International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
Volume 7, Number 2, 2026
https://ijble.com/index.php/journal/index

Digital Concealment in Money Laundering: A Technology-Neutral Approach to Aggravated Criminal Liability in Indonesia

Shendy Prasetyo[1], **Milda Istiqomah**[2], **Bambang Sugiri**[3]
Faculty of Law, Universitas Brawijaya, Malang, Indonesia[123]
Corresponding author: shendypr@student.ub.ac.id

Abstract
The misuse of digital anonymity technologies has altered the operational structure of money laundering and has created new difficulties for attribution, financial tracing, and asset recovery. Although Virtual Private Networks (VPNs) are legitimate privacy and cybersecurity tools, their deliberate use in laundering schemes may conceal digital identity, obscure transaction origins, and impede investigative reconstruction. This article examines whether Indonesian anti-money laundering law adequately addresses VPN-assisted money laundering and whether the intentional use of anonymity-enhancing technologies should operate as an aggravating circumstance. Using normative legal research, this study applies statutory, conceptual, and comparative approaches to Indonesian law and selected foreign regimes in the United States, the United Kingdom, and Singapore. The article finds that Indonesian law already criminalises money laundering committed through digital infrastructures because its substantive offences are drafted in technology-neutral terms. The central weakness is therefore not a criminalisation gap but a sentencing-differentiation gap: current law does not expressly distinguish ordinary laundering from laundering that deliberately exploits sophisticated digital concealment. The article argues that intentional technological concealment increases culpability, social harmfulness, investigative complexity, and the cost of enforcement. It therefore proposes a technology-neutral amendment to Law Number 8 of 2010 that treats the intentional misuse of VPNs and functionally equivalent anonymity-enhancing technologies as a statutory aggravating circumstance when used to obstruct identification, tracing, investigation, evidentiary processes, or asset recovery.

Keywords: Money laundering; digital concealment; virtual private network; technology-neutral regulation; aggravated criminal liability; sentencing policy; Indonesia.

DOI. https://doi.org/10.56442/ijble.v7i2.1517

INTRODUCTION

The digitalisation of financial services has transformed the architecture of money laundering. Contemporary laundering no longer depends solely on cash couriers, offshore companies, or conventional banking layers. It increasingly operates through online banking, virtual assets, encrypted communication systems, payment platforms, remote-access infrastructures, and identity-obscuring technologies. These developments increase the speed and geographical reach of laundering schemes while making attribution and asset tracing more complex (Levi & Reuter, 2006; Madinger, 2020; Teichmann, 2018; Unger, 2007).

International AML/CFT standards recognise that technological innovation produces both regulatory opportunities and vulnerabilities. The Financial Action Task Force (FATF) has encouraged jurisdictions to adopt risk-based regulation capable of addressing new technologies without suppressing legitimate innovation (FATF, 2021, 2025). The same logic is reflected in international policy documents on digital identity, virtual assets, and financial intelligence, which emphasise that privacy-enhancing technologies may support legitimate security objectives while simultaneously

complicating customer due diligence, transaction monitoring, and law-enforcement access (FATF, 2020a, 2020b; UNODC, 2023).

Within this technological environment, the Virtual Private Network (VPN) occupies an ambivalent position. On one hand, a VPN is a legitimate tool for protecting confidentiality, securing remote access, reducing exposure to hostile networks, and preserving privacy. On the other hand, because VPNs can mask Internet Protocol (IP) addresses, route traffic through remote servers, and reduce the visibility of network-origin data, they may also be deliberately used by offenders to frustrate digital attribution and investigative reconstruction (Casey, 2011; Clough, 2021; Murray, 2019). The legal issue is therefore not whether VPNs should be treated as inherently unlawful. The more precise issue is how criminal law should respond when a legitimate anonymity-enhancing technology is intentionally misused to facilitate money laundering.

Indonesian law already contains several instruments relevant to this problem. Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering establishes the substantive offences of money laundering. Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law strengthens the legal framework for electronic information and transactions. Law Number 27 of 2022 concerning Personal Data Protection recognises the legal importance of personal-data protection, while Law Number 1 of 2023 concerning the Criminal Code provides general criminal-law principles applicable to statutory offences (Republic of Indonesia, 2010, 2022, 2023, 2024).

The doctrinal problem is not that Indonesian law fails to criminalise VPN-assisted laundering. The problem is more specific: Indonesian law does not expressly differentiate between ordinary laundering and laundering carried out through deliberate technological concealment. As a result, offenders who merely transfer illicit proceeds through ordinary channels and offenders who deliberately deploy anonymity-enhancing technologies to obstruct identification, tracing, and evidence-gathering may remain subject to the same statutory sentencing range. This creates a proportionality problem because the second form of conduct involves additional planning, greater sophistication, and a stronger intention to frustrate enforcement (Arief, 2017; Ashworth, 2015; Hiariej, 2016).

Existing AML scholarship has extensively examined predicate offences, beneficial ownership, asset confiscation, financial intelligence, compliance duties, and virtual-asset risks (Alldridge, 2008; Mugarura, 2016; Ryder, 2012; Simser, 2015). Cybercrime scholarship has also analysed digital evidence, computer forensics, electronic attribution, and privacy-enhancing technologies (Brenner, 2010; Casey, 2011; Clough, 2021). However, limited attention has been given to the narrower sentencing-policy question: whether the intentional misuse of VPNs and functionally equivalent anonymity-enhancing technologies should be treated as an aggravating circumstance in money laundering cases.

This article addresses that gap. It argues that the intentional misuse of VPNs should not be criminalised as an independent offence, because such an approach would risk overcriminalising legitimate privacy and cybersecurity practices. Instead, the misuse should be treated as a technology-neutral aggravating circumstance when it is intentionally employed to conceal identity, obstruct attribution, impede financial tracing, or frustrate asset recovery. This argument preserves the legality of ordinary

VPN use while ensuring that technologically sophisticated laundering attracts proportionate criminal sanctions.

The research questions are therefore: first, does Indonesian positive law already criminalise money laundering committed through VPN-assisted digital infrastructures? Second, does the existing framework contain a normative gap in sentencing differentiation? Third, how can Indonesia formulate a technology-neutral aggravating provision that is consistent with legality, proportionality, privacy protection, and international AML/CFT standards?

METHOD

This study uses normative legal research because the principal object of analysis is the adequacy, coherence, and future development of legal norms. Normative legal research is appropriate where the inquiry concerns statutory interpretation, legal principles, doctrinal coherence, and ius constituendum proposals rather than the measurement of empirical behaviour (Marzuki, 2021).

The study applies three complementary approaches. First, the statutory approach examines Indonesian legislation on money laundering, electronic information and transactions, personal-data protection, and criminal law. Second, the conceptual approach analyses the doctrinal concepts of culpability, social harmfulness, proportionality, sentencing differentiation, digital concealment, and technology-neutral regulation. Third, the comparative approach evaluates selected foreign regimes in the United States, the United Kingdom, and Singapore. These jurisdictions were selected because they have mature AML frameworks, relatively developed sentencing or regulatory approaches, and practical relevance for assessing technology-facilitated financial crime.

The primary legal materials consist of Indonesian statutes, selected foreign statutes, sentencing materials, and international standards. The Indonesian materials include Law Number 8 of 2010, Law Number 1 of 2024, Law Number 27 of 2022, and Law Number 1 of 2023 (Republic of Indonesia, 2010, 2022, 2023, 2024). The comparative materials include 18 U.S.C. § 1956 and the United States Sentencing Guidelines, the United Kingdom's Proceeds of Crime Act 2002 and Sentencing Council guideline on money laundering, and Singapore's Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and payment-services AML/CFT framework (Monetary Authority of Singapore, 2022; Sentencing Council for England and Wales, 2014; Singapore, 1992; United Kingdom, 2002; United States Sentencing Commission, 2025). International materials include the FATF Recommendations, FATF guidance on virtual assets and digital identity, and UNODC materials on virtual assets and money laundering (FATF, 2020a, 2020b, 2021, 2025; UNODC, 2023).

The secondary materials consist of scholarly books, peer-reviewed journal articles, legal commentaries, and official reports concerning money laundering, cybercrime, sentencing theory, financial intelligence, and technology-neutral legislation. These materials are used to support conceptual interpretation and to locate the article's contribution within existing scholarship.

The materials are analysed qualitatively through descriptive, systematic, comparative, and prescriptive legal analysis. Descriptive analysis explains the existing legal framework. Systematic analysis examines the relationship between statutory

provisions and general criminal-law principles. Comparative analysis identifies relevant patterns from selected jurisdictions without assuming direct transplantation into Indonesian law. Prescriptive analysis formulates a technology-neutral ius constituendum model for aggravated liability in Indonesia's AML regime.

RESULTS AND DISCUSSION

The analysis produces three principal findings. First, Indonesian AML legislation is substantively capable of prosecuting money laundering committed through VPN-assisted digital transactions. Second, the current framework contains a normative gap in sentencing differentiation rather than a gap in criminalisation. Third, comparative materials support the view that deliberate technological sophistication and concealment may legitimately increase the seriousness of a laundering offence. These findings provide the basis for the proposed statutory reform.

1. Indonesian AML law already covers VPN-assisted money laundering

Law Number 8 of 2010 is drafted in functional terms. It criminalises acts such as placing, transferring, converting, spending, paying, granting, entrusting, carrying abroad, changing form, exchanging, concealing, or disguising assets known or reasonably suspected to constitute proceeds of crime. The statute does not confine liability to cash-based laundering or to any particular technological method. This drafting technique makes the law technology-neutral at the level of substantive criminalisation (Republic of Indonesia, 2010).

The legal consequence is important. If a person launders criminal proceeds through an online account, a virtual-asset platform, encrypted communication, or a VPN-assisted access route, the laundering conduct remains punishable because liability attaches to the act of concealing, disguising, transferring, or dealing with criminal proceeds. The VPN is not the object of criminalisation. It is part of the factual matrix by which the offender may conceal identity, location, or transaction origin.

This interpretation is strengthened by the broader Indonesian legal framework. The Electronic Information and Transactions framework recognises electronic information and electronic documents as legally relevant within Indonesian law, while the Personal Data Protection Law protects privacy interests without granting immunity for criminal conduct. The Criminal Code provides general principles relevant to culpability, proportionality, and punishment (Republic of Indonesia, 2022, 2023, 2024). These instruments enable Indonesian law to address digital evidence and electronic transactions without requiring a technology-specific money laundering offence.

Accordingly, the assumption that VPN-assisted laundering creates a total legislative vacuum is inaccurate. The current statute can already reach the laundering conduct. What remains unresolved is whether the deliberate use of anonymity-enhancing technologies should influence the severity of punishment. This distinction is essential because an overbroad focus on criminalisation could threaten legitimate privacy and cybersecurity practices, whereas a sentencing-focused approach targets only the offender's culpable misuse of technology.

2. The central defect is a sentencing-differentiation gap

Although Indonesian law criminalises VPN-assisted laundering, it does not expressly distinguish between ordinary laundering and laundering that deliberately uses anonymity-enhancing technologies to obstruct enforcement. This creates what this article calls a sentencing-differentiation gap: the statutory framework recognises

the offence but does not provide a structured mechanism for treating technologically sophisticated concealment as an aggravating factor.

Criminal-law theory supports the need for such differentiation. Proportional punishment requires attention not only to the label of the offence but also to the offender's degree of culpability, the seriousness of the conduct, and the harm or risk created by the offence (Ashworth, 2015; von Hirsch & Ashworth, 2005). In Indonesian criminal-law scholarship, similar concerns appear in discussions of sentencing policy, culpability, and the need for punishment to reflect the gravity of criminal conduct (Arief, 2017; Hiariej, 2016; Irmawanti & Alin, 2021).

The intentional misuse of VPNs is legally significant because it may demonstrate additional planning, technical capability, and a conscious effort to reduce detectability. It may also increase investigative costs by requiring more complex forensic reconstruction, cross-border requests, log analysis, and cooperation with service providers. These effects distinguish sophisticated digital concealment from ordinary laundering mechanisms. In doctrinal terms, the conduct reflects both higher culpability and greater social harmfulness.

The proposed differentiation does not punish privacy. It punishes intentional obstruction in the context of an already punishable laundering offence. A person who uses a VPN for personal security, professional confidentiality, or corporate remote access does not thereby commit an offence and should not face criminal aggravation. Aggravation should arise only when the prosecution proves that anonymity-enhancing technology was intentionally used to facilitate laundering or to obstruct identification, tracing, investigation, evidentiary processes, or asset recovery.

This approach is more defensible than creating a separate offence of VPN misuse. A standalone offence would be difficult to define without overbreadth, because VPNs have many lawful uses and are not inherently criminogenic. By contrast, an aggravating circumstance depends on the underlying money laundering offence plus proof of intentional technological concealment. It therefore preserves legality and proportionality while addressing the distinctive seriousness of technology-facilitated laundering.

3. Comparative analysis supports aggravation based on sophisticated concealment

Comparative legal materials support the proposition that sophisticated concealment may increase the seriousness of money laundering. The United States does not prohibit VPNs as such. However, federal money laundering law focuses on the concealment of the nature, location, source, ownership, or control of criminal proceeds, and the United States Sentencing Guidelines recognise 'sophisticated laundering' as a sentencing enhancement where complex or intricate conduct is used in the execution or concealment of the offence (United States, 1986; United States Sentencing Commission, 2025). This supports a conduct-based rather than technology-based model.

The United Kingdom adopts a similar approach. The Proceeds of Crime Act 2002 criminalises concealment, disguise, conversion, transfer, arrangements, acquisition, use, and possession of criminal property (United Kingdom, 2002). The Sentencing Council's guideline treats the sophisticated nature of the offence and significant planning as indicators of high culpability, and it identifies attempts to conceal or dispose of evidence as aggravating conduct (Sentencing Council for England and

Wales, 2014). The relevant factor is therefore the seriousness and sophistication of the conduct, not the intrinsic illegality of any particular technology.

Singapore also provides an instructive model. Its AML framework is supported by the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and regulatory obligations under the payment-services framework. The Monetary Authority of Singapore applies risk-based AML/CFT requirements to specified payment services, including risk assessment, mitigation, customer due diligence, and transaction monitoring (Monetary Authority of Singapore, 2022; Singapore, 1992). This confirms that emerging technologies are best addressed through risk, conduct, and function rather than through static lists of prohibited tools.

The comparative pattern is consistent. None of these jurisdictions treats VPNs or comparable anonymity-enhancing technologies as automatically unlawful. Instead, legal consequences are determined by the offender's conduct, intent, concealment strategy, and the effect on financial investigations. This pattern supports the Indonesian reform model proposed here: the law should remain technology-neutral, but sentencing should be capable of recognising intentional digital concealment as aggravating.

Table 1. Comparative treatment of sophisticated concealment in selected AML regimes

Jurisdiction	Core approach	Treatment of sophistication	Relevance for Indonesia
United States	Conduct-based AML offences and sentencing guidelines	Sophisticated laundering may increase sentencing seriousness	Supports aggravation based on intentional concealment rather than technology per se
United Kingdom	Money laundering offences under POCA 2002	Sophisticated offence/significant planning indicates high culpability	Supports culpability-based differentiation
Singapore	Risk-based AML/CFT regulation for payment services	Emerging technologies assessed by risk and function	Supports technology-neutral and adaptive drafting

4. Proposed technology-neutral legal reform

The proposed reform should be inserted into Law Number 8 of 2010 as a statutory aggravating circumstance rather than as a new independent offence. The objective is not to expand criminalisation but to improve sentencing proportionality. A technology-neutral formulation is preferable because technology-specific provisions rapidly become obsolete as offenders shift from VPNs to proxy chains, onion routing, privacy-preserving applications, decentralised networks, artificial-intelligence-assisted concealment, or future technologies not yet commercially available.

A technology-neutral provision should therefore regulate the function of concealment rather than the name of the tool. It should focus on technologies designed or used to conceal digital identity, disguise network attribution, obstruct transaction tracing, or impede investigative reconstruction. It should also require intentional use for a prohibited purpose. Without such a mens rea requirement, the provision would risk capturing ordinary privacy practices and would undermine legal certainty.

The following wording is proposed:

"Where an offence referred to in Articles 3, 4, or 5 is committed through the intentional use of technology designed or used to conceal digital identity, disguise network attribution, or obscure transaction origin, including Virtual Private Networks, proxy servers, onion routing, or any functionally equivalent technology, for the purpose of obstructing identification, tracing, investigation, evidentiary processes, or asset recovery, the maximum criminal penalty may be increased by up to one-third of the principal punishment."

This formulation has four advantages. First, it is technology-neutral because it refers to functions rather than a closed list of tools. Second, it is rights-sensitive because lawful privacy and cybersecurity uses remain outside the scope of aggravation. Third, it is proportionate because it does not create a new offence; it only increases the sentencing consequence of an existing laundering offence. Fourth, it is enforceable because prosecutors must prove intentional use for an obstructive purpose rather than merely prove the presence of a VPN connection.

For evidentiary purposes, the aggravating circumstance should be established through a combination of digital-forensic evidence, financial-transaction analysis, communication records, account-access patterns, server logs, device artefacts, and contextual indicators of concealment. The evidentiary standard should remain the ordinary criminal standard, and courts should avoid treating mere VPN use as conclusive proof of aggravation. The decisive issue is whether the technology was intentionally deployed to make laundering harder to detect, trace, investigate, or confiscate.

5. Policy implications, limitations, and future research

The proposed model has several implications for Indonesian legal policy. For legislators, it offers a narrowly tailored amendment that modernises AML sentencing without criminalising legitimate digital privacy. For prosecutors and investigators, it clarifies the kinds of facts that should be documented when technological concealment is alleged. For judges, it provides a structured basis for distinguishing ordinary laundering from sophisticated digital concealment while preserving proportionality and legal certainty.

The model also supports institutional coordination. VPN-assisted laundering may require cooperation among PPATK, investigators, prosecutors, electronic-system providers, financial institutions, and foreign counterparts. The aggravating-circumstance model encourages enforcement actors to integrate financial intelligence, digital forensics, and asset-recovery strategies rather than treating technological concealment as a purely cybercrime issue.

This study nevertheless has limitations. It is normative and doctrinal; it does not empirically examine sentencing decisions, prosecutorial files, investigative practices, or actual VPN-assisted laundering cases in Indonesia. The comparative analysis is limited to the United States, the United Kingdom, and Singapore and should not be read as a comprehensive survey of all AML regimes. In addition, the proposed wording has not been tested against real case outcomes or judicial sentencing data.

Future research should therefore examine Indonesian court decisions, prosecutor strategies, PPATK typologies, and digital-forensic practices involving anonymity-enhancing technologies. Comparative research may also be expanded to Australia, Canada, the European Union, Japan, and South Korea. Further scholarship should also explore the interaction between anonymity-enhancing technologies and crypto-mixing services, decentralised finance, privacy coins, blockchain analytics, artificial-

intelligence-assisted laundering, and emerging privacy-preserving communication protocols.

CONCLUSION

This article examined whether Indonesian law adequately addresses the intentional use of VPNs in money laundering and whether such use should justify aggravated criminal liability. The analysis shows that Indonesian law already criminalises money laundering committed through digital infrastructures because Law Number 8 of 2010 is drafted in functional and technology-neutral terms. VPN-assisted laundering is therefore not beyond the reach of existing substantive offences.

The central weakness lies in sentencing differentiation. Indonesian law does not yet expressly recognise the intentional misuse of anonymity-enhancing technologies as a factor that increases the seriousness of laundering. This gap matters because deliberate technological concealment reflects greater planning, higher culpability, increased investigative complexity, and broader social harm.

The article therefore proposes a technology-neutral aggravating provision for Law Number 8 of 2010. The proposed provision does not prohibit VPNs or criminalise privacy-enhancing technologies. It applies only where such technologies are intentionally used to obstruct identification, tracing, investigation, evidentiary processes, or asset recovery in connection with money laundering offences. This model preserves the lawful use of privacy and cybersecurity tools while enabling Indonesian AML law to respond proportionately to technologically sophisticated laundering.

The principal contribution of this study is to reframe VPN-assisted money laundering as a sentencing-policy problem rather than a criminalisation problem. By introducing the concept of normative differentiation, the article offers a doctrinally coherent and policy-sensitive framework for modernising Indonesian AML law in response to digital concealment.

Declarations

Acknowledgement: The author would like to express sincere gratitude to the supervisors for their invaluable guidance, constructive criticism, and continuous academic support throughout the completion of this research. The author also extends appreciation to the Faculty of Law for providing an academic environment that facilitated this study. Finally, heartfelt thanks are conveyed to family, colleagues, and friends for their encouragement and unwavering support during the research process.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Competing interests: The authors declare no competing interests.
Data availability: The dataset may be requested from the corresponding author subject to institutional permission and confidentiality requirements.

References

Abeysekera, I. (2014). Anti-money laundering and counter-terrorism financing strategy of financial institutions. Journal of Money Laundering Control, 17(3), 300-315.
Alldridge, P. (2008). Money laundering and globalization. Journal of Law and Society, 35(4), 437-463.
Arief, B. N. (2017). Bunga rampai kebijakan hukum pidana. Kencana.

Ashworth, A. (2015). Sentencing and criminal justice (6th ed.). Cambridge University Press.
Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.
Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.
Clough, J. (2021). Principles of cybercrime (3rd ed.). Cambridge University Press.
Egmont Group. (2021). Egmont Group operational guidance for financial intelligence units. Egmont Group.
Financial Action Task Force. (2020a). Digital identity guidance. FATF.
Financial Action Task Force. (2020b). Virtual assets red flag indicators of money laundering and terrorist financing. FATF.
Financial Action Task Force. (2021). Updated guidance for a risk-based approach: Virtual assets and virtual asset service providers. FATF.
Financial Action Task Force. (2025). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations. FATF.
Financial Crimes Enforcement Network. (2021). National AML/CFT priorities. U.S. Department of the Treasury.
Hiariej, E. O. S. (2016). Prinsip-prinsip hukum pidana. Cahaya Atma Pustaka.
Irmawanti, N. D., & Alin, F. (2021). Urgensi tujuan dan pedoman pemidanaan dalam KUHP nasional. Jurnal Hukum Pidana dan Kriminologi, 2(2), 97-114.
Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289-375.
Madinger, J. (2020). Money laundering: A guide for criminal investigators (4th ed.). CRC Press.
Marzuki, P. M. (2021). Penelitian hukum (Rev. ed.). Kencana.
Monetary Authority of Singapore. (2022). Notice PSN01: Prevention of money laundering and countering the financing of terrorism - specified payment services. MAS.
Mugarura, N. (2016). The global anti-money laundering regulatory landscape in less developed countries. Journal of Financial Crime, 23(2), 459-477.
Mugarura, N. (2017). Uncoupling the relationship between corruption and money laundering crimes. Journal of Money Laundering Control, 20(4), 343-356.
Murray, A. (2019). Information technology law: The law and society (5th ed.). Oxford University Press.
Republic of Indonesia. (2010). Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering.
Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection.
Republic of Indonesia. (2023). Law Number 1 of 2023 concerning the Criminal Code.
Republic of Indonesia. (2024). Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.
Ryder, N. (2012). Money laundering: An endless cycle? Routledge.
Sentencing Council for England and Wales. (2014). Fraud, bribery and money laundering offences: Definitive guideline. Sentencing Council.
Simser, J. (2015). Bitcoin and modern alchemy: In code we trust. Journal of Financial Crime, 22(2), 156-169.

Singapore. (1992). Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992.

Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies: A danger for Europe? Journal of Money Laundering Control, 21(4), 513-519.

Teichmann, F. M. J. (2020). Recent trends in money laundering and terrorism financing. Journal of Financial Crime, 27(3), 849-858.

Teichmann, F. M. J., & Falker, K. (2019). Cyber laundering: A threat to banking industries? Journal of Money Laundering Control, 22(2), 252-263.

Unger, B. (2007). The scale and impacts of money laundering. Edward Elgar.

United Kingdom. (2002). Proceeds of Crime Act 2002.

United Nations Office on Drugs and Crime. (2023). Manual on virtual assets and money laundering for criminal justice practitioners. United Nations.

United States. (1986). Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956-1957.

United States Sentencing Commission. (2025). Guidelines manual: §2S1.1 Laundering of monetary instruments; engaging in monetary transactions in property derived from unlawful activity. USSC.

von Hirsch, A., & Ashworth, A. (2005). Proportionate sentencing: Exploring the principles. Oxford University Press.