

# The Existence Of Notaries In Supporting Electronic Transaction Security Systems Related To Money Laundering And Terrorism Financing In Indonesia

Reza Rama Valiandra<sup>1</sup>, Efa Laela Fakhirah<sup>2</sup>, Ranti Fauza Mayana<sup>3</sup>, Danrivanto Budhijanto<sup>4</sup>

<sup>1</sup>Faculty of Law, Universitas Padjadjaran, Indonesia.

<sup>2</sup>Faculty of Law, Universitas Padjadjaran, Indonesia.

<sup>3</sup>Faculty of Law, Universitas Padjadjaran, Indonesia.

<sup>4</sup>Faculty of Law, Universitas Padjadjaran, Indonesia.  
[donvaliandra@yahoo.com](mailto:donvaliandra@yahoo.com)

## Abstract

Indonesia is the only G20 member country that is not yet a member of the Financial Action Task Force (FATF). However, notaries in Indonesia have a significant role in helping prevent money laundering and terrorism financing. The role can be conventionally by applying the Principles of Recognizing Service Users for Notaries (customer due diligence) or electronically as an electronic certificate registration authority (Registration authority) which is authorized to conduct an inspection, verification, identification of legal subjects of electronic certificate applicants before conducting electronic transactions. The principle of recognizing service users for notaries (customer due diligence) and the position of a notary as an electronic certificate registration authority are interoperability of the function of the notary's authority in assisting the government to prevent money laundering and terrorism financing as a suspect in reporting financial transactions. The application of the Principles of Recognizing Service Users, Reporting and Analysis of Financial Transactions for notaries is also one of the requirements for Indonesia to become a member of the FATF.

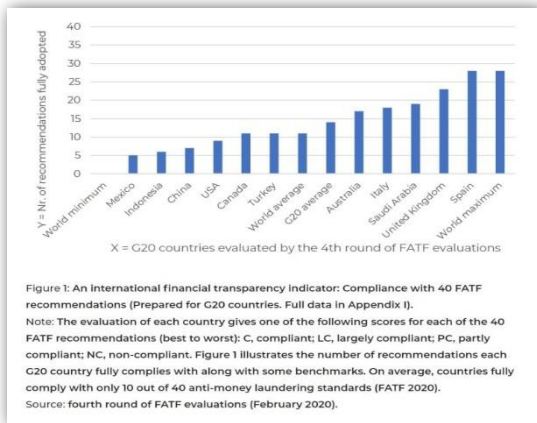
**Keyword :** The Existence of Notaries, Security Systems, Electronic Transactions, Money Laundering, Terrorism Financing.

## INTRODUCTION

Het recht hinkt achter de feiten aan or Law is too slow to keep up with new technology.<sup>1</sup> Whereas technology has become a source of information and will not function properly if there is a lack of multi-communication channels between parties.<sup>2</sup> However, the presence of technology itself is not always without problems, legal problems that occur due to the presence of new technology can only be anticipated by the legal system. Gregory

N Mandel, put firmness in his thinking in the title History Lessons For a General Theory of Law and Technology<sup>3</sup> that state "The marvels of technological advance are nor always risk free. The new legal issues created by technological advance frequently are quite challenging, such risks and perceived risks often create new issues and disputes to which the legal system must respond."

Mutual Evaluation Report (MER), Anti-money laundering and counter-terrorist financing measures, The Asia Pacific Group on Money Laundering (APG), reported that since 2008 Indonesia does not have effective security measures in mitigating the development of new technologies related to money laundering and terrorism financing.<sup>4</sup> In a 2020 Financial Action Task Force (FATF) report, Indonesia is the only



G20 member country that is not yet a member of the FATF.<sup>5</sup> Indonesia is also ranked second lowest after Mexico, a member of the G20 in terms of commitment and transparency of financial data according to FATF recommendation standards, related to money laundering and terrorism financing.<sup>6</sup> As shown in Figure 1 below:

**Picture. 1.** Transparency of G20 Member Countries' Financial Data Commitments in accordance with FATF Standards.

International Union of Latin Notaries (UINL) which has 89 member countries including notaries in Indonesia are members of the Legislature Activity Report 2017-2019 International Congress of Notaries held in Jakarta Indonesia on 27-30 November 2019, said:<sup>7</sup>

“The Union carries out its activities through continental and intercontinental commissions and working groups that work on a wide range of projects, such as training and education, research studies, notarial cooperation, human rights, strengthening of the notarial function and the authentic act, notarial deontology, new technologies, the fight against money laundering and terrorist financing.”

According to the Financial Transaction Reports and Analysis Center (PPATK), which is a Financial Intelligence Unit (FIU) in Indonesia, notaries are gatekeepers in identifying and verifying legal subjects related to legal actions that will be carried out by service users, whether related to money laundering or terrorism financing.<sup>8</sup> The French Financial Intelligence Unit (FIU), namely the Traitement du Renseignement et Action Contre les Circuits Financiers Clandestines (TRACFIN) stated, Latin notary characteristics or civil law state notaries have the authority of a set of rules that are able to detect suspicious financial transactions or detect legal smuggling in financial transactions.<sup>9</sup>

## RESEARCH METHOD

The data collection method in this study uses a normative juridical approach, namely research that emphasizes the use of secondary data or researching library materials, normative juridical research includes research on legal principles, legal systematics, and research on the level of vertical and horizontal synchronization.<sup>10</sup> This is reinforced by structured interviews conducted at the National Cyber and Crypto Agency of the Republic of Indonesia and the Central Board of

the Indonesian Notary Association (Notary Chamber of Indonesia).

## RESULTS AND DISCUSSION

Based on the report of the Financial Transaction Reports and Analysis Center (PPATK) in 2021 the potential loss to the State due to the Crime of Money Laundering reached 37.8 trillion Rupiah for the proceeds of Corruption in the Natural Resources Sector, 16.81 Trillion Rupiah for Corruption in the Financial Management of Investment Funds, while from the proceeds of Narcotics crime from Two different drug networks were found in the crime of money laundering worth 6.4 trillion rupiah and 27 trillion rupiah. According to PPATK, Corruption, Funds Transfer for suspected terrorism financing, Narcotics, Electronic Transaction Information (ITE) or SIBER are types of predicate offenses TPPU which are categorized as a high threat TPPU to Indonesia (Inward Risk).<sup>11</sup>

In this case, the PPATK recommendation to the Ministry of Law and Human Rights, as a notary builder in Indonesia, issued the Minister of Law and Human Rights Regulation number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries (Permenkumham number 9 of 2017) which is the

implementing technical regulation from Government Regulation number 43 of 2015 concerning Reporting Parties in the Prevention and Eradication of the Crime of Money Laundering. Article 2 point (4) of the Minister of Law and Human Rights number 9 of 2017 states :<sup>12</sup>

“The obligation to apply the principle of recognizing service users for Notaries is carried out when: **a.** conduct business relations with Service Users **b.** there is a Financial Transaction in rupiah currency and/or foreign currency whose value is at least or equivalent to Rp. 100,000,000.00 (one hundred million rupiah); **c.** there are Suspicious Financial Transactions related to the crime of Money Laundering and the crime of financing terrorism; or **d.** The Notary doubts the truth of the information reported by the Service User.”

The principle of recognizing service users for notaries according to Permenkumham number 9 of 2017 is :<sup>13</sup> Service User identification; Service User verification; and monitoring of Service User Transactions. The technical method is the recommendation of the UINL and FATF ratification results can be seen in the following table :<sup>14</sup>

**Table 1.** Method of Application of the Principle of Recognizing Service Users for Notaries in the Prevention of Money Laundering and Terrorist Financing.

<b>Permenkumham number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries</b>	<b>Method</b>
<b>Due Diligence of Service</b>	Identifying service users and verifying the identity of service users using reliable independent source documents, data or information.

<p><b>Users (Chapter II, Chapter III)</b></p>	<p>Identify the beneficial owner and take reasonable steps to verify the identity of the beneficial owner, so that the notary can be sure that they know who the beneficial owner is. For legal entities and other legal acts, this includes notaries in understanding the ownership status and control structure of the service user.</p> <p>Understand, as appropriate, in obtaining information about the purpose and nature of the service user's business relationship.</p> <p>Conduct due diligence on ongoing business relationships and close supervision of transactions carried out throughout the business relationship to ensure that transactions carried out are consistent with the notary's knowledge of service users, business profiles and risks, including, if necessary, the origin of the source of funds. This obligation should be understood in the case of a long-term business relationship involving a notary, whereas in occasional transactions it is not necessary.</p>
<p><b>Permenkumham number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries.</b></p>	<p><b>Method</b></p>
<p><b>Obligation to Keep All Records and Documentation, Conventionally and Electronically (Article 22, Article 23)</b></p>	<p>FATF recommendations require that notaries keep at least five years (this rule varies by country): for all records obtained for compliance with due diligence obligations (eg copies of records of official identification documents such as passports, identity cards, driver's licenses or similar documents), including analysis results carried out early (for example, comprehensive background and objective check questions regarding the value of unusually large transactions) as well as after the transaction. Notaries are also required to keep all necessary records of transactions made with service users, both local and international so that they are available if required by the authorities or authorities. Information and transaction records resulting from due diligence by a notary must be made available to the local authorities in charge of this matter.</p>
<p><b>Permenkumham number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries.</b></p>	<p><b>Method</b></p>
<p><b>Obligation of Deep Identification of</b></p>	<p>This obligation means that notaries, in addition to ensuring that they identify whether the service user or beneficial owner is a politically</p>

<p><b>Politically Exposed Persons (Article 17 points (2), (3) and (6))</b></p>	<p>well-known person or a Politically Exposed Person (PEP), must register due diligence steps that are even more strengthened. This implies, first of all, that a proper risk management system must be in place to determine whether the service user or beneficial owner is a politically well-known person, a notary must understand and understand this kind of situation at the time of carrying out transactions with service users. and must adopt appropriate and careful steps to determine where the assets come from and the origin of the funds that the service user wants to use in transactions. The requirement for a politically well-known person or Politically Exposed Person (PEP) must also apply to family or close members. The closest associates of someone who is politically famous or a Politically Exposed Person (PEP).</p>
<p><b>Permenkumham number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries.</b></p>	<p><b>Method</b></p>
<p><b>Implementation of Notary Office Internal Control Measures (Article 27, Article 28, Article 29)</b></p>	<p>This internal control program means that notaries are obliged to:</p> <ul style="list-style-type: none"> <li>• Establish Anti Money Laundering / Counter Terrorist Financing policies and procedures that will apply to their offices, including adequate screening procedures to ensure high standards when hiring Employees. Develop and maintain ongoing internal and external employee training.</li> <li>• Establish internal verification procedures to self-assess system operation.</li> </ul> <p>It is hoped that these internal control measures will prevent the prevention of money laundering and funding of funds.</p>
<p><b>Permenkumham number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries.</b></p>	<p><b>Method</b></p>
<p><b>Reporting Suspicious Financial Transactions (Article 24 number (2), Article 32)</b></p>	<p>Obligations of a notary if he suspects or has reasonable reason to suspect that the funds are the result of criminal activities, or are related to terrorist financing, the notary must report it to the competent authority or INTRAC for this matter. The obligation to report suspicious transactions also includes anti-tipping off to service users or third parties that the report is being submitted to the competent authority regarding this matter.</p>

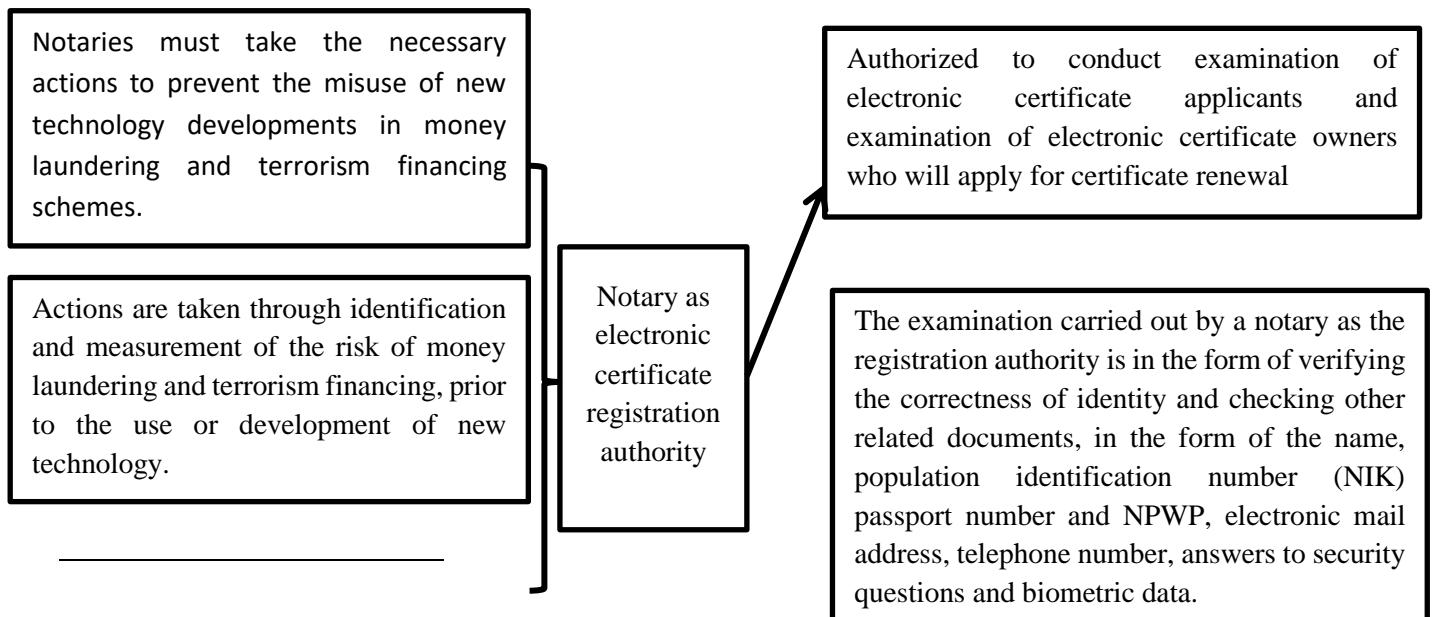
More specifically regarding the Existence of Notaries in Supporting Electronic Transaction Security Systems Related to Money Laundering and Terrorism Financing, Article 31 points (1), (2) and (3) of the Minister of Law and Human Rights Number 9 of 2017 states:

1. Notaries must take necessary actions to prevent misuse of new technology development in money laundering and terrorism financing schemes.
2. The necessary actions as referred to in paragraph (1) are carried out through identification, verification and measurement of the risk of money laundering and terrorism financing, before the utilization or development of new technology.
3. Notaries must manage and mitigate the risks of developing new technologies.

In realizing a notary and the development of new technology, the Minister of Communication and Information Technology Regulation Number 11 of 2018 concerning the Implementation of Electronic Certification (Permenkominfo Number 11 of 2018)<sup>15</sup> provides delegation of authority to a notary, in Article 27 and Article 28 in the form of:

“Notary as the registration authority to conduct inspections of electronic applications and check the owners of electronic certificates who will apply for certificate extensions.”

The examination carried out by a notary as the registration authority is in the form of verifying the correctness of identity and checking other related documents, in the form of the name, population identification number (NIK), passport number and NPWP, electronic mail address (electronic mail), telephone number, answers to security questions. question) and biometric data. Interoperability between the Application of the Principle of Recognizing Service Users for Notaries (Permenkumham number 9 of 2017) and a Notary as a registration authority authorized to conduct inspections, identity verification and other related documents, for legal subjects before taking legal actions electronically (Permenkominfo Number 11 Years) 2018) are gatekeepers of the notary function in preventing money laundering and terrorism financing, which is also part of the requirements for Indonesia to become a member of the FATF.<sup>16</sup> As can be seen in Figure 2 below :



Notaries must manage and mitigate the risks of developing new technologies.



**Source :** Image analysis by researcher

**Picture. 2.** Existence of Notary Authority in Supporting Electronic Transaction Security System Related to Money Laundering and Terrorism Financing.

Electronic certificates themselves according to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UUITE)<sup>17</sup> are electronic certificates containing Electronic Signatures and identities indicating the status of legal subjects of the parties in the Transaction Electronic.

An electronic certified electronic signature has the power for legal subjects who sign electronic documents to not be able to deny ( Non- repudiation ) their signature in the legal act.<sup>18</sup> According to Jonathan Gerhard, the Head of the Electronic Certification Center, the National Cyber and Crypto Agency, a notary as a registration authority is the front line in verifying the correctness of identity before an electronic certificate is issued by an electronic certification authority (certification authority), in private electronic certification providers, the registration authority must be carried out by a trusted third party, namely a notary in examining and verifying the identity of the electronic certificate applicant, due to the potential for misuse of identity that can be carried out in the examination and verification stage by the registration authority, including certain entities in money laundering and terrorism financing.<sup>19</sup>

The Central Board of the Indonesian Notary Chamber (Notary Chamber of Indonesia), stated, in the Preamble Considering letter (b), Law Number 2 of 2014 dated concerning Amendments to Law Number 30 of 2004 concerning Notary Positions (UUJNP).<sup>20</sup> It is stated that the State gives the mandate and authority to a notary in ensuring legal certainty, legal order and legal protection to the public, in the field of civil law actions, including the position of a notary as a registration authority mandated by the Regulation of the Minister of Communication and Information Number 11 of 2018 Regarding the Implementation of Electronic Certification, to protect the public in safe conventional and electronic transactions when using the services of a notary.<sup>21</sup>

Furthermore, according to the Central Board of the Indonesian Notary Association, notaries as gatekeepers for money laundering and terrorism financing, the Government through the Financial Transaction Reports and Analysis Center (PPATK) 2021 has launched the Government Anti-Money Laundering (goAML) application for notaries as transaction reports suspicious finances.<sup>22</sup>

## CONCLUSION

Indonesian Notaries are non-government institutions that play an active role in helping to combat money laundering and terrorism financing. The Indonesian Financial Intelligence Unit (FIU), namely PPATK, mentions Indonesian notaries as gatekeepers to prevent money laundering and terrorism financing

through the authority granted by the Minister of Law and Human Rights Number 9 of 2017 concerning the Application of the Principle of Recognizing Service Users for Notaries. In the electronic transaction security system related to the prevention of money laundering and terrorism financing, notaries are given delegation authority through the Minister of Communication and Information Technology Number 11 of 2018 concerning the Implementation of Electronic Certification as the registration authority for electronic certificates (registration authority) authorized to conduct inspection, verification and identification of electronic certificate applicants, before taking legal actions electronically or electronically.

## REFERENCES

1. Herlien Budiono, Collection of Civil Law Writings, In the Field of Notary, Third Book, Bandung, Citra AdityaBakti, 2007, hlm 211.
2. Radman, K., Babaeian Jelodar, M., Ghazizadeh, E., & Wilkinson, S. (2021). Causes of Delay in Smart and Complex Construction Projects. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 13(4), 05021006.
3. Gregory N Mandel, 2007, History Lessons For a General Theory of Law and Technology, *Minnesota Journal of Law in Science and Technology*, Vol. 8.2, hlm 551 – 552.
4. The Asia Pacific Group on Money Laundering (APG), Anti-money laundering and counter-terrorist financing measures on Indonesia, Mutual Evaluation Report September 2018, p 148.
5. Look in <https://www.ojk.go.id/apu-ppt/id/berita-dan-kegiatan/info-terkini/Pages/Pelaksanaan-MER-terhadap-Indonesia-tahun-2019-2020.aspx>. accessed 21 July 2022.
6. <https://www.g20-insights.org/policy-briefs/monitoring-countries-commitment-against-illicit-financial-flows/>. accessed 21 July 2022.
7. International Union of Notaries (UINL) Activity Report Legislature 2017 – 2019, Jakarta, 2019, p 7.
8. The Asia Pacific Group on Money Laundering (APG), Anti-money laundering and counter-terrorist financing measures on Indonesia, Mutual Evaluation Report September 2018, Op.,cit., p 4.
9. Ministère de l'Action et des Comptes publics, France's Financial Intelligence Unit, Tracfin 2019 Annual Report, hlm 32-33.
10. Soerjono Soekanto, Sri Mamudji, Normative Legal Research A Brief Overview, Jakarta, RajaGrafindo Persada, 2015, hlm 35.
11. M. Natsir Kongah, PPAK Public Relations Substance Group Coordinator, Email: [natsir.kongah@ppak.go.id](mailto:natsir.kongah@ppak.go.id). Press conference PPAK © 2021 Nomor : 001/HM.02.03/VIII/2021.
12. 12. As for Article 2 point (4) Permenkumham number 9 of 2017.
13. 13. Article 2 number (2) Permenkumham number 9 of 2017.
14. International Union of Notaries, Good Practices On The Prevention Of Money Laundering And Terrorist Financing In The Notarial Sector, 2018,. hlm 5-7.
15. Permenkominfo Number 11 of 2018.
16. Circular Letter of the Center for Financial Transaction Reports and Analysis, Number 02 of 2019 concerning Guidelines for Implementing the Principles of Recognizing Service Users and Submitting Suspicious Financial Transaction Reports for the Profession.
17. Article 1 number (9) of the ITE Law.
18. Edmon Makarim, Notary and Electronic Transaction. Jakarta, Raja Grafindo Perkasa, 2013, hlm 41-42.
19. Interview with Researcher date 14-2-2022.



20. Fully Handayani Ridwan, Central Board of the Indonesian Notary Chamber (Notary Chamber of Indonesia), Interview with Researchers dated 15-3-2022.
21. Regulation of the Minister of Communication and Information Technology Number 11 of 2018.
22. <https://goaml.ppatk.go.id/Home/>, Retrieved 21 July 2022.