FIGHTING AGAINST MONEY LAUNDERING

MOH ZALI,

University of Madura (Madura, Jawa Timur, Indonesia)

ACH MAULIDI,

University of Edinburgh (Edinburgh, United Kingdom)

DOI: 10.21684/2412-2343-2018-5-3-40-63

This paper argues for the formation of a new deterrence concept which is useful for banks and state policymakers to fight against elite money laundering. The paper offers insights to enhance our understanding of the nexus of corruption, local business and money laundering scandals. These insights are synthesised from contemporary thinking and current research findings by adopting conspiracy theory. The evidence shows that fraud schemes involving corruption syndicates have become intractable, either because of influence peddling or high-profile people implicated in corruption scandals, making it difficult for anti-corruption provisions to be implemented. Therefore, it is clearly necessary to provide a cautionary note and to consider the analysis of structural forces that reveal the logic of criminal forms and conduct. The paper also points out that the establishment of money laundering laws and the creation of anti-money laundering agencies (strict law enforcement) can effectively deter predatory activities of financial intermediaries in facilitating money laundering practices. In an aggregative analysis of the underlying economic model of crime, the findings of the study provide significant support for a number of the postulates of the conspiracy theory of crime. These include the deterrence effect in respect of perpetrators such as unscrupulous local business staff, corrupters and launderers.

Keywords: deterrence concept; money laundering; corruption; law enforcement.

Recommended citation: Moh Zali & Ach Maulidi, *Fighting Against Money Laundering*, 5(3) BRICS Law Journal 40–63 (2018).

Table of Contents

Introduction

Money laundering is a method employed by criminals to disguise the origin of ill-gotten gains with the intent of enjoying their "cleansed" money without interference from predatory underworld rivals or law enforcement agencies. The nature of the relationship between the recent emergence of networks of corruption and the related problem of money laundering is little understood at present.[1] For example, Mugarura suggests that the dynamics of corruption make it a global issue given that many foreign banks may be (and may already have been) used to transmit the illicit proceeds of corruption for safe custody abroad.[2] The epistemological difficulties are the sort of evidence one uses to account for the structuring of criminal behaviour; the range of criminal behaviour that comes under the umbrella of any group of criminals; how far up the political chain one reaches in one's delineation of who the organised criminals are (in Indonesia, for example); and how valid the evidence is upon which one relies. Therefore, we propose a framework for banks and state policymakers (governments) that bridges the security, control and governance aspects of banking and information technology (IT) as well as law enforcement to

[1] Mark P. Hampton & Michael Levi, *Fast Spinning into Oblivion? Recent Developments in Money-Laundering Policies and Offshore Finance Centres*, 20(3) Third World Quarterly 645 (1999).

[2] Norman Mugarura, *The Effect of Corruption Factor in Harnessing Global Anti-Money Laundering Regimes*, 13(3) Journal of Money Laundering Control 272 (2010).

tackle organised money laundering. The application of this new concept will help in forming a strong anti-money laundering environment, and may provide a very important point of departure for strategies in the field of crime policy. Before going further, we will first give an overview of the current scandals relating to money laundering, in the context of Indonesia.

1. Background of the Study

1.1. Shell Companies

The nature of organised crime remains deeply contested terrain. Career criminal activity in Indonesia has been massive over the last two decades. All occupations present specific opportunities for criminal behaviour. For example, knowledge or contacts obtained during licit activities may be used for criminal purposes. Related to transit crime, certain occupations are a fertile breeding ground for illegal smuggling activities. Experienced criminals commonly set up a shell company (a non-trading company formed as a front for an illegal business activity), compile false financial statements, report business turnover and profit untruthfully, and then pay many different forms of taxes to cover up or conceal the source or nature of the illicit funds. Seeing the success of this conduct, naturally, their colleagues ultimately become partners in the crimes.

Most large-scale corruption cases in Indonesia involve the use of legal entities to conceal the ownership and control of corrupt proceeds. Currently, the chairman of Indonesia's House of Representative is allegedly involved in the e-KTP mega corruption scandal. The budget allocated for this electronic identity card project, resulting in state losses, was more than Rp 7 trillion (approx. US$547 million). The grid and group dimensions of certain occupations and work settings in that case cannot be denied. This is because Muhammad Nazarudin, the treasurer of the Democrat Party and a member of the parliamentary lower house, the House of Representatives, and Democrat Party chairman Anas Urbaningrum, who was widely regarded as a possible presidential candidate to replace President Yudhoyono, who must retire at the 2014 election, were said to have received 11 percent of the distributed funds (i.e. according to the indictment). In addition, those two senior politicians and government officials, two high-ranking officials from the Home Ministry, Irman and Sugiharto, have been accused at trial of embezzling funds from the mega project, resulting in state losses of Rp 2.3 trillion. This is a simple example of how public officials and their associates conceal their connection to ill-gotten funds by exploiting legal and institutional loopholes that allow opacity in the activities of companies, foundations and trust-like structures.

What is interesting in this case is that existing contacts with colleagues are also used to enter into new collaborative relations, in combination with their specific privileges, presented to them along with the ideal opportunity to embezzle public funds. One modus operandi employed in that case by the wealthy and powerful

was to use shell companies to thwart the corruption case relating to the multi-million dollar procurement of electronic identity cards (e-KTP). Shell companies are employed as a means to conceal shady business transactions, relying on exploiting anonymous companies and trusts. Thus, there is no doubt that this project could not have been undertaken without the contributions of a large number of individuals and organisations. Essentially, this type of organised crime (may) be the crime-enterprise of those minorities in Indonesia whose businesses are family matters, which should not be equated with impersonal syndicates. Among advanced industrial nations, the closest similarity to this "political coalition" organisational model occurs in Australia, where extensive narcotics, cargo theft and labour racketeering rings have been discovered, and in Japan, where gangs such as the Yakuza specialise in vice and extortion, including extortion on the part of separate groups of Sokaiya, by threatening exposure and subsequently embarrassment of large corporations at their Annual General Meetings. Both of these illustrations, however, also suggest that the coalition – in which campaign funds also play an important role – is not entirely formed by consent: business people would rather not pay blackmail if they felt they had any realistic alternative.

Mexico provides another example in the scheme by Raul Salinas, as mentioned in the report, "The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It." Salinas, the brother of former Mexican President Carlos Salinas, transferred to the United States US$100 million in questionable assets using a private banking relationship formed with Citibank. Between 1992 and 1994 Citibank assisted Salinas's transfers and effectively disguised the source and destination of the funds by employing – in this particular situation not shell companies, but rather – shelf companies (i.e. legally registered "paper companies," having no activity, assets or liabilities, registered for the purpose of being sold). Upon setting up the offshore private investment company Trocca Ltd., to hold Salinas's assets, Citibank appointed three Panamanian shelf companies – Madeline Investments S.A., Donat Investments S.A. and Hitchcock Investments S.A. – to serve as Trocca's board of directors. All three of these companies had been incorporated in 1979, nearly 15 years before Trocca's incorporation. In addition, another shelf company from the Cayman Islands, Tyler Ltd., incorporated in 1984, was named as a principal shareholder. With the help of Citibank, Salinas avoided his name being connected to the scheme by circumventing the incorporation process, and thus no documentation identified Salinas as the beneficial owner of the accounts.

In that connection, throughout Indonesia, as in many other countries of the world, the involvement of state officials in illegal activity is both ubiquitous and a matter of public knowledge. This topic is sensitive because it raises questions about the ethics of public figures (among high-ranking public officials), which is something that affects the trust people have in government and suggests that an event affecting national political priorities was the result of a secret plot by political insiders who used

their power and influence to keep their intrigues hidden. Public opinion surveys in Indonesia itself record alarmingly low levels of trust in public institutions, and the common view that corruption is all-pervasive. Indonesia's public political domain is still characterised by animated discussion of corruption and the abuse of power by public officials: this alone makes a scholarly treatment of this topic urgent and appropriate. Certainly, such crimes and the criminogenic circumstances surrounding them warrant scientific inquiry, not only to better understand elite politics but also to identify institutional vulnerabilities so that protections can be established or strengthened. In the following discussion we will deliberate on this elite political crime as well as (shell) local businesses grounded in the case of money laundering.

2. Literature Review

2.1. Money Laundering

Money laundering has been defined in a variety of ways by a variety of sources. While the definitions used by various regulators, criminal codes and law enforcement agencies are valid, they and others like them mostly focus on the criminal aspects, the accounting aspects or the illicit nature of the actions. Traditional definitions focus on the activities involved and are usually divided into three phases: (1) placement, (2) layering and (3) integration, or some variation on those themes. However, in today's modern world, the definition of money laundering needs to expand to encompass a series of actions where the money launderer conceals his actions from a perceived threat – but not from all possible lines of discovery. This means that the actions of launderers are not only to hide, but to legitimise. For example, an essential element in the process is the conversion of a wide range of illicit funds, including the proceeds from the corruption of officials, from street crime, corporate fraud, bribes and even from terror financing, into apparently legitimate income.

Today, the attraction of money laundering is profit – it is a service-oriented business where readily available knowledge can position people to make significant profit with little perceived risk. This ability – and the willingness of people to take the risk – to compensate individuals and organisations for their involvement creates a subtle encouragement for both participation and silence. According to Simser, who explores money laundering, typologies and also emerging trends and threats in Canada, money laundering may be defined as:

> A technique used by criminals to disguise the origin of ill-gotten gains with the intent of enjoying their "cleansed" money without interference from predatory underworld rivals or law enforcement.[3]

[3] Jeffrey Simser, *Money Laundering: Emerging Threats and Trends*, 16(1) Journal of Money Laundering Control 41 (2012).

In relation specifically to crime, here, for example, we have witnessed the proliferation of lightweight, expensive and enjoyable consumer products not only that we want to buy but also that are good to steal. We also seem to prefer self-service shops, albeit they create ideal conditions for shop theft.[4] We like to cross borders with minimal impedance, albeit this creates conditions that facilitate smuggling, drug trafficking and people trafficking. We enjoy the convenience of cell phones, albeit they can be used as resources for committing crimes and also comprise attractive crime targets. We like to attend concerts and major sports events, albeit they create helpful conditions for pick-pocketing and ticket-touting. We have welcomed the growth in opportunities for women to earn a living outside the home, albeit this has improved opportunities for burglars.[5] And so on. With all just elaborated in mind, money laundering in the criminal sense involves the use of illicit or criminal funds and assigns criminal liability to otherwise legitimate business practices. Therefore, the first task in defining money laundering is to understand that it is a business function.

2.2. The Case of Money Laundering and Local Businesses

Businesses are not only potential victims of a criminal offence as reported by the Association of Certified Fraud Examiners (ACFE), they may also become involved in scandalous activities, including those of organised crime, such as money laundering – local businesses are sometimes believed to be used as fronts for organised crime. Money laundering almost always involves a lot of cash, which makes it possible for organised crime to offer businesses illicit goods or services. The success of money laundering activities hinges largely on getting the dirty money into domestic pecuniary companies, for example through transfer to different accounts for deposit, or via the purchase of real estate or other tangible or intangible assets. It is true to say that the heart of the complexity of the process of money laundering favours the participation of specialists and experts in the financial markets in this type of crime. Steinko[6] and Tilley and Hopkins[7] suggest that the international laundering of money is often not done by the same individuals who engage in the criminal and illegal activities but by experts who are familiar with the workings of the international capital markets, and who are thus able to determine the risks of detection and to exploit differences in controls and regulations among countries. And that coordination and cooperation tends to occur informally and on an ad hoc basis. As a consequence,

---

4 Nick Tilley, *Crime Reduction: Responsibility, Regulation, and Research*, 11(2) Criminology & Public Policy 361 (2012).

5 Marcus Felson, *Crime and Everyday Life* (Thousand Oaks: Sage, 2002).

6 Armando F. Steinko, *Financial Channels of Money Laundering in Spain*, 52(6) British Journal of Criminology 908 (2012).

7 Nick Tilley & Matt Hopkins, *Organized Crime and Local Businesses*, 8(4) Criminology and Criminal Justice 443 (2008).

soaring markets stimulated speculative operations with legal as well as illegal money and caused huge damage to the integrity of trust companies.

The concept of the participation of financial markets specialists and experts is congruent with conspiracy theory. A core theoretical insight is that such a conspiratorial mindset is activated particularly in uncertain, fearful or threatening situations, which has been found to be attributable to people's sense of motivation. One of the ironies is that the sorts of networks involved in money laundering syndicates are always heterogeneous rather than a single phenomenon. In short, the high technical complexity of money-laundering operations – the underlying phenomenon – has remained elusive, due to a comparative criminal advantage arising from the combination of high technological skills and high motivation. People can use corporations or professions as a means to attain fraudulent ends, and they can do so either at the start (pre-planned fraud) or as an afterthought in a changing situation. In this context, those corporations can be substantive and real or mere fronts or shells for the perpetration of intentional wrongdoings. Analyses of this kind are understood as multiple-person crimes – a complex series of interrelated actions that have different degrees of importance and involvement, in which the objectives of the participants typically are motivated by profit-driven crimes. The actors within these spheres predominantly have the capacity of learning either law-abiding or law-breaking behaviour, given their differential associations with intimate groups. The response to the increasing mobility and sophistication of criminal entrepreneurs as illustrated above can be a difficult exercise. This is because some agencies do not provide any information about the methodology of organised crime (often hidden from the general public). In addition, establishing a connection to organised crime, and ranking the relative seriousness of the problem for longer-term investigation and targeting purposes, are difficult problems that rarely are addressed in a systematic fashion.

We argue that the existence of a conspiracy may make the detection of the crime of conspiracy by the authorities less probable, because of the ability of conspirators to falsify apparently independent items of evidence. In keeping with this analysis, conspiracy theories may promise to make people feel safer as a form of cheater detection, in which dangerous and untrustworthy individuals are recognised and the threat they pose is reduced or neutralised. Continuing criminal conspiracies that constitute organised crime require insiders and outsiders to connect suppliers with customers and also to protect the enterprise from law enforcement. One thing that determines what degree of success an anti-laundering legal regime in any country can achieve is the ease or otherwise with which criminals and their cohorts can open fraud-intended or laundering-intended bank accounts. If criminals can easily open accounts in their proper names or assumed names, they can very easily launder the fruits of crime through those accounts. Perpetrators of advance fee fraud, for instance, always operate under assumed names. For each scam, therefore, they need a bank account in the assumed name or in the forged name of the person (often

a purported public officer) who they present as the beneficiary of the bribe the victim of the scam has been asked to pay. Some jurisdictions have taken steps to make the opening of bank accounts and transactions or relationships with designated financial institutions a difficult process to arrange.

Identifying high-risk individuals and groups in connection with high-risk illicit markets requires an understanding of important market variables. Previous examinations of illicit markets and organised crime have made it apparent that supply, demand, regulators and competition are crucial variables to measure in order to determine markets at risk.[8] The opportunity to commit white collar crime, in the social exclusivity of the business world (which is rapidly evaporating), has expanded in response to the globalisation of commerce and financial transactions. For example, it has been found that white collar crime is indubitably an expanding criminal enterprise. And they also mention that they have repeatedly identified the major threat as money laundering, for this criminality has the potential to destabilise the world's financial markets. Basically, the operational principles of money laundering are a three-stage process that requires: first, to deposit criminal proceeds into the financial systems (placement); second, to conceal the criminal origin of the proceeds (layering); and third, to create an apparent legal origin for the criminal proceeds and then use them for personal benefit. Essentially, a person who commits a crime will initially try to prevent his actions from being noticed by the tax department, police and/or law enforcement authorities.

The deeper the "dirty" money gets into the international banking system, the more difficult it is to identify its original source. Financial criminals use "legal" tricks such as "walking" accounts, where bank officials have been instructed to move accounts to another jurisdiction at the first hint of inquiry by law enforcement. Scholars have suggested that conspiracy theories valorise the self and the in-group by allowing blame for negative outcomes to be attributed to others. Thus, they may help to uphold the image of the self and the in-group as competent and moral but as sabotaged by powerful and unscrupulous others. In this regard, conspiracy theory can be defined as explanatory beliefs, involving multiple actors who join together in secret agreement and try to achieve a hidden goal that is perceived as unlawful or malevolent. In this sense, conspiracy theories might be seen as an ironic or self-defeating manifestation of motivated social cognition – the conspiracy theory fulfils the needs of some people.

2.2.1. The Challenge of Money Laundry Deterrence

Transactional organised crimes as a global topic has been the subject of much more attention lately, especially money laundering, for academics, criminal justice agencies as well as international bodies. The major techniques promoted and employed to deal with these concerns typically consist of aggressive enforcement measures

[8] Jay S. Albanese, *Risk Assessment in Organized Crime: Developing a Market and Product-Based Model to Determine Threat Levels*, 24(3) Journal of Contemporary Criminal Justice 263 (2008).

intended for the detection, seizure and confiscation of assets, and the prosecution of the offenders. Unfortunately, these measures have not appreciably mitigated or terminated the nature of the issues related to transactional organised crime. In other words, recent endeavours to tackle the unlawful activities of perpetrators who are highly organised have been unsuccessful and imperfect because criminal networks are often exacerbated by and coalesced through significant intervention that only ostensibly tries to alleviate the cases. This might conceivably be important, in that the search for conclusive evidence of the existence of extant national criminal networks requires not simply the availability of usable data but the means with which to analyse and explore the relational links that combine to form whole networks.

Generally speaking, money laundering has grabbed the attention of an ever-widening pool of people and countries around the world. This is because of worldwide illicit conspiracies to link disparate forms of malicious activity with lower risk and greater profitability than before. From this strategic standpoint, it is very important to note that organised criminal conspiracies do not suddenly come into being. These fraudsters involve or are supported through a process of individual or group engagement in less serious types of crime before engaging in, or being recruited into, more serious types of organised criminal conduct.[9] Similarly, Rezaee and Riley stipulate that white-collar crime in a fraudulent financial statement context commonly starts with a small misstatement of earnings on quarterly financial reports that appears not to be material but ultimately grows into full-blown wrongdoing and ends in substantially misleading annual financial reporting.[10] And a large majority of individuals who get involved in serious scandals commonly come from an ingenious squad of knowledgeable fraudsters (e.g. high executives) with a set of well-designed arrangements involving fraud and considerable skill at gamesmanship.

In all conditions, laundered money – the dirty money laundered in legitimate financial systems – directly or indirectly has a high demoralising impact on the reputation of the international banking system, since banks have been one of the most important channels of money laundering in recent decades. With measures widely developing in the growing fixation with, and expansion of, crime policy and law enforcement, the organisational system's adaptability in response to exploiting vulnerabilities is essentially concerned with enhancing possible crime prevention techniques. By expanding the scope of potential precaution options with regard to many types of offences, virtual situational crime deterrence is considered to propose an efficient and cost-effective approach to various crime nuisances.[11] However, as a booming phenomenon in which certain aspects frequently go unobserved, studies

---

[9] Michel Marcus, *Faces of Justice and Poverty in the City* (Paris: European Forum for Urban Security, 1995).

[10] Zabihollah Rezaee & Richard Riley, *Financial Statement Fraud: Prevention and Detection* (2nd ed., Hoboken: Wiley, 2010).

[11] Patricia L. Brantingham & Paul J. Brantingham, *Criminality of Place: Crime Generators and Crime Attractors*, 3(3) European Journal of Criminal Policy and Research 5 (1995).

associated with money laundering still remain ineptly constrained, and these veins are considered to be exceedingly vexing problems.

Here, the search for the concepts of this organised crime is made particularly difficult by a set of unscrupulous groups that employs intelligence processes to attain an inappropriate level of anonymity and non-transparency in the execution of financial transactions. In the case of organised crime, the dark figure is of exceptional concern, because many forms of organised offences in high-risk activities, such as money laundering, are so-called consensual crimes. Indeed, there is fairly widespread agreement that organised crime groups have a well-structured hierarchy, with leaders or bosses and followers in some order of rank and authority. Of course, the members of this group engage in conspiracies to carry out crimes; the structure of these groups is amorphous, free floating and flat, and thus lacking in a rigid hierarchy. However, Cuéllar interestingly notes:

> [T]he fight against money laundering is designed not just to punish a few people who happen to get caught with money after committing a crime, but to punish instead the larger infrastructure that allows domestic and global criminal networks to profit from and finance crime.[12]

More broadly, anti-money laundering regulations are held to be the key to preserving the integrity and stability of the financial system, given the amount of money being laundered.[13] But a prime question in all these cases concerns the propriety and practicality of holding responsible those creating the conditions with overall adverse unintended consequences because of the patterned choices they facilitate. Therefore, the ongoing effort applied towards preventing, investigating and detecting money laundering occurs in a typically undisclosed manner. It is important that steps be taken at an early stage to obstruct the path of this criminal act and to prevent an individual from becoming a chronic offender, all of which should be prioritised. For this to be possible it is necessary early on to be able to predict which types of feasible opportunities show a high risk, because the application of preventative techniques in relation to organised crime activity is typically complex, multifaceted and extensive, but inherently it depends on various characteristics directly and indirectly facilitating each stage of the money laundering process.[14]

Furthermore, the most widespread scheme to launder money is to make use of pecuniary institutions (banks, financial services companies and networks of business

---

[12] Mariano-Florentino Cuéllar, *The Tenuous Relationships Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93(2/3) Journal of Criminal Law & Criminology 311, 324 (2003).

[13] Jackie Johnson & Y.C. Desmond Lim, *Money Laundering: Has the Financial Action Task Force Made a Difference?*, 10(1) Journal of Financial Crime 7 (2002).

[14] Nicholas Gilmour, *Preventing Money Laundering: A Test of Situational Crime Prevention Theory*, 19(4) Journal of Money Laundering Control 376 (2016).

advisers). Those institutions offer multiple services that (may) facilitate launderers in perpetrating wrongful activities. For example, one stage in the laundering of proceeds of crime is currency smuggling, meaning that launderers illegitimately transfer a large amount of money, in surreptitious proceeds, to another country or territory. This cross-border crime is generally applied to describe a group of individuals who proceed together on a long-term basis to perpetrate serious offences for (financial) gain. In addition, archetypal crime syndicates often associated with money laundering are best viewed as a set of shifting coalitions between groups of offenders. According to the International Monetary Fund, their illicit activities will likely have harmful consequences for a country's financial stability and macroeconomic performance, such as welfare losses, draining resources from more productive economic activities and even a destabilising spillover effect on the economies of other countries.

With regard to these challenges, if crime prevention is not to be taken seriously at a local or national level, then attention needs to be directed at those conditions creating crime opportunities. The formulation of effective opportunity-reducing policies ordinarily will require analytic resources to identify persistent concentrations and to work through the conditions giving rise to them. Eck and Eck[15] provide a comprehensive overview of the central arguments and literature that underpin the call to policymakers to focus more crime control efforts on the places, not on the people, generating most crime problems. This finding is supported by Mazerolle and Ransley that policymakers should redirect crime control policies to focus less on offender-centric initiatives and more on place-centric strategies.[16] Tilley, however, expresses some doubts.[17] He illustrates that architects do not start fires or earthquakes, toy manufacturers do not choke children, and food manufacturers do not intend to cultivate botulism; yet each is regulated in ways that encourage them to internalise known risks.

2.3. Corruption: Additional Element of Money Laundering

Corruption and money laundering are fundamentally linked. They have the potential to bring catastrophic harm to economic development, and are generally perpetrated for the purpose of obtaining private gain. Corruption is viewed as a cause, and also as a predicate offence, of money laundering offences. Either the laundered assets are proceeds relating to corruption or the process of laundering is facilitated by corrupting law enforcement agencies or officials in the financial institutions to place illicit proceeds into the system.[18] Money laundering is the process

---

[15] John E. Eck & Emily B. Eck, *Overview of Crime Place and Pollution: Expanding Crime Reduction Options Through a Regulatory Approach*, 11(2) Criminology & Public Policy 279 (2012).

[16] Lorraine Mazerolle & Janet Ransley, *Crime, Place, and Pollution*, 11(2) Criminology & Public Policy 335 (2012).

[17] Tilley 2012.

[18] Charles Goredema, *Money Laundering in Southern Africa Incidence, Magnitude and Prospects for Its Control*, 92(1) Institute for Security Studies 1 (2004).

of concealing illicit gains that were generated from criminal activity: by successfully laundering the proceeds of a corruption offence, the illicit gains may be enjoyed without fear of being confiscated. Combating money laundering is the cornerstone of the broader agenda to fight organised and serious crime by depriving criminals of ill-gotten gains and by prosecuting those who assist in the laundering of such ill-gotten gains. The Financial Action Task Force (FATF) recognises the link between corruption and money laundering, including how the Anti-Money Laundering and Counter Terrorism Financing (AML/CFT) measures help combat corruption.

Criminals, to achieve their nefarious objectives, employ various methods to disguise the identity of their ill-gotten money. Using people to transfer drugs or money has been a long-standing practice by criminals. However, it is now on the rise and being replicated in a high-tech crime environment. In addition, in an interconnected world and amid rapid changes in the technology paradigm, the smallest of breaches can snowball and be exploited for ulterior gains. It is a dichotomy that while digitalisation is a tool for democratisation, it has also been used as a weapon to undertake large-scale money laundering. FATF has long understood the risks that corrupt politically exposed persons (PEPs) pose to the financial system. As explained in the FATF 2003–2004 Annual Report:

> [T]he sources for the funds that a PEP may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds but also may be embezzlement or outright theft of State assets or funds from political parties and unions, as well as tax fraud. Indeed in certain cases, a PEP may be directly implicated in other types of illegal activities such as organised crime or narcotics trafficking. PEPs that come from countries or regions where corruption is endemic, organised and systemic seem to present the greatest potential risk; however, it should be noted that corrupt or dishonest PEPs can be found in almost any country.[19]

Unfortunately, banks too often fail to make the proper checks on suspect clients or funds and regulators do not punish them for these failures. Without this form of complicity from the international system, crime and corruption of this kind would be much harder to get away with. As such, business relationships with PEPs may lead to increased risks due to the possibility that PEPs may misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of family and close associates. These individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as the result of abuse of their official position; and PEPs' families and close associates have sometimes been

[19] FATF, Report on Money Laundering Typologies 2003–2004 (2004), at 19 (Sep. 3, 2018), available at http://www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf.

found to benefit from corruption themselves. PEPs may also seek to use their power and influence to gain representation and/or access to, or control of, legal entities for similar purposes.

Those avenues are congruent with conspiracy theories as illustrated by Räikkä[20] and Coady[21] that the prevalence of conspiracy theories sometimes have reference to a truly global or mega-conspiracy. Some theorise that with intellectually respectable corrupt PEPs (real criminal conspiracies) they can conceal their conspiratorial machinations. On this point, it signifies that the perpetrators of corruption-related offences, in order to launder the proceeds of corruption smoothly, create corporate crime, business crime, political crime and government crime.[22] These concepts do not mean that the overall category of white-collar crime is composed of an accidental collection of unrelated offences; meaning that the rubric of white-collar crime encompasses a wide range of illicit behaviour.

This standpoint reflects sustained attention to some of the problems that arguably attend the vulnerabilities leading to an increased risk of corruption-related money laundering. The conspiracy approach here has proved to explain a hereditary component in money laundering. The nexus between corruption and money laundering has manifested itself in the form of tax evasion, the looming threat of currency counterfeiting and the swindling of government funds often at the expense of government development programmes. There is a close connection between corruption and the concomitant growth of financial crimes such as money laundering.[23] In many cases where money launderers cannot achieve their aims through the use or threat of the use of violence, corruption will be one of the best alternatives.[24]

2.4. Framework in Preventing Money Laundering

There are numerous international efforts being made to combat money laundering, particularly the recommendations of the Financial Action Task Force, and many countries around the globe have established Anti-Money Laundering and Counter Terrorism Financing laws and regulations. But organised money laundering is still difficult to terminate.

In this section, banks are viewed as a key component in the fight against financial crime, and we will present the best possible precautions to be undertaken in order to tackle the problem.

---

20 Juha Räikkä, *On Political Conspiracy Theories*, 17(2) Journal of Political Philosophy 185 (2009).

21 David Coady, *Conspiracy Theories and Official Stories*, 17(2) International Journal of Applied Philosophy 197 (2003).

22 Marshall B. Clinard & Peter C. Yeager, *Corporate Crime*, 9(3) Journal of Criminal Justice 253 (1980).

23 Susan Rose-Ackerman, *Corruption and Government: Causes, Consequences, and Reform* (Cambridge: Cambridge University Press, 1999).

24 Mugarura 2010.

2.4.1. The Need for IT Controls of an Organisation

One method of getting money into the banking system that is more sophisticated and subtle than smurfing is to provide a rationale or cover for its existence as cash. Money launderers may use a legitimate business as a front, or they may use shell companies, often chartered in another country.[25] In accordance with the current modus operandi, combating money laundering may be fully aligned with the overall safety and soundness of the banking system and with the primary objective of banking supervision. As a result, banks must be obliged to have adequate plans of what to do in particular situations that have been agreed officially by a group of people or a business organisation, and processes, including strict customer and/or colleague due diligence rules to promote high ethical and professional standards in the banking sector and prevent the bank from being employed, intentionally or unintentionally, for criminal activities. Control Objectives for Information and Related Technologies (initially well known as COBIT) provide a determination of process capability in monitoring the activities of technical teams to maintain IT governance. The standardisation of IT-based processes is likely to advance reliability, predictability, agility and boost flexibility in software development and/or computer systems[26] in the same way that the management of technology resources allied to corporate strategy found support in maturity models that arose from the necessity to incorporate IT in corporate governance.

The COBIT framework was formed at the end of the 1990s by the IT Governance Institute.[27] Its objective is associated with the control of IT management rather than its execution, with the most important features providing strategic alignment of IT to business in order to maximise returns, ensuring that IT resources are used sparingly and that risks associated with IT are mitigated.[28] This practice, which also helps in handling system risks by continuously guaranteeing security and offering services, and monitoring as well as managing financial record-keeping deeds and IT performance on a regular basis, is done to improve the quality of products and services, the suitability of resource use and investments, and compliance with organisational governance requirements. These points can benefit from management emphasising that information about the significant amount of comprehensive manual checks and judgmental bias should be considered the main focus in dealing with money laundering. In this context, the banks should undertake review or screening at

[25] U.S. Congress, Office of Technology Assessment, Information Technologies for Control of Money Laundering, OTA-ITC-630 (September 1995) (Sep. 5, 2018), available at https://www.princeton.edu/~ota/disk1/1995/9529/9529.PDF.

[26] Roger S. Debreceny & Glen L. Gray, *IT Governance and Process Maturity: A Multinational Field Study*, 27(1) Journal of Information Systems 157 (2013).

[27] Marcia C. Machado et al., *Sustainability in Information Technology: An Analysis of the Aspects Considered in the Model Cobit*, 14(1) Journal of Information Systems and Technology Management 88 (2017).

[28] *Id.*

the transaction level, account level, customer level and industry/peer group level. Anomalous indicators revealed through these examinations are then manually verified, first by the front-end squads and subsequently by the compliance workforce, to look into and specify their veracity. Any transaction assessed as suspicious must be reported to regulators through a suspicious activity report as formed in those banks.

It broadly can be accepted that, because (potential) launderers commonly use the banking sector to conceal the proceeds of illicit acts, customer profiling might be one of the possible ways to know as well as assess the anomalous signs of money laundering. It is one way to construct customer profiles (explicit knowledge) to help authorities make design decisions concerning effective fraud management. Customer profiling methods constitute a special class of checking because they present specific potential patterns that may provide trigger alarms. One approach to building a system of deception detection is to classify individual transactions in comparison with the legitimacy of the business and the source of money. The discovery of unusual transactional behaviour could contain indications of fraud. The assessment here primarily focuses on cash and cross-border transactions which have identified vulnerabilities and red flag indications.

2.4.2. The Effectiveness of Law Enforcement Agencies' Approach to Money Laundering Control

The main difficulty facing law enforcement agencies is that regulators are not acquainted with many of the characteristics of the businesses whose cooperation they depend upon for effective regulation of money laundering activity. In the anti-money laundering literature, the fundamental problem for effective anti-money laundering regulation, according to Araujo, is to design a system of procedures and incentives that induce the agent, that is, the financial institution, to act effectively with regard to the production of the information required by the principal, that is, the competent authority.[29] Most large-scale money laundering control measures are intended to be multi-agency endeavours, because money laundering is frequently masked by legal business transactions and those who carry out money laundering offences often have professional expertise and knowledge. Furthermore, they also make use of their aptitude not only to perpetrate money laundering but also to cover up any evidence of the misdeed. Law enforcement agencies should strongly encourage increased emphasis on the comprehensive collection, analysis and sharing of information, especially illegitimate sources and unlawful application of illicit gains which is concealed or disguised to make the gains appear legitimate.

Moreover, in response to terrorist financing, governments have to ensure that there are effective mechanisms in place that enable cross-border agencies and departments,

[29] Ricardo A. Araujo, *Assessing the Efficiency of the Anti-Money Laundering Regulation: An Incentive-Based Approach*, 11(1) Journal of Money Laundering Control 67 (2008).

concerning the deterrence of money laundering and misuse of financial systems, to cooperate and coordinate domestically so as to identify targets for investigation of money laundering and other financial crimes. When undertaking an evaluation of suspicions that offences have occurred in respect of certain subjects, accounts and transactions, the competent authorities should be able to have access to all necessary information and documents, and employ a wide range of investigative techniques (e.g. electronic interception of conversations through telephone wiretap). Also, the use of a broader set of red flags in their predictive cues drives data acquisition. In addition, the efficacy of a systematic prediction model adopted by law enforcement officials and analysts merely summarises and helps to perform numerous tests relating to the anomalies. After investigating and testing the significant suspicious transactions, each set of results can later be used as a cross-reference tool and lead to the discovery of hidden relationships in databases. In this context, an artificial intelligence technology that has powerful pattern recognition capabilities and acts on the database by detecting an existing, hidden and underlying trend should be prudently acknowledged. These efforts can then be considered to be sophisticated data mining (data-driven fraud techniques).

Sometimes, suspect wire transfers are effectively hidden by the huge volume of legitimate transfers, and due to the lack of a strong compliance ethic the creation of an audit trail that would allow law enforcement agents to track large cash transactions, which might be a powerful tool in assisting in anti-money laundering operations, is difficult to discover. These strategies tend to focus on the flow of illegal transactions by integrating and analysing information from a wide range of multiple databases to relate and link disparate bits of data and thereby reveal relationships or patterns that are, or may be, indicative of illegal monetary activities. In these ways, a variety of clues which are obtained by the competent authorities that investigate criminal activities surrounding money laundering is valuable not just to the government ministries and agencies, but also to the financial regulators and other government bodies. Presently, it is openly recognised that initiatives to deal with money laundering and terrorist financing will be more effective and sophisticated if cooperation among institutions is truly built up – government authorities as well as the reporting agencies have to take steps on a combined and coordinated approach in the overall fight against dirty money and the discovery of terrorist financing.

2.4.3. Severity of Punishment

To begin with, obedience to a piece of legislation relies heavily on the expected penalty facing violators – compliance with laws and regulations is not taken for granted, and public and private resources must be adequately spent in order both to prevent offences and to apprehend offenders. Generally, a person's decision to participate in illegal activities can be viewed as motivated by the costs and gains from such activities. For those concerned with the economic theory of offence,

one set of experiments is particularly interesting. In those experiments, children were warned not to play with a very desirable toy – otherwise they would face punishment. One group faced strong admonishment if they broke the rules and the other group faced only a light scolding if they broke the rules. The children were then permitted to play for some time in a room containing the toy. Several weeks later the children were again put in the room with the toy, only this time the threat of punishment was withdrawn. Those who had been threatened with the more severe punishment proved more likely to play with the forbidden toy than those threatened with mild punishment.[30] However, Bailey and Smith pointed out that regulatory enforcers should focus more on increasing the severity of punishment than on increasing the probability of detection.[31] This is good news for regulators facing a limited enforcement budget, as the cost of imposing (monetary) punishment is typically less than the cost of catching violators. Consequently, an increase in the severity of the punishment raises the likelihood that an offender will be discovered and convicted, and the nature and extent of punishment differ greatly from person to person and activity to activity.

Furthermore, deterring criminal activities or wrongdoings basically depends on the probability of the sanctioning strategies and penalties imposed on financial institutions which do not comply with reporting requirements. Along with criminal sanctions it is pertinent to note that,

> Some persons become "criminals," therefore, not because their basic motivation differs from that of other persons, but because their benefits and costs differ.[32]

It is openly acknowledged that a legitimate rationale for the existence of governments is to procure for the citizenry the safety and security of their persons and possessions, including the economic and political stability of states themselves. Unfortunately, governments are never fully successful in this regard. A central result of Becker's theoretical formulation is that an increase in the probability and/or severity of punishment (representing the costs of criminal behaviour) will reduce the potential criminal's participation in illegitimate activities. Deterrence theory, as mentioned by Bailey and Smith pointed out the importance of the severity, certainty and celerity aspects of punishment.[33] Typically, however, only the severity feature has

---

30 William T. Dickens, *Crime and Punishment Again: The Economic Approach with a Psychological Twist*, 30(1) Journal of Public Economics 97 (1986).

31 William C. Bailey & Ronald W. Smith, *Punishment: Its Severity and Certainty*, 63(4) Journal of Criminal Law and Criminology 530 (1973)

32 Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76(2) Journal of Political Economy 1, 9 (1968).

33 Bailey & Smith 1973.

been examined, and usually merely quite narrowly.[34] To prevent malicious crime from disturbing economic and financial stability, hence, criminal law must accentuate the penalties to persuade companies to comply with the law. Punishment that is too severe is unjust, and punishment that is not severe enough will not deter criminals from perpetrating crimes. In other words, along with increases in the severity of punishment, governments and competent authorities have to make sure that punishment actually takes place whenever a criminal act is committed and discovered.

2.4.4. Customer Due Diligence (CDD)

This aspect is most closely associated with the fight against money-laundering, which is essentially the province of the cornerstone of suggested internal controls for banks. Some believe that U.S. banks are required to generate and keep records on their customers. This is necessary to ensure that the financial system is not exploited to transmit the criminal proceeds from crimes. In addition, financial institutions are asked to make reasonable efforts and determine the true identities of all customers requesting their services – expanding current regulations by requiring financial institutions to identify the beneficial owners of legal entity customer accounts. In this regard, in Indonesia financial institutions would work closely with Indonesian government agencies to detect and prevent money laundering.

Along this line of thought, four critical minimum areas of customer due diligence measures for financial institutions have been pointed out: (1) Identifying and verifying the identity of customers; (2) Identifying and verifying the identity of beneficial owners of legal entity customers; (3) Understanding the nature and purpose of customer relationships; and (4) Conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

Additionally, monetary institutions are required to regularly supervise accounts and update beneficial ownership information on a jeopardy basis.

With regard to CDD, in 2001 the Basel Committee on Banking Supervision suggested that all banks and other financial institutions providing service of transferring money should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements." And they put the implementation of adequate due diligence on new clients and existing clients as the key part of banking control policies. Specifically, the Basel Committee requires banks to espouse apparent recognition policies on high-risk customers, and to impose stricter due diligence measures on them. In relation to new client credentials, the Basel Committee requires that banks and other financial institutions must obtain satisfactory information about each customer's identity

[34] George Antunes & A. Lee Hunt, *Impact of Certainty and Severity of Punishment on Levels of Crime in American States: An Extended Analysis*, 64(4) Journal of Criminal Law & Criminology 486 (1974).

and the purpose of the client's transactions. The sufficiency and quality of customer information depend on which categories (enterprise or individual) of accounts the new customer plans to apply for and the anticipated amount of money in the accounts.[35] As a result, the inadequacy or absence of CDD standards can subject banks to severe repercussions, including legal, operational, reputational and concentration risks, any one of which can result in serious monetary costs to the banks.

When an account has been activated, if the problem of authentication arises in the banking connection which cannot be determined, the bank must lock the account and give back the monies to the source from which they were received. The need for taking special care when dealing with a method of operating anonymous accounts can be a sufficient measure for recording information about the customer or the customer's beneficial owner. This is necessary for data processing and building databases on customer profiles. The primary purpose of this is to safeguard financial institutions from being exploited by criminals as avenues through which to perpetuate financial crimes such as money laundering and tax evasion. In this same regard, to ensure that information remains up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially or when there is a material change in the way that the account is operated.

2.5. Roles of Tax Examiners and Forensic Auditors

Structured misdeed groups can be located in a socioeconomic terrain that is essentially unremarkable. It is necessary to provide a cautionary note and to consider the analysis of structural forces that reveal the logic of criminal forms and activities. In the same regard, tax examiners and forensic auditors are often well placed to recognise the first symptoms of the likelihood of money laundering and tax crimes. Globally, their training and educational background allows them to become aware of mistrustful transactions. In this manner, the typical focus on sorting the available information and the awareness of tax examiners and forensic auditors of the possible implications of transactions or activities associated with money laundering and tax crimes can assist them in avoiding conclusions based on assertions or assumptions instead of based on verified facts. And the review of the extant transactions or activities can provide general support in explaining crime-analogous behaviour since money laundering is well planned and strategically executed.

When performing the audit or examining the possible transactions or activities related to money laundering and tax crimes, tax examiners and forensic auditors must acknowledge the indicators of the occurrence of money laundering. For instance,

---

[35] Tang Jun & Lishan Ai, *The International Standards of Customer Due Diligence and Chinese Practice*, 12(4) Journal of Money Laundering Control 406 (2009).

white-collar and common offenders may direct an external accountant to make contact with credit institutions for the purpose of opening accounts even though the company does not conduct any business in the country and the client does not have any clear insight into its future activities in the country. Additionally, money laundering records often involve companies, including financial institutions, that have been established in tax havens or offshore centres. Temporary transit accounts are frequently employed for funds originating overseas. These monies are then transferred as quickly as possible to the accounts of companies that are based in tax havens or offshore centres. Disclosing entities must be particularly attentive when business involving tax havens and offshore centres are involved. These indicators might be built into the initial checks that are carried out to confirm the scope of the audit and the issues to be audited. Some of these preliminary indicators can relate to tax crimes as well as to other criminal activities. When carrying out the audit of an enterprise, the auditors may also audit the individual tax affairs of the business owners. Money linked to tax crimes (e.g. by unrecorded sales) may become visible at some time in the future, for instance, through a personal loan to the company or detected in an unreported individual capital gain on the disposal of an asset acquired with questionable funds by the owner of the company.

Furthermore, tax examiners and forensic auditors should monitor economic transactions utilising cross-sectional data and report suspicious movements to the government agencies, which diagnose targets for investigations based on those reports. And the bank should carry out costly monitoring and reporting by thinking the unthinkable and be as creative as the fraudsters, as the government imposes fines on the bank if money laundering is successfully prosecuted and the bank did not report the transaction. The most important point in this regard is that all of the employees within the company should be mandated to become involved in anti-fraud education and training via a fraud awareness programme, and additionally trained in the specific certain alarm symptoms and prevention and detection methods that are pertinent to their department's functions. It is because the modus operandi of money laundering is dynamic that, unsurprisingly, both auditors and banks are sometimes reluctant to provide such negative information, which creates an agency problem. If this does happen, auditors are sanctioned for false negatives, that is, for not disclosing transactions which later substantially affect the firm's value. Thus, excessive fines may make auditors disclose more transactions as material, thereby failing to identify the truly important ones. Such general preventive (deterrent) measures primarily determine the extent to which the laws and prevailing regulations will be obeyed.

Conclusion

Money laundering is an economically significant crime. Several hundred billion U.S. dollars are washed through the financial sector in Indonesia, and money laundering facilitates crimes as harmful as drug trafficking and terrorism.

The aim of this study is to provide effective suggestions to formulate a schema for the analysis of preclusion initiatives (deterrence) for money laundering crime. The validity and limitations of existing knowledge relating to the concept are indicated. And, the necessity for a precise specification of the particular problem under study is emphasised. Money laundering indeed corrupts the financial markets and definitively erodes or even devastates the public's faith in the global financial system. Cases involving corruption schemes have become intractable, either because of influence peddling or high profile people implicated in corruption scandals, making it difficult for anti-corruption provisions to be implemented. However, a correct measure of money laundering may help to mitigate more accurately the sort of vulnerable factors, the underlying clandestine nature of illicit conduct carried out by organised and transnational criminal parties. In reality, even though a set of policies, regulations and intelligence systems are put in place, there is no effective precaution framework that can direct organisations to adhere to these policies and to efficiently employ information technology for this intention. This phenomenon in a period of enormous upheaval becomes both a practical issue and a central focus of research. Therefore, the legitimated range of responses, and the whole raft of reforms in respect of the proliferation of money laundering – aggrandising for the individual or group that carries out the conduct – must be vigorously taken into account by state policymakers (governments), practitioners and theorists as well as investment communities.

Conspiracy theory in this sense is a secret plan by a group to do something unlawful or harmful, and help people to make sense of a world containing evil forces beyond the control of individuals. This study also suggests that conspiracy theory provides an outlet for the expression of negative feelings. The likelihood of a conspiracy negates or at least modifies criminogenic circumstances secretly planned by introducing the perpetrators of conspiracies, who use impersonation, hacking, forgery or the use of co-conspirators to override the controls and force the entire system and every document or file accessible to fraud. Indeed, when more than one person agrees to engage in the criminal activity, the likelihood of the accomplishment of the crime is increased. It is pertinent to note, however, that a specific penalty may be quite efficacious as a deterrent measure in one society, yet have little effectiveness in another. In addition to postulating rational behaviour on the part of the potential criminal, the conspiracy theory of crime incorporates the notion of rational, maximising behaviour on the part of the potential victims of crime. Thus, establishing a connection to organised crime allows offenders potentially to have a rich source of information about crime but, unfortunately, comparatively few

are caught. Certainly, such crimes and the criminogenic circumstances surrounding them warrant scientific inquiry, not only to better understand elite illicit networks, but also to identify institutional vulnerabilities which might be caused by systemic weaknesses and institutional rivalries, so that protections can be established or strengthened. In addition, the creation of a serious anti-money laundering effort requires the state to re-examine the interconnection of government, citizens and local businesses. Government may need to redesign public programmes, overhaul the public administration and the operation of the cross-border-transaction systems and become more open to outside scrutiny and input from citizens.

Because conspiracy theories in this sense are aimed at shaping a public problem, the proposed model here also is to explore theoretically the agency problem between the bank and government law enforcement agencies closely following the observed reporting setup. The bank monitors transactions and reports suspicious activity to the government, which identifies targets for investigation based on these reports. The bank undertakes costly monitoring and reporting because the government imposes fines on the bank if money laundering is successfully prosecuted and the bank did not report the transactions. Because illicit opportunistic trigger is a dynamic variable, another theme that recurs in the discussion of combating corruption and other forms of illegality such as money laundering is the transition from clientelism to the citizenship approach. Even though one of the biggest challenges in combating international crime we face is the very nature of its global reach, neither certainty nor severity of formal sanctions is an important deterrent to crime, but that informal sanctions, socialisation and moral considerations are key determinants of criminal activity. Furthermore, in spite of the diversity of conspiratorial activities defined as illegal, any violation of the law can be conceived of as yielding an increase in the offender's pecuniary wealth, in the pecuniary equivalent of his psych wealth, or in both. These well-established offenders, of course, have linkages with local businesses, which could act as camouflage for criminal activity and provide cover for organised crime.

These illegal activities are widespread and involve such sizeable sums that they pose a threat to the stability of the global system of finance and even to the global trading system.

References

Albanese J.S. *Risk Assessment in Organized Crime: Developing a Market and Product-Based Model to Determine Threat Levels*, 24(3) Journal of Contemporary Criminal Justice 263 (2008).

Antunes G. & Hunt A.L. *Impact of Certainty and Severity of Punishment on Levels of Crime in American States: An Extended Analysis*, 64(4) Journal of Criminal Law & Criminology 486 (1974).

Araujo R.A. *Assessing the Efficiency of the Anti-Money Laundering Regulation: An Incentive-Based Approach*, 11(1) Journal of Money Laundering Control 67 (2008).

Bailey W.C. & Smith R.W. *Punishment: Its Severity and Certainty*, 63(4) Journal of Criminal Law and Criminology 530 (1973).

Becker G.S. *Crime and Punishment: An Economic Approach*, 76(2) Journal of Political Economy 1 (1968).

Brantingham P.L. & Brantingham P.J. *Criminality of Place: Crime Generators and Crime Attractors*, 3(3) European Journal of Criminal Policy and Research 5 (1995).

Clinard M.B. & Yeager P.C. *Corporate Crime*, 9(3) Journal of Criminal Justice 253 (1980).

Coady D. *Conspiracy Theories and Official Stories*, 17(2) International Journal of Applied Philosophy 197 (2003).

Cuéllar M.-F. *The Tenuous Relationships Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93(2/3) Journal of Criminal Law & Criminology 311 (2003).

Debreceny R.S. & Gray G.L. *IT Governance and Process Maturity: A Multinational Field Study*, 27(1) Journal of Information Systems 157 (2013).

Dickens W.T. *Crime and Punishment Again: The Economic Approach with a Psychological Twist*, 30(1) Journal of Public Economics 97 (1986).

Eck J.E. & Eck E.B. *Overview of Crime Place and Pollution: Expanding Crime Reduction Options Through a Regulatory Approach*, 11(2) Criminology & Public Policy 279 (2012).

Felson M. *Crime and Everyday Life* (Thousand Oaks: Sage, 2002).

Gilmour N. *Preventing Money Laundering: A Test of Situational Crime Prevention Theory*, 19(4) Journal of Money Laundering Control 376 (2016).

Goredema C. *Money Laundering in Southern Africa Incidence, Magnitude and Prospects for Its Control*, 92(1) Institute for Security Studies 1 (2004).

Hampton M.P. & Levi M. *Fast Spinning into Oblivion? Recent Developments in Money-Laundering Policies and Offshore Finance Centres*, 20(3) Third World Quarterly 645 (1999).

Johnson J. & Lim Y.C.D. *Money Laundering: Has the Financial Action Task Force Made a Difference?*, 10(1) Journal of Financial Crime 7 (2002).

Jun T. & Ai L. *The International Standards of Customer Due Diligence and Chinese Practice*, 12(4) Journal of Money Laundering Control 406 (2009).

Machado M.C. et al. *Sustainability in Information Technology: An Analysis of the Aspects Considered in the Model Cobit*, 14(1) Journal of Information Systems and Technology Management 88 (2017).

Marcus M. *Faces of Justice and Poverty in the City* (Paris: European Forum for Urban Security, 1995).

Mazerolle L. & Ransley J. *Crime, Place, and Pollution*, 11(2) Criminology & Public Policy 335 (2012).

Mugarura N. *The Effect of Corruption Factor in Harnessing Global Anti-Money Laundering Regimes*, 13(3) Journal of Money Laundering Control 272 (2010).

Räikkä J. *On Political Conspiracy Theories*, 17(2) Journal of Political Philosophy 185 (2009).

Rezaee Z. & Riley R. *Financial Statement Fraud: Prevention and Detection* (2nd ed., Hoboken: Wiley, 2010).

Rose-Ackerman S. *Corruption and Government: Causes, Consequences, and Reform* (Cambridge: Cambridge University Press, 1999).

Simser J. *Money Laundering: Emerging Threats and Trends*, 16(1) Journal of Money Laundering Control 41 (2012).

Steinko A.F. *Financial Channels of Money Laundering in Spain*, 52(6) British Journal of Criminology 908 (2012).

Tilley N. & Hopkins M. *Organized Crime and Local Businesses*, 8(4) Criminology and Criminal Justice 443 (2008).

Tilley N. *Crime Reduction: Responsibility, Regulation, and Research*, 11(2) Criminology & Public Policy 361 (2012).

Information about the authors

Moh Zali (Madura, Jawa Timur, Indonesia) – Senior Lecturer and Researcher, University of Madura (Jl. Panglegur No. 5, Tlanakan, Kabupaten Pamekasan, East Java, 69317, Indonesia; e-mail: moh.zali.unira@gmail.com).

Ach Maulidi (Edinburgh, United Kingdom) – Researcher, Association of Certified Fraud Examiners – Indonesia Chapter, Business School, University of Edinburgh (29 Buccleuch Pl, Edinburgh EH8 9JS, United Kingdom; e-mail: s1779047@sms.ed.ac.uk).