rapidity grants them the ability to carry out their illicit activities before law enforcement or security measures can effectively intervene. AI-driven payment systems have enabled the swift transfer of illicit funds, automating and optimizing financial transactions for faster processing and fund transfers. These systems utilize advanced algorithms and machine learning to analyze extensive data sets, identify patterns, and facilitate seamless transactions.

2.3 Elements of Cyber-laundering

One of the elements that cybercriminals use to conceal their identities and activities is encryption. Information is encoded using encryption so that only those with the right decryption key can decode it. Cybercriminals can make it difficult for law enforcement officials and other parties to intercept and decipher their communications by encrypting them. For example, Virtual Private Networks (VPNs) can be used to encrypt internet traffic. VPNs can make it more difficult to track or monitor the online activities of hackers. VPNs encrypt the data sent between the user’s device and the VPN server as they establish a secure tunnel.

Furthermore, cybercriminals frequently use phishing and social engineering to trick people into giving them sensitive information or granting them unauthorized access to networks. Both these techniques require persuading people to divulge private information or do activities that are advantageous to the attacker by manipulating human behavior and psychology. Phishing is a type of cyberattack where attackers pretend to be trustworthy organizations like banks, social media platforms, or online services to trick victims into thinking that is a legit website and make them disclose sensitive information like usernames, passwords, and credit card numbers (Gurav, 2023). For instance, the attacker sends an email or message that appears to be from a trusted source, often mimicking the design and branding of a well-known organization. The user is prompted to input passwords or submit personal information on a fake website that mimics the authentic website via the link or attachment. The attacker seizes the data once the user enters it, obtaining access to the victim’s accounts or personal information.

Social engineering is a tactic used by cybercriminals to trick people into providing them information or doing things they shouldn’t. It involves techniques like pretending to be someone trustworthy such as family members or friends, creating fake stories, or using psychological tricks to deceive people. One of the most famous tactics used by cybercriminals is spear phishing where a targeted phishing attack is customized for a specific individual or organization. (Bullee, 2017). To increase the likelihood of success, the attacker gathers information about the target to construct a highly personalized and convincing phishing attempt.

Next, cybercriminals use people known as ‘money mules’ to assist them in launder money gained through illicit means (Rani et al., 2023). These activities can include online scams, phishing attacks, or other forms of financial fraud. Money mules are often unaware of the fact that criminal activities are being conducted. However, their direct or indirect involvement in money laundering can have serious legal consequences, as they facilitate the movement of illegal funds (Raza et al., 2020). The entire procedure is examined, commencing with the criminals surveilling the victim's account and concluding with the money laundering and retrieval. Primarily, cybercriminals have access to the victim's account. Upon accessing the victim's account, the cybercriminal sends out recruiters to find money mules. Once money mules are recruited, the victim's money is transferred to the mules' accounts, initiating the process of money laundering. Recruiters withdraw money from ATMs using bank cards and pin codes obtained from mules when the money is available. Recruiters ultimately return the money to the criminal group while safeguarding the cybercriminal's identity. This is how these three elements could impact an auditor in combating cyber-laundering.

2.4 Process of Cyber-laundering

Placement is the beginning phase of cyber-laundering. It involves introducing the illicit fund into the legitimate financial system. This can be accomplished in several ways, including by making deposits into bank accounts, purchasing assets, and making investments in companies. The main purpose of this is to make the illegally obtained funds seem to be more legitimate and non-distinct from legally acquired funds (Zul Kepli & Nasir, 2016). For example, cyber-laundering often occurs in digital coins like Bitcoin. It can be purchased using fiat currency or other cryptocurrencies. However, online cryptocurrency trading platforms vary in their obedience to financial transaction regulation. Due to the anonymity these platforms provide, some exchanges might not enforce strong anti-money laundering (AML) legislation, which makes it easier to launder money (Zul Kepli & Nasir, 2016).

Once the funds have been successfully placed into the financial system, the next step is layering. Layering techniques often involve multiple transfers between different accounts, financial institutions, or countries which makes it difficult for authorities to detect the money trail (Zul Kepli & Nasir, 2016). The goal of this phase is to hide the source and trace of the illegal funds by constructing a complicated web of transactions. The money can spin up to ten times before entering the financial system (Zul Kepli & Nasir, 2016). Furthermore, this stage is crucial to make sure the transactions remain anonymous. For instance, the laundering of cryptocurrencies can leave digital traces that can be followed by keeping an eye on transactions on the blockchain. Conversely, it is expected that organized crime groups are currently implementing anonymization tools like the dark web to hide the source of money, making it difficult for forensic investigators to identify money laundering activities. Thus, the connections between cryptocurrency transactions are lost, making them anonymous.

The final phase of cyber-laundering involves integrating the laundered monies back into the legitimate economy and portrayed as genuine assets or income (Zul Kepli & Nasir, 2016). This can be accomplished by purchasing assets such as real estate, expensive items, or investments with layered funds. By engaging in this activity, it allows them to earn unlawful money while remaining undetected. Moreover, cyber-laundering activity is extremely difficult to differentiate between legitimate and illegitimate money (Handa & Ansari, 2022). For instance, cryptocurrencies provide criminals with an effective method to conceal the source of their income and transfer money across borders without being caught.

2.5 Risk related to Cyber-laundering

Cyber-laundering can expose auditors to various risks. The risk of cyber-laundering is significant which threatens the integrity and professionalism of the auditors. The common risks associated with cyber-laundering are reputation, regulatory, and geographical risk.

The first risk is reputation risk. This can harm the reputation of the auditors when they cannot detect any unlawful activities of cyber-laundering from a company that is commonly reported with those activities. The accuracy and integrity of financial reporting must be guaranteed by trustworthy specialists known as auditors. If auditors miss cases of cyber-laundering during their audits, they lose credibility and harm their reputations. This makes it suspicious for the audit firm as they are not able to discover any cyber-laundering activities of their client. People may make assumptions regarding the audit firm such as they might receive bribes to ensure that the company is clean and not involved with unlawful activities. This can affect their existing and potential customers or investors starting to lose confidence in their integrity in following the rules and regulations that have been set by the regulators. Thus, they expose themselves to the risk of their reputation which people may not want to use their audit services.

Secondly is regulatory risk. As cyber-laundering is still a new crime that evolves in today’s era, there are still no strong laws that are imposed to mitigate this crime. Legislation may not have caught up with the rapidly evolving techniques and technologies used by cybercriminals. This creates difficulties for auditors in detecting the non-compliance of the companies to the law and may be more difficult for auditors to determine whether businesses have implemented sufficient controls to prevent cyber-laundering in the absence of defined standards and clear regulatory requirements. It is also harder for auditors to identify and report cyber-laundering activities accurately to the board of directors and senior management. Auditors that fail to detect and prevent financial crimes, may face regulatory sanctions, fines, and legal actions.

Lastly is a geographical risk. Cyber-laundering is still a new financial crime and is not common in certain countries. Therefore, different countries have different laws, regulations, and enforcement (Rebe, 2023). Irresponsible persons may take advantage of countries that have poor or no national laws in place to detect, prevent, and terrorist financing. They will take advantage of these flaws to move their illicit fund to countries that have less strict regulations. Keeping up with the changing cyber-laundering laws in various nations or regions may be difficult for auditors. Cultural and language differences also impose challenges for auditors in conducting investigations of cyber-laundering activities. Communication barriers can hinder the effectiveness of collaboration and sharing information with the local authorities and other relevant parties. Misinterpretations and misunderstandings of the local practices by the auditors also may occur which can impact the accuracy and effectiveness of audits and lead to oversight of cyber-laundering activities (FATF, 2020).

3. Conclusion

In conclusion, cyber-laundering presents substantial difficulties for auditors in the contemporary digital era. Auditors struggle to identify and stop cyber-laundering activities as criminals take advantage of technological improvements and the complexity of the internet environment. It is now challenging for auditors to track transactions and determine the genuine source of illicit cash because of the rise of cryptocurrencies and the anonymity they offer. The usage of internet platforms, anonymizing techniques, and encryption all make it more difficult to identify fraudulent transactions. cyber-laundering has a wide range of effects on auditors. When they miss illegal activity, they run the danger of losing credibility and trust as well as their reputation. Due to the dynamic nature of cyber-laundering and the absence of well-defined standards and definite regulatory criteria, regulatory concerns exist. Because many nations have varied cyber-related laws, regulations, and enforcement procedures, auditors may also face geographical concerns.

Various recommendations can be provided to address these issues. Public awareness and education on cyber-laundering are essential to help individuals and organizations recognize and prevent such crimes. Auditors should receive proper training and continuously update their knowledge and skills to successfully detect and prevent cyber-laundering operations (Yusoff et al., 2023). Auditors must obtain the essential information and abilities to prevent cyber-laundering. Even if they are not conducting forensic audits, they must nonetheless be vigilant in spotting any indications of fraud, misrepresentation, and money laundering as part of their regular audit duties. The regulations and procedures are frequently updated and changed. Auditors should be held accountable for abiding by all regulations and protocols set by related agencies that can investigate cyber-laundering cases to take further action. Auditors can enhance their understanding of cyber-laundering mechanisms, techniques, and signs through adequate training.

The emergence of technologies such as system of rules, artificial intelligence, and cybersecurity have a positive impact on the identification of financial crimes and cyber-laundering. For numerous years, compliance and risk departments have employed a system of rules to identify transactions associated with money laundering (Labanca et.al, 2022). A system of rules is a logical construct consisting of conditions with certain thresholds that represent a risk profile. If a transaction exceeds the threshold, a deeper investigation will be carried out if it is deemed suspicious. Moreover, the capability of artificial intelligence in the financial sector with intelligent algorithms and models capable of mimicking and learning from the behavior of money launderers (Alsuwailem & Saudagar, 2020). It will help an organization to detect the presence of cyber-laundering activities. Cybersecurity, a new technology of the 4th industrial revolution, has emerged to counteract cyberlaundering. Cybersecurity establishes the essential criteria, regulations, and norms that an organization must adhere to counter and reduce the threat of cybercrime and cyber-laundering (Taherdoost, 2022). Examples of cybersecurity measures aimed at preventing cybercrime and cyber money laundering include shutting the online portal after three unsuccessful tries to log in due to a forgotten password, installing a mobile token, utilizing facial recognition technology, and requiring access confirmations through numerical codes.

In addition, collaboration between auditors, IT experts, and law enforcement organizations is essential to increasing the capacity to tackle cyber-laundering. To counter cyber-laundering and provide auditors with clear guidance, governments and regulatory agencies should adopt thorough legislation. Thus, combating cyber-laundering necessitates a multidisciplinary strategy and ongoing efforts to keep up with the development of cybercrime techniques. To effectively manage the problems posed by cyber-laundering in the digital era, auditors must adapt and strengthen their competencies. Auditors play a critical role in guaranteeing financial transparency and regulatory compliance.

Acknowledgements

Funding: This research project was supported by Universiti Teknologi MARA under Special Research Grant number 600-TNCPI 5/3/DDF (AKAUN) (004/2023)

References

Alsuwailem, A.A.S., & Saudagar, A.K.J. (2020). "Anti-money laundering systems: a systematic literature review", *Journal of Money Laundering Control, 23*(4), 833-848. https://doi.org/10.1108/JMLC-02-2020-0018

BasuMallick, C. (2023). *What Is the Internet? Meaning, Working, and Types*. Retrieved from https://www.spiceworks.com/tech/networking/articles/what-is-the-internet/

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). "Spear phishing in organizations explained", *Information and Computer Security, 25*(5), 593-613. https://doi.org/10.1108/ICS-03-2017-0009

Calafos, M. W., & Dimitoglou, G. (2022). Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency. In *Principles and Practice of Blockchains* (pp. 271-300). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-10507-4_12

Financial Action Task Force. (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*. Paris: FATF Retrieved from: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets -Red-Flag-Indi cators.pdf

Gurav, A.B. (2023). Cyber Crimes in Financial Activities, *ILE Consumer Protection Law and Review, 1*(1), 51-50. ISBN – 978-81-961120-4-2.

Handa, R. K., & Ansari, R. (2022). Cyber-laundering: An Emerging Challenge for Law Enforcement. *Journal of Victimology and Victim Justice, 5*(1), 80-99. https://doi.org/10.1177/25166069221115901

Harahap, H. H. (2020). Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang. *Jurnal Pengabdian Kepada Masyarakat*, *4*(2), 186-190. https://doi.org/10.32696/ajpkm.v4i2.551

Irina, C. (2018). Cryptocurrencies Legal Regulation. *BRICS Law Journal*, *5*(2), 128-153. https://doi.org/10.21684/2412-2343-2018-5-2-128-153

Jensen, R. I. T., & Iosifidis, A. (2023). Qualifying and raising anti-money laundering alarms with deep learning. *Expert Systems with Applications, 214*, 119037. https://doi.org/10.1016/j.eswa.2022.119037

Labanca D, Primerano L, Markland-Montgomery M, Polino M, Carminati M, & Zanero S. Amaretto. (2022). *An active learning framework for money laundering detection*. IEEE Access. 2022;10:41720-41739. https://doi.org/10.1109/ACCESS.2022.3167699

Lazic. (2023). *39 Worrying Cyber Crime Statistics*. Retrieved from https://legaljobs.io/blog/cyber-crime-statistics/

Malaysia: Number of e-commerce scams 2022. (n.d.). *Statista*. Retrieved from: https://www.statista.com/statistics/1346657/malaysia-number-of-e-commerce-scams/ #:~:text=As%20of%20May%202022%2C%20there

Nimma, S. (2022). Origin, Growth and Evolution of Money Laundering in The Cyber World. *International Journal of Creative Research Thoughts*. http://ijcrt.org/viewfull.php?&p_id=IJCRT2203525

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2023). The Trends and Challenges of Money Mule Investigation by Malaysian Enforcement Agency. *International Journal of Business and Technopreneurship, 13*(1), 37-50. https://doi.org/10.55493/5007.v13i3.4737

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role Of Money Mules in Money Laundering and Financial Crimes A Discussion Through Case Studies. *Journal of Financial Crime, 27*(3), 911-931. https://doi.org/10.1108/JFC-02-2020-0028

Rebe, N. (Ed.). (2023). *Cyber-laundering: International Policies and Practices*. World Scientific. https://books.google.com/books?hl=en&lr=&id=eGOzEAAAQBAJ&oi=fnd&pg=PR 5&dq=risk+relating+cyber+laundering+&ots=LqS81xiNRA&sig=sJ4wq42JtJUhVt bPOaewNNsJyk8

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C.A., Barbosa, J. L. V., Antuens, R.S., Scorsatto, R, & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications, 56,* 101207. https://doi.org/10.1016/j.elerap.2022.101207

Rodriguez, K. (2015). *Anonymity and Encryption*. Retrieved from https://www.ohchr.org/sites/default/files/Documents/

Rusanov, G., & Pudovochkin, Y. (2021). Money laundering in the modern crime system. *Journal of Money Laundering control, 24*(4), 860-868. https://doi.org/10.1108/JMLC-08-2020-0085

Samagaio, A., & Diogo, T. A. (2022). Effect of computer assisted audit tools on corporate sustainability. *Sustainability, 14*(2), 705. https://doi.org/10.3390/su14020705

Sampson, E. (2023). *Money-laundering criminals are adapting to new technology faster than authorities can keep up, EU report says*. Retreived from https://www.icij.org/investigations/fincen-files/money-laundering-criminals-are-adapting-to-new-technology-faster-than-authorities-can-keep-up-eu-report-says/

Samuel, O., Pelumi, I., & Fasilat, O. (2021). Effect of internal control system on fraud prevention among deposit money banks in Kwara State, Nigeria. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(1), 264-271.

Seetharaman, A., Patwa, N., & Niranjan, I. (2017). Role of Accountants and Auditors in Mitigating Digital Crimes. *Journal of Applied Economics & Business Research, 7*(1).

Taherdoost H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181

Wayo, A. (2023). *The Role of Forensic Accounting in Combating Money Laundering in Ghana* (Doctoral dissertation, Northcentral University).

Wronka, C. (2022). "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

Yusoff, Y. H., Ghazali, N. I., Maz Fazel, A. A., Jamaludin, N., Tawil, N. L., & Madzlan, N. (2023). Roles of Auditor in Combating Money Laundering: A Concept Paper. *International Journal of Academic Research in Business and Social Sciences, 13*(4). https://doi.org/10.6007/IJARBSS/v13-i4/16593

Zul Kepli, M. Y., & Nasir, M. A. (2016). Money Laundering: Analysis on the Placement methods. *Science*, *582*, 181-194.

Copyrights