JURNAL AKTA
Volume 9 No. 4, December 2022
SINTA 2 by Nationally Accredited Journal,
Decree No. 164/E/KPT/2021

The Model Regulation of Know Your Customer Principles in Technology-Based Lending and Borrowing in Indonesia

Putri Purbasari Raharningtyas Marditia[*)]
[*)] Faculty of Law, Universitas Katolik Indonesia Atma Jaya
E-mail: putri.purbasari@atmajaya.ac.id

Ridani Faulika[**)]
[**)] Faculty of Law, Universitas Katolik Indonesia Atma Jaya
E-mail: ridanifa@gmail.com

Abstract. *The Financial Services Authority Regulation Number 77 /POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services does not provide details on the process of applying the know-your-customer principle. As Article 42 of the Financial Services Authority Regulation Number 77 /POJK.01/2016 only states that organizers are required to implement anti-money laundering and terrorism financing prevention programs in the financial services sector. Cases on users who can use many online loan applications (pinjol) unfairly, proves that there are loan companies disregarding the background, eligibility and ability of the borrower or known as credit scoring, which is the method used by a financing institution/bank in determining whether or not it is appropriate to receive a loan from the institution. Currently, the Financial Services Authority (OJK) itself has prepared a Draft OJK Circular Letter (RSEOJK) on Guidelines for the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs for Information Technology-Based Borrowing-Lending Service Providers which can be used as a basis for implementing KYC p2p lending activities in Indonesia. This research is conducted based on the above, the writing method is a normative juridical method with a statutory and conceptual approach. The purpose of this study is to provide an overview and analysis related to the implementation of KYC consisting of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD), which may provide better protection than previous regulations. Based on this, the writer is interested in doing this research*
Keywords: Customer; Information; Principles; Services; Technology.

1. INTRODUCTION

Indonesia still needs various kinds of regulations to support the development of Technology-Based Lending and Borrowing Information Services (referred to as LPMUBTI). Until now, Bank Indonesia has at least made a number of regulations related to fin-tech, namely: (1) PBI Number 18/40/PBI/2016 regarding the Implementation of Payment Transaction Processing; (2) PBI Number 19/12/PBI/2017 regarding to the Implementation of Financial Technology; (3) Board of Governors Regulations Number 19/14/PADG/2017 regarding the Trial (Regulatory Sandbox) of Financial Technology; (4) Board of Governors Regulations Number 19/15/PADG/2017 regarding Procedures for Registration, Submission of Information, and Monitoring of Financial Technology Operators.

While the Financial Services Authority (OJK) only issues Financial Services Authority Regulations Number. 77/POJK.01/2016 regarding LPMUBTI but the regulation is deemed insufficient to cover problems that may arise from the implementation of LPMUBTI, especially in the application of the know-your-customer principle (referred to as e-KYC). This principle needs to be applied as the main gateway to verify the correctness of the profiles of customers and prospective customers who will conduct business relations with bank or non-bank financial service providers. Furthermore, it is further regulated at SEOJK No. 6/SEOJK.05/2021 which is used as the basis for carrying out KYC p2p lending activities in Indonesia. Specifically in Roman IV number 5 SEOJK, KYC consists of: *Customer Due Diligence (referred to as CDD)* and *Enhanced Due Diligence (referred to as EDD).*[1]

CDD includes activities in the form of identification, verification, and monitoring carried out by the Operator, with the aim of ensuring that the business relationship or transaction is in accordance with the profile, characteristics, and/or transaction pattern of Potential Customers and Customers. Meanwhile, EDD is a more in-depth CDD action carried out by the Operator against a High-risk Potential Customer or Customer including PEP and/or in a high-risk area. Implementation of CDD and EDD through electronic systems. It is also known as electronic Know Your Customer or e-KYC. Quoting from Tempo, e-KYC is a procedure to identify and verify customer identity digitally or online. The process of e-KYC consists of a series of checks that are carried out in the first stage of communication with the client to verify that they are the correct person according to their identity.[2]

This regulation introduces the use of Electronic Video as a tool to identify and verify customer profiles as a material for assessing and implementing know-your-customer principles. On the other hand, the practice and implementation of these regulations face obstacles that do not match the needs that arise because although they have determined the criteria and components of the principle of knowing customers, they do not also regulate the stages and procedures for implementation or Standard Operations (SOP), the capacity of the electronic customer verification authority holder, as well as the basis of reference regarding the verification criteria and the limitations of the interpretation of suitability in assuming the verification criteria. So, it can be seen that the implementation of e-KYC in Indonesia is still in the development stage.

According to Claus Christensen, there are 4 models of e-KYC in the world, namely Hong Kong, Germany, Sweden, India and the United Kingdom.[3] Germany itself has a rule that is Geldwäschegesetz – GwG Money Laundering Act which regulates the implementation of KYC through CDD and EDD. Germany also has a special Circular which is used to carry out the identification and verification customer process via video

[1] Article 1 point 8 and number 9 of OJK Regulation Number. 12/POJK.01/2017 Regarding the Implementation of AML and CFT Programs in the Financial Services Sector, Prospective Customers are parties who will use the services of Financial Services Actors (PJK)

[2] https://bisnis.tempo.co/read/1393366/gandeng-nasabah-baru-cukup-5-menit-dengan-lintasarta-e-kyc/full&view=ok, accessed 12 November 2020, at 19.54

[3] https://www.regulationasia.com/the-four-e-kyc-models-around-the-world/, accessed 12 November 2020, at 20.06

conferencing, namely Circular 3/2017 (GW) - video identification procedures. Therefore, to be able to create a regulatory model that can support acceleration in the realization of the CDD and EDD implementation system, the author wants to study further about the CDD and EDD mechanism in the financial services authority circular number 6/seojk.05/2021 with circular 3 of 2017 in Germany with hope that it can be used as a study material in developing and formulating a model concept of regulation of know your customer principles in technology-based lending and borrowing in Indonesia**.**

2. RESEARCH METHODS

The method being used is normative legal research through **Model Regulation of Know Your Customer Principles in Technology-Based Lending and Borrowing in Indonesia. The research was conducted with a library-based approach that focuses on reading and examining primary and secondary legal sources. Primary legal sources are actual sources of law, namely laws and court decisions and regulations related to model regulation of know your customer principles in technology-based lending and borrowing in Indonesia. Meanwhile, secondary legal sources are materials that include commentary on the law discovered in legal literature and journals. The approach used by the author for this legal writing in this study a statutory approach.**

3. RESULTS AND DISCUSSION

Enforcement of CDD and EDD. CDD and EDD in banking are carried out in the context of implementing *prudential banking* principles to avoid suspicious financial transactions and protect banks from risks that may arise in the Bank's business activities, CDD can be repeated if there is a change in the risk value based on:[4] Transaction value increased significantly; A significant change in customer profile was found; information on Customer profiles available in the *customer identification file (CIF)* has not been accompanied by documents for verification. The Operator can perform EDD if it finds high-risk Customers and Potential Customers or *Politically Exposed Persons (PEP)* at the time of the implementation of the CDD.

3.1. CDD and EDD in Germany according to Geldwäschegesetz – GwG

Article (1) Section 12 of the GWG explains that the Operator identifies and examines parties as the implementation of e-KYC is carried out in 2 stages: identity verification through documents and Identity verification through video. In order to understand the implementation of e-KYC, it will focus on the following objectives:

a. Standardization of documents that support the implementation of identity verification through documents
b. Standardization of the implementation of identity verification through video
c. The location of implementation of identity verification
d. The identity verification officer

[4] Roman IV number 7 SEOJK Guidelines for the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs for Information Technology-Based Borrowing-Lending Service Providers

e. Conducting and Monitoring the implementation of identity verification

With the following description:
First, the arrangement for implementing identity verification through documents is carried out by distinguishing the provisions for individuals and legal entities as follows:[5] Personal Identity Verification, a valid official identity document that includes a photo of the holder and meets the passport and identification requirements in Germany, passport or identity card recognized or accepted under German provisions for foreign nationals. When identity will be verified using an electronic signature, then the signature needs to meet the requirements for electronic signature validation in accordance with Article 32 (1) of Regulation (EU) No 910/2014. Verification of the identity of a legal entity includes (a) Excerpts from commercial lists or cooperative association lists or comparable official lists or directories; (b) Formal documents or equivalent supporting documents or; (c) Documented inspection required by the entity itself over data in registers or directories. The Federal Ministry of Finance may consult with the Federal Ministry of the Interior and Community *(Bundesministerium des Innern),* to request further appropriate documents to verify identity through regulations that do not require approval from the *Bundesrat*."
Identity document verification is required to ensure that the document used as proof of identity contains optical security features that can be visually identified in white light. The optical security features which include: Hologram; Identigram; Kinematic structure; Personalization technology (Laser Engraving Images, Typography); *Window* (e.g. Personalized); Security thread (Personalized); Optical variable ink; *Security Printing* (Microlettering, *Guilloche* Structure). Through appropriate Information Technology program (IT), it must be ensured that the optical security features that are visually identifiable in white light during video identification match the form and content of the individual features found on the identity document (for example by comparing primary and secondary photos such as Identigrams, Laser Engraving Images, and others.) or one that matches a reference from the identity document database.
Officers also prepare questions to be used in obtaining variations of statements to match documents. Match documents must be assumed if the verification criteria of at least three security features selected at random from different categories in the list above for identification purposes and belonging to the identity document are met. In addition, institutions are required to ensure that the Location and Parties to the transaction are being held and carried out by all or one of them is a person who is domiciled in: Other member states of the European Union, or Contracting States in the European Economic Area or Third countries where the credit institution is subject to due diligence and record-keeping requirements that equivalent to the due diligence and record-keeping requirements set out in Directive (EU) 2015/849 and whose supervision is overseen in a manner consistent with Chapter IV Part 2 of Directive (EU) 2015/849.

Second, the arrangement for the implementation of identity verification through video is carried out based on BaFin[6] issued Circular 3/2017 (GW) - video identification procedures on video identification procedures that can be used by all entities required under the German Money Laundering Act (*Geldwäschegesetz*) subject to BaFin

[5] *Geldwäschegesetz* – GwG *Section* 12 (1)
[6] BaFin is a financial authority in Germany

supervision. This is intended to ensure safe identification and to ensure that identity verification uses a video identification procedure which is based on all domestic and foreign identity documents based on the optical security features of each of these documents. The requirements for carrying out identity verification through video are listed in another circular, namely: (a) Conducted by officers who have received training so that the officer understands the features of documents that are permitted in the video identification procedure which can be verified by means of video identification and applicable verification methods and is able to understand matters relevant to anti-money laundering and data protection regulations. Because prior to identification, the Customer to be identified must give their explicit consent to the entire identification process as well as photos or screenshots of them and their identity documents taken. This consent must be recorded / recorded explicitly in terms of Data Protection.

During visual identification, the person to be identified must tilt the document horizontally or vertically in front of the camera and perform additional movements as instructed by the officers. Verification of the validity and reasonableness of the data and information contained in the identity document must be carried out as part of the video identification procedure. Among other things, this includes checking whether the issuance date and expiration date of the identity document match each other. Another required element of the identification process is the automatic calculation of the check digits in the machine-readable zone and cross-checking the information provided with the information shown on the identity document. In addition, the digit orthography, authority code, and typography used must be checked to ensure correctness. The customer to be identified must share the full serial number of their identity document during video transmission.

Third, the location of implementation of identity verification, during the identification process, the implementation must be placed in a separate location with limited access. Video identification should be done simultaneously and without interruption. In addition, the image and communication sound quality must be sufficient to allow the identification process to take place. Security feature checks that have been categorized can be verified visually in white light as well as checks carried out to check whether documents have been damaged or manipulated are also carried out in this identification process. During the video transmission process, each Verification Officer must take a photo/screenshot that clearly shows the Customer to be identified as well as the front and back of the identity document used by that person for identification purposes and the information stored in this document.

Fourth, the verification officer for the customer to be identified. The verification officer must ensure the suitability and consistency of photographs and personal descriptions such as the date of issue of identity and date of birth on the identity document used in accordance with the person to be identified. The officer who conducts the verification must ask the Customer questions such as the place of birth date listed in the identity document with the aim that the Customer being identified knows that such a question is required in the identification process. The officer who conducts the verification must verify that all details about the person to be identified listed on the identity document match those known to the Operator and are available to the employee (if any). This identification mechanism is carried out at 2 steps including: (a) Simplified due diligence can be carried out on Customers who have a low risk of Money Laundering and Terrorism Financing, especially those relating to customers, transactions and services or products that only require simplified due diligence requirements. Prior to

implementing SDD requirements, the Operators are required to ensure that the business relationship or transaction actually contains a lower risk of money laundering or terrorist financing. The Officer will ensure oversight of transactions and business relationships in such a way as to enable them to identify and report unusual or suspicious transactions. (b) *Enhanced due diligence* is carried out as a series of general due diligence. This is done through risk analysis or taking into account the determined risk factors. Organizers are required to determine the extent to which specific actions should be taken according to the higher risk of money laundering or terrorist financing.

Fifth, Verification Implementation and Supervision includes provisions for Termination of the video identification process; Transmission sequence number; Retention and record keeping; Data protection. With the following description: Termination of the video identification process, the identification process can be stopped if the video quality does not meet the requirements, for example lack of lighting, lack of image or video quality and/or verbal communication cannot be done. If such a situation occurs, then verification by other means is allowed as long as it is in accordance with *Geldwäschegesetz;*

Transmission sequence number, During the video verification, the Customer who will be identified must directly enter the number sequence through online system which is only valid for this purpose, created centrally and sent to the Customer (via email or SMS) by the Employee who performs the verification and must immediately reply to the Transmission sequence number to Employees electronically in order to complete the identification process; Retention and recording, the identification process for the Customer must be documented by the Operator or a Third Party appointed by the organizer or involved to carry out this identification process in accordance with Section 7 (2) GwG and Section 7 (1) GWG; The requirement for Documentation require visual, sound recording and complete storage procedures, therefore the Customer must be asked for the Customer approval in the documentation process. Records must be retained for five years in accordance with Section 8(3) GwG; Data protection The above-mentioned surveillance requirements apply despite of any other requirements to be complied with pursuant to sections 7 and 8 of the GwG and without prejudice to data protection requirements which must be complied with in parallel.

3.2. Comparison of Customer Due Diligence and Enhanced Due Diligence in Information Technology-Based Lending and Borrowing Service Providers in Indonesia - in Germany

SEOJK 6/2021 and Circular 3/2017 GW both regulate the implementation of the verification process for Customers and Prospective Customers using electronic video facilities. However, there are things that have not been regulated in detail in SEOJK 6/2021 but have been regulated in Circular 3/2017 which will then be presented in Table 1.

Table 1. comparison between SEOJK 6/2021 and Circular 3/2017 GW regarding the implementation of customer and prospective customer verification via electronic video
Source: Primary data, 2020 (Edited).

Indicator	SEOJK 6/2021	*Circular* 3/2017 GW
Approval of Customers and Prospective	SEOJK 6/2021 does not regulate requests for approval made by officers	Regulates requests for approval by officers who verify customers and

Customers in order to document the verification process via electronic video	who verify customers and prospective customers to carry out documentation during verification activities.	prospective customers to carry out documentation during verification activities.
Verification is carried out by officers who have received prior training	Does not regulate verification activities to Customers and Prospective Customers are carried out by Officers who have received prior training.	Officers who carry out verification activities to Customers and Prospective Customers have received prior training.
The scenario of match verification	Does not regulate the criteria regarding the scenario of match verification that carry out the verification process via electronic video. To provide additional confidence for the Operator, verification carried out electronically by the Operator may utilize artificial intelligence technology, or an algorithm that is matched with the Operator's database.	Regulate in detail the verification criteria and specifying the condition of suitability should be assumed if the verification criteria of at least three security features selected at random from different categories in the above list for identification purposes and belonging to the identity document are met.

Based on the Table 1, there are 3 indicators that distinguish SEOJK 6/2021 with Circular 3/2017 GW in the implementation of identification and verification of Customers and Potential Customers carried out by the Operator. SEOJK 6/2021 Roman IV number 13 Letter b (6) regulates that in conducting CDD, Operators are required to document Customers who receive simplified CDD treatment which also contains information regarding the reasons for determining the risk of the Customer so that it is classified as a low-risk Customer and gets *simplified CDD* treatment. However, OJK does not stipulate that before documenting customer and prospective customer information, the Operator asks the willingness of the customer and prospective customer to document verification via electronic video.

Implementation contrary to Law (UU) no. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Electronic Transaction Information (UU ITE) Article 26 Paragraph (1) which regulates that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned unless otherwise regulated by legislation.

SE-OJK 6/2021 Roman IV number 9 letter (g) Number 1 (c) regulates that in the case of the Provider conducts an electronic verification process, a third party must obtain approval from the Financial Services Authority in order to carry out face-to-face verification using electronic means belonging to the third party. SEOJK 6/2021 Roman IV number 9 number (1) letter (d) arranges that in conducting electronic verification, in order to give a sense of belief for the Operator in carrying out the face to face verification process through electronic means as referred to in letter a), The Operator may add to the use of motion detection mechanisms and/or technology to ensure that the Prospective Customer or Customer is a living subject and there are no attempts at identity fraud. Meanwhile, in number (2) letter (c) to provide additional sense of belief

for the Operator in the non-face to face verification process, the Operator may: (1) adding another authentication factor, namely *what you know*, which can include Personal Identification Number (PIN), password, one-time password (OTP), and/or challenge-response; and/or (2) adding the use of motion detection technology to ensure that the Prospective Customer or Customer is a living subject and that there is no attempt at identity fraud. However, SEOJK 6/2021 does not regulate the scenario where verification is said to be suitable in carrying out the verification process via electronic video.

3.3. Model Regulation of Know Your Customer Principles in Technology-Based Lending and Borrowing in Indonesia

The implementation of CDD and EDD activities in the management of LPMUBTI is given to Prospective Customers who wish to apply for loans to the Operator. This right is a form of implementation of Know Your Customer Principles carried out by the Operator. According to Roman I number 1 letter (q) EDD will only be carried out if the Prospective Customer meets the criteria as a high-risk customer, including a *Politically Exposed Person* (PEP) and/or is in a high-risk area. In practice, most LPMUBTI Operators only carry out the identification and verification process through CDD. This is adjusted to the requirements set by each Operator. Although OJK has regulated the process of implementing CDD and EDD in SEOJK 6/2021, in its implementation, there are still differences in criteria between one Provider and another. At Company X loan applications can be made in the following ways:

1. Prospective Customers shall download the Company X application on their *smartphone*, in this case, Prospective Customers can download the application through Playstore
2. Prospective customers must register and fill in complete personal data in the Company X application
3. Prospective Customers prepare Identity cards and bank accounts in the name of Prospective Customers
4. Prospective Customers take a recent photo of themselves while holding their Identity cards. Photo must be clear
5. Company X will perform facial recognition and Identity cards automatically using the software
6. Prospective Customers are required to have a bank account in accordance with the Prospective Customer's full name listed on Identity cards. This is intended so that Company X can send funds borrowed by the Prospective Customer to the registered bank account if the loan application made by the Prospective Customer is approved by Company X.

Based on the explanation above, can be observed that the CDD process carried out by Company X refers to Roman IV point 9 points (2), namely *non-face to face* verification which can be described as follows:[7]

1. *Non-face to face* verification is carried out using software belonging to the Operator with hardware belonging to the Operator or hardware belonging to the Customer or Prospective Customer.
2. *Non-face to face* verification is required to utilize population data that fulfills Two Factor Authentication. What is meant by "Two Factor Authentication" includes:

[7] Roman IV point 9 letter G number (2) SEOJK Guidelines for the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs for Information Technology-Based Borrowing-Lending Service Providers

a. *What you have*, namely identity documents owned by Prospective customers; And
b. *What you are*, namely bio-metric data, among others in the form of fingerprints, irises belonging to Prospective Customers, and/or facial recognition technology. Access to population data can be obtained by referring to the laws and regulations governing the granting of access rights and utilization of population data, which can be accessed through *web services*, *web portals*, and *card readers*.

3. To provide additional sense of belief for the Operator in the non-face to face verification process, the Operator may:
   a. Adding another authentication factor, namely what you know, which can include personal identification number (PIN), password, one-time password (OTP), and/or challenge-response; and/or
   b. Added the use of motion detection technology to ensure that the Prospective Customer or Customer is a living subject and there are no attempts on identity fraud.

At Company Y, the application for the loan process can be done with the following steps:

1. Prospective Customers are required to download the Company Y application on their *smartphone*
2. Prospective Customers are required to complete personal data information according to the questions in the Company Y application
3. Prospective customers choose the amount and duration of the loan
4. Prospective customers need to wait for the system to review the loan request
5. Prospective Customers will receive loan funds into the Prospective Customer's bank account

In the credit application process, Company Y will make phone calls to the prospective customer and the party listed as an emergency contact by the prospective customer for data verification purposes. This is considered odd because of the provisions regulated in SEOJK 6/2021 Roman IV point 9 points (1) that the Operator can verify electronically by means of face-to-face meetings (*face to face* verification) which can be used using the video call feature to ensure correctness. data used by prospective customers in applying for loans.

The ease of the verification process for Prospective Customers offered by the Loan Provider can also be a lose-lose situation. On the one hand, this is in accordance with the principle offered by LPMUBTI, namely ease of access by the public. However, on the other hand, it can have legal consequences. Although Verification of Prospective Customer data can be done *non-face to face* only by checking identity cards, this is not enough to ensure that Prospective Customer data is valid. This is due to the rise of cases of personal data trading on the internet.

Based on the description of the stages and analysis, note that such implementation must be supported and synchronized in its implementation, especially in the provision of Standardization of Documents that support the implementation of identity verification through documents; Standardization of implementation of identity verification through video; Location of Verification; Verification implementation officer; Verification Implementation and Monitoring.

4. CONCLUSION

The verification and identification of Customers and Prospective Customers can be done via electronic video. Germany has established guidelines for carrying out verification and identification of Customers and Potential Customers have been stated in *Circular 3/2017 GW* which regulates the procedures for implementing such verification and identification. Indonesia is still referring to SEOJK 6/2021 in verifying and identifying customers and prospective customers through electronic videos with a focus on providing Standardization of Documents that support the implementation of identity verification through documents; Standardization of implementation of identity verification through video; Location of Verification; Verification implementation officer; Verification Implementation and Monitoring.

5. REFERENCES

Journals:

Imanuel Adhitya Wulanata C, *SWOT Analysis of Implementation of Financial Technology Against the Quality of Banking Services in Indonesia*, Economy and Business, Vol. 20 No. 1, April 2017.

Irma Muzdalifa, Inayah Aulia Rahma, Bella Gita Novalia, *The Roles of Fin-tech in the Improvement of Inclusive Financial of UMKM in Indonesia (Shariah Financial Approach)*, Masharif al-Syariah Journal: Journal of Shariah Banking and Economy Vol. 3, No. 1, 2018, p. 7-8.

Dedi Rianto Rahadi, *FINANCIAL TECHNOLOGY It Is An Emerging Industry That Uses Technology To Improve Activities In Finance*, Bogor, 2020, p. 60-61

Sugangga Ryan, Erwin Hari Sentoso, Legal Protection Against Illegal Online Lending Users, Volume 01, No 01, January-June 2020, p. 57

Neni Sri Imaniyati, *Money Laundering within the Perspective of Banking and Islamic Law*, Bandung: Unisba, 2005, p. 104-105

Khemal Pratama Sumba, LEGAL ASPECT OF BANKING LOAN DISTRIBUTION ACCORDING TO LAW NO 10 OF 1998 REGARDING BANKING, Lex Administratum, Vol. V/No. 1/Jan-Feb/2017, p. 67-68

Niniek Wahyuni, S.H.,M.Hum, IMPLEMENTATION OF 5C PRINCIPLES IN LOAN DISTRIBUTION AS BANK PROTECTION, Lex Journal: Law & Justice Studies, Vol 1, No 1 (2017)

Claus Christensen, The Four e-KYC Models Around the World, accessed 27 November 2020, at 13.31

Erdiansyah, *Implemetation of Know Your Customer Principles as a form of Bank Role in Anticipating Money Laundering to PT Bank Negara Indonesia (Persero) Tbk* Pekanbaru Branch, Law Journal Vol.3, No.1, p. 7

Asep Rozali, *Know Your Customer Principle) in Banking Practices*, Law Studies Journal, Vol. 24 No. 01 February 2011, p. 304

Lim Kek Cheng Patrick, "*Anti Money Laundering + Know Your Customer = Plain Business Sense*", Insight To A Changing World Journal, Volume 2008 Issue 3, p.49.

Alis Yulia, *Know Your Customer Principle by Financial Service Provider in Capital Market Sector,* Volume 9, No. 1-March 2019, p. 5

Jaya, Hendro K., & Purnawan, Amin. (2020). *Review Of The Implementation Process Of Completion Of Juridical Code Violations Of Notary In Kendari*. *JURNAL AKTA*: Vol.7, No. 2, p. 169-176. Retrieved from http://jurnal.unissula.ac.id/index.php/akta/article/view/7881

Books:

Bambang Sunggono, *Introduction Banking Law*, Bandung: Mandar Maju, 1995, p.11-16

Djumhana Muhammad, Banking Law in Indonesia, PT Citra Aditya Bakti, Bandung, 2012, p. 50

Hermansyah, *Hukum Perbankan Nasional Indonesia,* Kencana Prenada Media Group, Jakarta, 2014, p. Ix

Husnawati, *ANALIYSIS OF IMPLEMENTATION OF KNOW YOUR CUSTOMER PRINCIPLES TO BANK ACEH SYARIAH BANDA ACEH*, p. 48

Jamal Wiwoho, *Indonesian Banking Law*, Surakarta: UNS Press, 2011, p. 52

Jonker Sihombing, *Financial Service Authority, concept, Regulation and Implementation*, Ref Publisher, Jakarta, 2012, p. 51

Uswatun hasanah, *Banking Law*, Malang: setara press, 2017, p. 21-24

Sri Susilo Y, et.al., Bank and Other Financial Institution*, Jakarta: Salemba Empat*, 2000, p. 127

Zulkarnain Sitompul, *Efforts on Preventing and Eradicating Money Laundering*, Sinar Grafika, Jakarta, 2004, p. 29.

Regulations:

Bank Indonesia Regulation Number 19/12/PBI/2017 concerning Implementation of Financial Technology

Attachment to Circular Letter of Bank Indonesia No. 15/21/DPN dated June 14, 2013 concerning Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs for Commercial Banks

Financial Services Authority Regulation Number 12 /POJK.01/2017 concerning the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs in the Financial Services Sector

SEOJK Guidelines for the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs for Information Technology-Based Money Lending and Borrowing Service Providers

Internet:

Yogie Maharesi, **Fintech and Transformation of Financial Industry,** https://www.pwc.com/id/en/media-centre/pwc-in-news/2017/indonesian/fintech-dan-transformasi-industri-keuangan.html, accessed 24 November 2020, at 23.13

https://www.ojk.go.id/id/kanal/iknb/financial-technology/Pages/-Penyelenggara-Fintech-Terdaftar-dan-Berizin-di-OJK-per-14-Agustus-2020.aspx, accessed 24 November 2020, at 23.15

Fahira Nabila, **Understanding the Types of *Financial Technology,*** https://smartlegal.id/smarticle/2019/01/08/mengenal-jenis-jenis-financial-technology/, accessed 24 November 2020, at 23.17

Noviyanto, growth of *Peer to Peer Lending (P2P Lending)* in China, https://koinworks.com/blog/pertumbuhan-p2p-lending-di-china/, accessed 26 November 2020, atl 14.34

Abdul Rasyid, FINTECH REGULATION IN CHINA, https://business-law.binus.ac.id/2016/10/31/regulasi-fintech-di-china/, accessed 25 November 2020, at 14.46

Allen Taylor, German Alternative Lending Market: An Overview, https://lending-times.com/2017/12/06/german-alternative-lending-market-an-overview/, accessed 26 November 2020, at 21:48

https://ekonomi.kompas.com/read/2018/03/09/205533926/ini-cara-membedakan-fintech-peer-to-peer-lending-dengan-payday-loan accessed 18 Agustus 2019

https://koinworks.com/blog/ketahui-tentang-peer-peer-lending/ acessed 18 Agustus 2019

https://bisnis.tempo.co/read/1393366/gandeng-nasabah-baru-cukup-5-menit-dengan-lintasarta-e-kyc/full&view=ok, accessed 12 November 2020, at 19.54

https://finansial.bisnis.com/read/20190325/89/904258/uang-teman-dan-investree-siapkan-strategi-e-kyc, accessed 12 November 2020, at 19.59

https://www.regulationasia.com/the-four-e-kyc-models-around-the-world/, accessed 12 November 2020, at 20.06

Fintech or FinTech is an acronym of Financial Technology meaning a computer and other technology used for supporting or activating banking and financial services, http://binus.ac.id/malang/2017/09/mengenal-fintech-sebagai-inovasi-bisnis-keuangan/, accessed pada 18 Agustus 2019

Bank Indonesia, What is financial technology?, accessed from https://www.bi.go.id/id/edukasi-perlindungan-konsumen/edukasi/produk-dan-jasa-sp/fintech/Pages/default.aspx, accessed 25 November 2020, at 22.16

ONLINEPAJAK, OJK: History, Function, Rules and Institution Structure, https://www.online-pajak.com/otoritas-jasa-keuangan, accessed 25 september 2019, at 20.59

FAQ Financial Services Authority, https://www.ojk.go.id/id/Pages/FAQ-Otoritas-Jasa-Keuangan.aspx, accessed 25 september 2019, at 20.55

https://m.hukumonline.com/berita/baca/ lt5bb4adade68803/simak-ulasan-notaris-soal-perbedaan-oss—ptsp—ahu-online-dan-sisminbakum, accessed on 24 March 2020