Role of Law Enforcement to prevent Cyber laundering and Asset Recovery from Overseas

by Eddy Rifai

Submission date: 12-Dec-2022 08:11AM (UTC+0700)
Submission ID: 1978428200
File name: Role_of_Law_Enforcemen.pdf (422.43K)
Word count: 6884
Character count: 39530

International Journal of Cyber Criminology
Vol 16 Issue 1 January – June 2022

Role of Law Enforcement to prevent Cyber laundering and Asset Recovery from Overseas

Eddy Rifai[1]*, H.S. Tisnanta[2]
University of Lampung

Abstract

The research investigates the role of law enforcement in the recovery of assets from cyber laundering offenses committed overseas. The study takes a normative legal approach. According to the survey findings, dealing with cyber laundering offenses whose earnings are deposited overseas necessitates the collaborative efforts of many agencies, including the PPATK, Police, Attorney General's Office, KPK, and the Ministry of Law and Human Rights. In addition, collaboration between agencies (agent to agent) and Mutual Legal Assistance refer to the Law of the Republic of Indonesia No. 1 of 2006 on Mutual Assistance in Criminal Matters and the Law of the Republic of Indonesia No. 7 of 2006 on Ratification of the United Nations Convention Against Corruption (United Nations Convention Against Corruption). Law enforcement against the Crime of Money Laundering (TPPU) continue to face challenges in both substantive law (material law) and procedural law (ceremonial law), as outlined in the Money Laundering Law. The restrictions in issue are those relating to establishing the predicate crime, and the regulations governing reverse proof and its implications have not been controlled. In reality, the aforementioned requirements are troubling and must be rectified soon in order to provide legal clarity.

Keywords: Law enforcement; asset recovery; money laundering criminal

Introduction

The cybercrime arena has widened as a global plague since the increased use of Internet and the overdependence of all commercial activity on the Internet (Chawki, 2022; Zagaris, 2022). As an estimate, approximately 40% of the world population (2.5 billion) use the Internet, and another 1.5 billion people will get access to the internet over the next four years (Goni, 2022). The number of connected devices with the Internet has tripled from 13.4 billion in 2015 to 38.5 billion in 2020. Such illegal financial activities, conventionally known as money laundering and bank frauds, are now termed as cyber laundering, a kind of mechanism in which the Internet is used to launder illegal money into 'clean' money (Richet, 2013).

[1] Faculty of Law, University of Lampung. Email: eddy.rifai@fh.unila.ac.id
[2] Faculty of Law, University of Lampung.

Money laundering now thus appears in a new garb of cyber laundering, an attempt by cybercriminals to bye-pass laws and evade the law enforcement agencies (Şcheau & Zaharie, 2017). The Internet is responsible for the birth of this this new breed of crime. Cyber criminals make use of several avenues to commit cyber laundering, including online banking, e-gambling, online auctioning, cryptocurrency, and digital payments methods (Chawki, 2022; Mabunda, 2018). Various new and evolving technologies have provided complete anonymity to cyber criminals, which further increased their crime events and made it possible to disguise their illicit and unlawful fund transactions (Mugarura & Ssali, 2020; Şcheau & Zaharie, 2017).

Cyber laundering is carried out through some changes in the modus operandi of hackers, who alter and optimize the existing payment mechanisms into fraudulent methods. (Zagaris, 2022). There are at least two types of cyber laundering: first, online gaming, in which the criminals launder money by opening numerous accounts on various online games. Second, micro laundering, which is more popular as cyber criminals use various sites like PayPal, job advertising sites, and like where online and mobile micro-payments are connected with net banking services or credit cards to avoid detection (Filipkowski, 2008). The money launderers move large amounts of money through thousands of small electronic transactions to and from these payment methods. It is difficult to detect such transactions because the criminals use virtual credit cards, prepaid e-sims in their mobile phones, virtual currencies such as Bitcoin; they often use a scammed bank account to make instant transactions, thus becoming eligible to open a PayPal account or on any other similar payment portal (Mugarura & Ssali, 2020; Şcheau & Zaharie, 2017).

These cybercriminals can hack the 'traditional' money transfer mechanisms like wire transfers and online payments, cash deposits and withdrawals. They use accounts opened with lost documents or documents of nominees hacked; they create fictitious companies and make transactions in their accounts, and convert such stolen funds into cash/cash withdrawals via banks ATMs (Wronka, 2021). The Budapest Convention (Campina & Rodrigues, 2022) identified a few categories of cybercrime offences that help in money laundering, namely cyber fraud to gain illegal possession of funds, access information illegally; and hack the information management systems of individuals and organizations to access their vital credentials. The main types of money laundering crimes by cyber criminals include unauthorized removal of funds from bank accounts, payments card fraud, use of malware and spread of computer viruses, and attacks on websites

Several countries have passed legislations to fight against cyber laundering (Chistyakova, Wall, & Bonino, 2019; Joveda, Khan, & Pathak, 2019; Saputra, 2016; Wronka, 2021) like Financial Action Task Force on Money Laundering (FATF), legal frameworks of Anti Money Laundering (AML), besides having National Criminal Justice Systems related to the financial sector (Zolkaflil, Nazri, & Omar, 2022). The international Financial Crimes Enforcement Network (FINCEN) has released a series of advisories for financial institutions to stay vigilant for cybercrime The European Union has also issued Ant-Money Laundering Directive (AMLD), which lists 22 money laundering predicate offences, like human trafficking, drug trafficking, counterfeiting, and theft. The European union introduced a new compliance obligation for firms to screen their customers and transactions for evidence of cyber laundering activities.

In order to prevent cyber laundering, in addition to laws and regulations, the enforcement agencies also use another strategy, namely asset recovery (Byrnes & Munro, 2022; Zolkaflil et al., 2022). Asset recovery aims at deterring money laundering offenses and to eliminate criminals' hold on the assets, either by taking away all the assets or confiscating any profits generated from such assets or by freezing the assets, regionally or internationally, so that wealth can be returned to the legitimate state or its owners. Confiscation is in the form of the seizure of property belonging to the person who committed the crime, and who was responsible for the loss of revenue to the state. Anti-Money Laundering Law allows the state to utilize the confiscated wealth as state assets or restore them to the original owners. Thus, asset recovery involves returning the assets of the criminal offense to their lawful owners. Such asset recovery is done under the leadership of a prosecutor and within the directions of a law enforcement agency (Brun et al., 2022)

This paper first examines money laundering and cybercrime as two fundamental phenomena, from where cyber laundering originated. While exploring these two disciplines, the paper also examined legal regulations that aim at preventing cyber laundering, particularly in Indonesia. The paper also took the issue of asset recovery as the right of the state or of the community, which suffered the loss due to cyber laundering or any crime associated with Internet fraud or phishing. Hence the issue in this research, also included justifying the repatriation of assets (asset recovery) arising from money laundering offenses from overseas location with the help of legislations.

Problem statement

There exists a huge network of cybercrime money laundering activates through which criminals target vulnerable individuals and organizations, posing a threat to the organized economy. The current global scenario is vulnerable to cyber laundering owing to the data-driven financial landscape, which becomes an easy arena for committing cybercrimes. Cybercriminals, by exploiting the Internet and the computer systems, have created a parallel online network of financial services to execute money laundering, fraud and other crimes. In 2015, cybercrime had cost the global economy around $3 trillion, which rose to $6trillion in 2021. This figure is expected to grow by around 15% annually over the next 5 years, reaching around $10.5 trillion in 2025.

Due to the pandemic, there was too much reliance on online transactions for all commercial and financial purposes which gave cyber criminals the opportunity to devise newer methods of online fraud and theft. They were seen indulged in cyber-events such as compromising or gaining unlawful access to the victim's computer along with its data, resources and information. The cyber-enabled crimes such as frauds, drug-dealing, sexual exploitation, weapons trafficking, and online blackmailing, also increased. other examples include illegal access to computers and networks via email phishing, hacking attacks, fraud and forgery committed with the use of computers, online content-related crimes including child pornography or incitements to violence or racism, and last but not the least, intellectual property crimes such as the unauthorized reproduction, distribution and sharing of copyrighted materials such as films, music, and software, most of which have financial connotations (Diniyya, Aulia, & Wahyudi, 2020).

With the growing diversity in their modus operandi and making use of innovative methods, it is very challenging for the banks, financial institutions and other regulatory enforcement bodies to control these cybercriminals. It is important that there exists a cybercrime money laundering response mechanism in every bank and financial institution which alerts its customers against risk and insist for the compliance of the safety measures.

Research Methods

This study utilized the normative legal document analysis methodology, for which data was collected from secondary and tertiary legal archives. The juridical analytical method examined the laws and regulations pertaining to cyber laundering and their limitations (Karo & Sebastian, 2019). This analytical method is pertinent to qualitative research designs (Creswell & Miller, 2000) and useful for deductive and inductive reasoning required in normative research. The research data also included the concerning laws and regulations, related to cyber laundering and assets recovery or repatriation of laws. Moreover, conducting a research on cyber laundering activities posed an inherent challenge, as most criminals and their banks are inaccessible to discuss criminal offenses. Likewise, the victims are also not willing to disclose their saga of fraud, and prefer anonymity to getting justice.

After the data was collected, it was filtered and irrelevant threads were discarded. Consequently, the data available was analyzed thorough content analysis methods to derive out threads, which were synthesize in the form of findings of this study.

Literature Review

- *Anti-Money Laundering*

Money Laundering crimes are becoming more diversified (Teichmann, 2017), which result in both tangible and intangible losses. It is believed that such crimes would offer a maximum penalty, thus deterring criminals from repeating their activities. With money laundering becoming more prevalent in Indonesia, the government has made every effort to prevent and destroy it. One method is enactment of rules on the prevention and eradication of money laundering offences, e.g., Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes (Go & Benarkah, 2019). Although the Anti-Money Laundering Law regulates penalties for money laundering criminals, this does not always diminish the number of money laundering offences. This is because the punishment for criminals is generally incarceration, which is insufficient to deter money laundering (Levi, 2020).

Anti-Money Laundering (AML) comprises policies, laws, and regulations to prevent financial crimes. AML originates from cybersecurity, which aims to combat all types of cybercrimes through legislations. The Financial Crime Enforcement Network (FinCEN) released cybersecurity guide to regulate financial services and integrating cyber incidents with AML programs. One of the guidelines is to incorporate compliance units in every Information Management and Information Security department. Senior money laundering managers in banks, brokerage houses, and other financial services should familiarize with their company's cybersecurity regimes, resources and security protocols. The FinCEN also issues advisory to all

banks and financial institutions to understand the Bank Secrecy Act (BSA) obligations related to cyber laundering and cyber-related crimes. The bank managers are required to prepare a Suspicious Activity Report (SAR), which would act as a tool to track suspicious activities as well as a part of anti-money laundering laws. The SAR will also identify customers involved in money laundering, fraud, or terrorist funding.

Such legislations require all financial units to set up cybersecurity units, risk departments, fraud prevention units, BSA/AML management boards, AML intelligence units, AML analysts/investigators and well trained network administrators. These legislations can also provide training to the personnel involved in the business of Anti Money laundering, to timely detect offences and suspected money laundering. The Budapest Convention on Cybercrime 2001 is the best example of international treaty on cybercrimes committed via the internet and other computer networks. The convention emphasized on harmonizing the regional laws with international regulations.

- *Asset recovery laws*

Money laundering criminals often attempt to divert the profits of their crime into lawful enterprises, complicating law enforcement efforts There is a provision in the form of restoring state financial losses, carried out by the seizure of assets arising from criminal activities that have the following goals like (i) returning state assets taken by corruptors; (ii) preventing corruptors from utilizing stolen assets to perpetrate additional crimes like money laundering; and (iii) punishing those who want to conduct corruption (Brun et al., 2022; Byrnes & Munro, 2022; Zolkaflil et al., 2022). Law enforcement agencies called this provision as asset recovery practiced through methods like confiscation, profit and loss, and other measures (Chistyakova et al., 2019). When an asset is recovered, it is ensured that its value remains maximum when it is returned to the state. Such an asset recovery is supposed to serve as a deterrence to offenders of money laundering offenses. Because asset recovery seeks to remove the perpetrator's link with the assets he has from the profits of a criminal conduct, both at home and abroad, by taking the assets. This will make criminals think carefully about money laundering since if they are found, they will face severe punishment and their assistance may be seized.

Practices in numerous nations demonstrate that the problem of asset recovery has been incorporated into the legal system, with the prosecutor's office serving as the primary component. This legal practice stems from the prosecutor's office's function as the hub of an integrated criminal justice system. In Indonesia, the prosecutor should take the lead in asset recovery.

- *Money laundering in Indonesia and Asset recovery laws*

In Indonesia, money laundering is defined as any act that meets the elements of a criminal act by the provisions of the law in Article 1 number (1) of Law Number 15 of 2002 concerning the Crime of Money Laundering as amended by Law Number 25 of 2003 concerning Prevention of the Crime of Money Laundering as amended by Law Number 8 of 2010 concerning Prevention and The Eradication of the Crime of Money Laundering (UU TPPU) (Saputra, 2016; Suryadi & Budianto, 2022; Yusuf, Chandra, & Sinaulan, 2022). The definition of money laundering can also be found in Articles (3), (4), and (5) of the Anti-Money Laundering Law, which state that "the crime of money

laundering is a type of crime committed by either a person or a corporation intentionally placing, transferring, spending, paying, granting, entrusting, bringing abroad, changing the form, exchanging for currency or securities, or other actions on assets which are known or reasonably suspected."

The wealth accumulated through money laundering is turned into clean money through three stages: placement, layering and integration. The Placement the stage in which one places cash derived from a crime into the financial system or attempts to place it in demand deposits (cheques, bank drafts, certificates of deposit, etc.), to send it back into the authentic financial system, particularly the banking system. The Layering stage refers to an endeavor to move assets derived from illegal activity (dirty money) that have been effectively placed with Financial Service Providers (particularly banks) as a consequence of placement efforts to other Financial Service Providers. Layering makes it harder for law enforcement to determine the origin of assets. By doing so, it looks that the lawful business operations are the consequence of bank credit rather than filthy money. The Integration stage attempts to employ assets derived from criminal crimes that have entered the financial system through placement or transfer in order for them to look as clean money for legitimate commercial operations or to refinance illicit activities (Saputra, 2016; Suryadi & Budianto, 2022).

As stated in the Anti-Money Laundering Law, the regulation of asset recovery in the crime of money laundering has controlled attempts to take assets without penalty, known as Non-Conviction Based (NCB) Asset Forfeiture (Maguchu & Ghozi, 2022; Priyatno, 2018). The NCB Asset Forfeiture mechanism positions assets suspected of being the proceeds or means of criminal acts as legal subjects/parties, with the parties consisting of countries represented by money laundering investigators as applicants/prosecutors versus assets suspected of being the proceeds or means of criminal acts as the respondent. This approach allows for the confiscation of assets without the need for a judicial judgment for criminal actors.

The Indonesian Asset Recovery law clearly state the policies related to the assets recovered. According to Article 67 of the Anti-Money Laundering Law, investigators may petition the District Court to determine whether funds suspected of being the proceeds of a criminal crime should be utilized as state assets or restored to those entitled (Marwan, Jiow, & Monteiro, 2022). This article states that (i) If no individual or third party files an objection within 20 (twenty) days after the Transaction's temporary suspension, the PPATK can provide the management of Assets known or reasonably believed to be the proceeds of crime to the investigator for inquiry; (ii) if the accused perpetrator of a criminal conduct is not located within 30 (thirty) days, the investigator may petition to the district court for a determination that the aforementioned assets are state assets or that they should be restored to those who are entitled to them; and (iii) the court, as mentioned in section (ii), must make a decision within 7 (seven) days (Go & Benarkah, 2019; Maguchu & Ghozi, 2022; Setiyawan, 2019).

Results and Discussion

Asset recovery against money laundering is carried out in several countries during the pre-confiscation stage for preparation and analysis, such as: seeing the priority of confiscated assets, confiscation methods, profit and loss, management, and other issues (Chistyakova et al., 2019) so that when the purchase is seized, it can be easily

managed and its value remains maximum when it is returned to the state. The phases of asset recovery are classified as Tracking, Blocking, Confiscation and Return. The first phase of Tracking is the initial step when the investigator gathers and assesses evidence pertaining to the assets of money laundering crimes concealed by the offenders to be recognized, tallied, and counted. Tracking might begin during an inquiry by searching for aspects of a criminal conduct during the study to discover the suspect and his assets. Furthermore, the tracking process may begin even if no cases exist. The second stage of Blocking is also known as the freezing stage. Blocking may be defined as an attempt to prevent the assets of a criminal act from being transferred to another person by temporarily freezing the aid of a criminal. This stage also allows investigators, public prosecutors, and courts to intervene. If the assets to be banned are situated overseas, coordination between Indonesian and destination country law enforcement officers is necessary. This is required for ease of blocking and restoring assets to Indonesia. The establishment of Mutual Legal Assistance is one of the actions made to ease the management of these assets.

The third stage of Confiscation, according to the Criminal Procedure Code (KUHAP), is a set of steps taken by an investigator to take over and or retain custody of moveable or immovable, tangible or intangible assets for use as evidence in an investigation, prosecution, or trial. Confiscation, according to Indonesian criminal law, is the seizure of property belonging to a person who has committed a crime as an extra penalty imposed by a court in addition to the original criminal violation, as provided in Article 10 of the Criminal Code (KUHP). The MLA Law also defines Confiscation as a coerced attempt to seize rights to assets or income gained or potentially obtained by persons as a result of illegal conduct undertaken in accordance with court rulings in Indonesia or other countries. The final stage of Return is a part of the criminal asset management process, which includes storage, security, maintenance, appraisal, transfer, usage, utilization, distribution, and criminal assets. If a criminal asset is purchased in another country, this stage of return includes the procedure of returning the asset despite the local support. The person named in the court ruling is responsible for returning this asset. This is in accordance with the Supreme Court of the Republic of Indonesia Regulation No. 1 of 2013 on Procedures for Settlement of Applications for Handling Assets in the Crime of Money Laundering or Other Crimes. The purpose of this regulation is to fill the legal void left by Article 67 of the Money Laundering Law.

The return of assets arising from a criminal conduct is an attempt to take strategic actions to secure assets suspected of having been earned through illegal profits. The phrase "return of support" suggests that the possession of assets by criminal offenders is not founded on legal considerations since they are the profits of crime. As a result, these assets must be restored to the entity that has legal ownership of them, namely the state. The state reclaims or repatriates' assets that are rightfully theirs from criminals who have illegally possessed these assets by returning purchases.

Returning assets is not just a procedure, but also a law enforcement operation carried out via a variety of legal instruments. This is consistent with the findings of Maguchu and Ghozi (2022), who defines returning assets resulting from criminal acts as a law enforcement system carried out by countries victims of criminal acts to revoke, confiscate, and eliminate rights to assets resulting from criminal acts through

a series of processes and mechanisms, both criminally and civilly, purchases resulting from criminal acts, both domestically and abroad, are tracked, frozen, confiscated, handed over, and returned to the state.

According to Sihite and Mustofa (2021), criminal activities are used as a tool or method to accomplish further unlawful actions, and they serve as a deterrent to offenders and prospective perpetrators of criminal acts. According to the formulation of this understanding, there are several essential elements of returning assets resulting from criminal acts, namely:

a. Asset recovery is a law enforcement system;
b. Law enforcement is carried out both through criminal and civil channels;
c. Assets resulting from criminal acts are tracked, frozen, confiscated, confiscated, handed over, and returned to the state victims of the crime through these two channels;
d. Tracking, freezing, confiscation, handing over, and returning to the state victims

1) Restoring the loss to the victim of a crime caused by the perpetrator of the crime;
2) Preventing criminal perpetrators from using or utilizing these assets as tools or facilities to commit other illegal acts, such as money laundering, terrorism, and other transnational crimes; and
3) Acting as a deterrent to other parties who intend to commit a crime.

Returning the assets of a criminal offense is a law enforcement system, that requires a process of removing rights to the help of the perpetrator from the victim country by, among other things, removing rights to the perpetrator's assets civilly or criminally; this can be done through confiscation, freezing, and confiscation, both locally and regionally, as well as internationally, so that wealth can be returned to the legitimate state (victim). The theory of asset return, on the other hand, is a legal theory that describes the legal system for creating assets based on social justice principles, which offers capacities, obligations, and responsibilities to state institutions and legal institutions in order to provide protection. Opportunities for individual prosperity in society.

This approach is founded on a basic principle: do what is good for the state. The rights of the state include state duties that are individual rights of the community, ensuring that the code is equitable and consistent with the idea of offering to the people what the people's rights are. When the practice of moving assets crosses national borders, it becomes more difficult to trace the outcomes of illegal activities, particularly corruption. The return of assets resulting from illegal actions committed by perpetrators abroad can be carried out by referring to the provisions of the United Nations Anti-Corruption Convention (KAK), which consists of four (four) stages, which are as follows:

a. asset tracking to track assets;
b. preventive measures to stop the movement of assets through freezing or confiscation mechanisms; and
c. confiscation, and only after going through and fulfilling these stages can the stages be completed. One of the highlights of creating KAK has been attempts to return assets that were purchased/obtained unlawfully, either directly or indirectly. These assets are often so valuable that their repatriation necessitates a difficult process (Mendell, 2017).

The capacity of investigators to uncover signs of ownership of unlawfully acquired money and assets or locate the offenders is critical to the effectiveness of monitoring money laundering crimes, public sector crimes, and economic crimes in general (Mendell, 2017). Tracking often shows malevolent intent, identifies criminals, and may pave the road for the confiscation and surrender of illegally acquired revenues by freezing or seizing or confiscating assets. If the frozen or seized assets are within the legal jurisdiction of the victim's nation, the order allows for prompt freezing or confiscation. Assume the assets are beyond the legal jurisdiction of the victim nation but within the legal jurisdiction of another country (recipient country). In such instance, the freezing and confiscation order may only be carried out by the destination country's responsible government.

There are two ways to carry out the victim country's freezing or confiscation order in the receiving country's legal jurisdiction, namely: (i) If the national law of the beneficiary country allows the competent authority of that country to carry out a freezing and confiscation order issued by the competent authority of another country from which the assets were obtained illegally, the demand from the victim country can be carried out.(ii) If the receiving country's national law prohibits its agencies from carrying out freezing and confiscation orders issued by competent authorities of other countries, the leaders of the victim country must request that the receiving country's competent authorities issue orders freezing or confiscating assets illegally placed in the receiving country.

Furthermore, during the stage of asset confiscation, a confiscation order is generally issued by the receiving nation's court or competent body after a court judgment imposes a crime on the offender of a crime in the victim country. Confiscation may be carried out without a court order if the perpetrator of the offense has died or gone, or if the prosecutor, as the public prosecutor, is unable to prosecute. With a confiscation order, the victim country's court or competent authority demands that the confiscation order be carried out by the receiving government. The confiscation order may be executed if the recipient country's national legislation allows the competent authorities to carry out the confiscation order. However, suppose the beneficiary nation's federal legislation prohibits its police from carrying out a confiscation order issued by another country (the victim's country). In such instance, the victim country's responsible government must request that the receiving country's leaders issue a seizure order for the assets.

In addition to the legislative measures, asset recovery operations are carried out in collaboration with the Stolen Asset Recovery Initiatives (STAR). The World Bank (World Bank) and the United Nations collaborate with STAR in order to promote international cooperation in recovering assets originating from criminal crimes, particularly in poor nations. Stolen Asset Recovery Initiatives (STAR) aims to give actual support to Indonesia in the recovery of assets stolen through criminal activities.

The following are examples of STAR activities, particularly in Indonesia: (1) *Development of Asset Recovery Capacity.* Stolen Asset Recovery Initiatives (STAR) Initiative assists in improving the quality of human resources possessed by asset recovery agencies in Indonesia. (2) *Legal Structure.* Stolen Asset Recovery Initiatives (STAR) worked with Indonesian law enforcement to revise the Asset Confiscation Bill (RUU) and the Anti-Money Laundering Law. (3) *Technical Support.* Stolen Asset

Recovery Initiatives (STAR) offers technical support through hosting worldwide conferences. Representatives from each nation may create collaboration relating to asset recovery or relevant MLA submissions in this forum. Friends of STAR is a worldwide networking group comprised of finance ministers and international central bank governors.

Asset recovery operations are also carried out in partnership with MLA (Mutual Legal Assistance) between Indonesia and Switzerland. With this collaboration, the Indonesian government may petition for the banning of accounts associated with the criminal offender's crime. Furthermore, the transaction data collected from the Swiss bank may be used as legal evidence in court. In Indonesia, asset return law enforcement includes several law enforcement agencies, including PPATK, police, prosecutors, KPK, the Ministry of Law and Human Rights, and the Ministry of Foreign Affairs, are still not properly coordinated. In general, the prosecutor's office serves as an organization that manages seized assets. It is therefore the prosecutor's responsibility to preserve the worth of the assets so that they do not deteriorate. The prosecutor's office should establish a work unit dedicated to asset recovery. The Asset Recovery Center is the name of the group (PPA). The PPA's principal duty and role is to offer services for collecting criminal assets and restoring criminal assets to those who are entitled, including the state.

Conclusion

Based on the preceding discussion, the following conclusions can be drawn:

a. When dealing with money laundering crimes with proceeds stored abroad, law enforcement officers require the integrated cooperation of various agencies, such as PPATK, Police, Attorney General's Office, KPK, and the Ministry of Law and Human Rights. As well as cooperation between agencies (agent to agent) and Mutual Legal Assistance (referring to the Law of the Republic of Indonesia No. 1 of 2006 on Mutual Assistance in Criminal Matters and the Law of the Republic of Indonesia No. 7 of 2006 on Ratification of the United Nations Convention Against Corruption (UN Anti-Corruption).
b. Whereas, as stipulated by the Money Laundering Law, law enforcement against the Crime of Money Laundering (TPPU) continues to face impediments in both substantive law (material law) and procedural law (ceremonial law). The restrictions in issue are those relating to establishing the predicate crime, and the regulations governing reverse proof and its implications have not been controlled. In reality, the aforementioned requirements are troubling and must be rectified soon in order to provide legal clarity.

Some recommendations may be made based on the findings and conclusions of the study:

a. Improving coordination among law enforcement authorities, such as PPATK, Police, Attorney General's Office, KPK, Ministry of Law and Human Rights, and Ministry of Foreign Affairs, as a form of integrated cooperation, to address the issue of money laundering, whether deposited overseas, and subsequently asset recovery under the prevailing laws.

b. Enacting rules and regulations governing reverse evidence and its implications, in order to provide legal clarity about the crime of money laundering, wherever deposited by the cyber launderers.
c. As the use of Internet grows, opportunities for criminals to involve in their money laundering scams continue to grow. This creates an increasingly difficult situation for various law enforcement agencies that are already being put to the test by such criminals who devise myriad untraceable means to launder illegally obtained money. As individuals, it is the responsibility of the state and financial institutions to stay informed, and always be aware of the methods these criminals use to launder money illegally.

In addition, the practice of cyber laundering can be stopped by early detection of crime being planned or a mechanism being created. The financial agencies and law enforcement bodies should develop an investigation plan, gather enough information about money launder and their modus operandi, and look for evidence of origins of criminal property including circumstantial evidence, forensic evidence and use of audit trails. For the purpose of asset recovery, it is important to confiscate all proceeds of crime acts, obtain information about bank accounts and restrain any future criminal proceedings. Surveillance measures must continue through specialist cybercrime investigation units.

References

Brun, J. P., Gomez, A., Julien, R., Ndubai, J., Rao, S., & Soto, Y. (2022). *Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes*. World Bank Publications. https://books.google.com.pk/books?id=DK57EAAAQBAJ

Byrnes, W. H., & Munro, R. J. (2022). *Money Laundering, Asset Forfeiture and Recovery and Compliance--A Global Guide*. LexisNexis. https://books.google.com.pk/books?id=cVLUdo4JQv4C

Campina, A., & Rodrigues, C. (2022). Cybercrime and the Council of Europe Budapest Convention: prevention, criminalization, and International Cooperation. *The Book of Full Papers-7th International Zeugma Conference on Scientific Researches, 1*(1), 112-123. http://hdl.handle.net/10284/10766

Chawki, M. (2022). Cybercrime and the Regulation of Cryptocurrencies. In *Future of Information and Communication Conference* (pp. 694-713). Springer. https://doi.org/10.1007/978-3-030-98015-3_48

Chistyakova, Y., Wall, D., & Bonino, S. (2019). The Back-Door Governance of Crime: Confiscating Criminal Assets in the UK. *European Journal on Criminal Policy and Research*. http://researchonline.ljmu.ac.uk/id/eprint/11313/

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into practice, 39*(3), 124-130. https://doi.org/10.1207/s15430421tip3903_2

Diniyya, A. A., Aulia, M., & Wahyudi, R. (2020). Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study. *Ihtifaz: Journal of Islamic Economics, Finance, and Banking, 3*(2), 67-87. https://doi.org/10.12928/ijiefb.v3i2.2703

Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Techniques. *International Journal of Criminal Justice Sciences, 3*(1). https://www.researchgate.net/profile/Wojciech-Filipkowski/publication/222099776

Go, L., & Benarkah, N. (2019). Quo Vadis legal profession participation in anti-money laundering. *Journal of Money Laundering Control, 22*(4), 764-769. https://doi.org/10.1108/JMLC-12-2018-0072

Goni, O. (2022). Cyber Crime and Its Classification. *Int. J. of Electronics Engineering and Applications, 10*(1). https://www.researchgate.net/profile/Osman-Goni-10/publication/360383932

Joveda, N., Khan, M., & Pathak, A. (2019). Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information. *International Journal of Economics and Finance, 11*(10), 54-65. https://econpapers.repec.org/article/ibnijefaa/v_3a11_3ay_3a2019_3ai_3a10_3ap_3a54-65.htm

Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. *Lentera Hukum, 6*, 1. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lenth6

Levi, M. (2020). Evaluating the control of money laundering and its underlying offences: the search for meaningful data. *Asian Journal of Criminology, 15*(4), 301-320. https://link.springer.com/article/10.1007/s11417-020-09319-y

Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICABCD.2018.8465467

Maguchu, P., & Ghozi, A. (2022). The Role of Civil Society Organisations in Asset Recovery. *Indonesian Journal of International Law, 19*(2), 317-338. https://doi.org/10.17304/ijil.vol19.2.6

Marwan, A., Jiow, H. J., & Monteiro, K. (2022). Cybersecurity Regulation and Governance During the Pandemic Time in Indonesia and Singapore. *International Journal of Global Community, 5*(1), 13-32. https://www.riksawan.com/IJGC-RI/index.php/IJGC-RI/article/view/109

Mendell, R. L. (2017). *How to Do Financial Asset Investigations: a Practical Guide for Private Investigators, Collections Personnel and Asset Recovery Specialists*. Charles C Thomas, Publisher, Limited. https://books.google.com.pk/books?id=TSA3DwAAQBAJ

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

Priyatno, D. (2018). Non Conviction Based (NCB) Asset Forfeiture for Recovering the Corruption Proceedings in Indonesia. *Journal of Advanced Research in Law and Economics, 9*(1), 219-233. https://doi.org/10.14505//jarle.v9.1(31).27

Richet, J.-L. (2013). Laundering Money Online: a review of cybercriminals methods. *arXiv preprint arXiv:1310.2368*. https://doi.org/10.48550/arXiv.1310.2368

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. In *2016 International Conference on ICT For Smart Society (ICISS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICTSS.2016.7792846

Şcheau, M. C., & Zaharie, S. P. (2017). Methods of Laundering Money Resulted from Cyber-crime. *Economic Computation and Economic Cybernetics Studies and Research, 51*(3), 299-314. https://ideas.repec.org/a/cys/ecocyb/v50y2017i3p299-314.html

Setiyawan, A. (2019). National cybersecurity policy in the US and Indonesia. *UNTAG Law Review, 3*(1), 71-87. https://doi.org/10.36356/ulrev.v3i1.1071

Sihite, M. I., & Mustofa, M. (2021). Asset recovery policy strategy of corruption proceeds placed abroad within the perspective of the state as a victim. *Technium Social Sciences Journal, 19*(1), 15–38. https://techniumscience.com/index.php/socialsciences/article/view/3117

Suryadi, P., & Budianto, A. (2022). Money Laundering And Tax Evasion Resulting From Cyber Crimes Through Digital Currency (Crypto Currency). In *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2022, 16 April 2022, Semarang, Indonesia*. EAI. https://doi.org/10.4108/eai.16-4-2022.2320042

Teichmann, F. M. J. (2017). Twelve methods of money laundering. *Journal of money laundering control*. https://doi.org/10.1108/JMLC-05-2016-0018

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

Yusuf, M., Chandra, T. Y., & Sinaulan, R. L. (2022). Cyber Crime Law Enforcement Against Illegal Access to Online Banking in Indonesia. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 5*(3). https://doi.org/10.33258/birci.v5i3.6619

Zagaris, B. (2022). Cybercrime, Espionage, and Intellectual Property Enforcement. *IELR, 38*, 113. https://heinonline.org/HOL/LandingPage?handle=hein.journals/ielr38

Zolkaflil, S., Nazri, S. N. F. S. M., & Omar, N. (2022). Asset recovery practices in combating money laundering: evidence from FATF mutual evaluation report of FATF member countries of Asia pacific region. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-11-2021-0127

Role of Law Enforcement to prevent Cyber laundering and Asset Recovery from Overseas

ORIGINALITY REPORT

23%	21%	11%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Curtin International College Student Paper	4%
2	complyadvantage.com Internet Source	3%
3	www.iap-association.org Internet Source	2%
4	Ezzah Nariswari Lupianto. "Asset Recovery for Victims of “Binary Option” Case in Review of International Criminal Law", Corruptio, 2022 Publication	2%
5	sanctionscanner.com Internet Source	1%
6	research-repository.griffith.edu.au Internet Source	1%
7	docplayer.net Internet Source	1%
8	www.cybercrimejournal.com Internet Source	1%

9	ijmmu.com Internet Source	1 %
10	Midian Hosiholan Rumahorbo, Risa Mahdewi, Desia Rakhma Banjarani. "The Role Of The Prosecutors In The Effort Of Assets Recovery From Corruption Crimes", Ius Poenale, 2022 Publication	1 %
11	seajbel.com Internet Source	1 %
12	www.jurnalhukumdanperadilan.org Internet Source	1 %
13	"Anti‐Money Laundering: International Law and Practice", Wiley, 2012 Publication	1 %
14	Submitted to University of Sussex Student Paper	1 %
15	Submitted to Universitas Islam Indonesia Student Paper	<1 %
16	www.ejournal.warmadewa.ac.id Internet Source	<1 %
17	www.flevin.com Internet Source	<1 %
18	www.ppatk.go.id Internet Source	<1 %

19	Sutarno Bintoro, Sjamsiar Sjamsuddin, Ratih Nur Pratiwi, Hermawan. "International cooperation to combat money laundering in the capital market: Indonesia and Australia experience", Journal of Investment Compliance, 2020 Publication	<1 %
20	lppm-unissula.com Internet Source	<1 %
21	Submitted to Fakultas Hukum Universitas Lampung Student Paper	<1 %
22	journal.unnes.ac.id Internet Source	<1 %
23	ijsshr.in Internet Source	<1 %
24	Abdul Wahid, Sulbadana, Vivi Nurqalbi, Fathul Hamdani. "The Effects of Decision Number: 15/PUU-XIX/2021 of the Constitutional Court on Indonesia's Money Laundering Law Enforcement", European Journal of Law and Political Science, 2022 Publication	<1 %

Exclude quotes On

Exclude matches < 15 words

Exclude bibliography On