GUIDANCE OF CUSTOMER DUE DILIGENCE PRINCIPLE

Non-Bank Payment System Service Provider & Non-Bank Money Changing Service Providers

Department of Policy and Payment System

June 2020

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1
Introduction

Chapter 1 | Introduction

1.1. Background

1. The rapid development of technology and information systems has created various payment system innovations. Innovation has led to more complex products, services, transactions and business models, thereby intensifying the risk of money laundering and/or terrorism financing. The risks faced must be offset by higher quality and more effective anti-money laundering and/or counter-terrorism financing measures in terms of payment system services and exchange foreign currencies.
2. Pursuant to Article 3 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Counter-Terrorism Financing for Non-Bank Payment System Service Providers and Non-Bank Money Changers (PBI AML/CFT), one requirement of AML/CFT implementation are written policies and procedures for the Service Providers.
3. Furthermore, Article 6, paragraphs (1) and (2) of the PBI AML/CFT state that Service Providers are required to have, implement and develop written policies and procedures to manage the risk of Money Laundering and Terrorism Financing. The written policies and procedures must at least contain the following elements:
   (i) Customer Due Diligence (CDD);
   (ii) Data, information and document management; and
   (iii) Suspicious Financial Transactions Report (STR) and other reports.
4. Article 13 and Article 14 of the PBI AML/CFT as well as FATF Recommendation 10 (CDD) state that Service Providers must conduct customer due diligence on Service Users to ensure effective AML/CFT implementation. CDD implementation procedures include identification, verification, ongoing due diligence and understanding the purpose and intention of business relationships or transactions processed as well as the funding sources used.
5. CDD implementation referred to in Point 4 consists of the following activities:
   a. identifying Service Users, parties acting for and on behalf of Service Users and/or the Beneficial Owners of Service User transactions;
   b. verifying the identity of Service Users, parties acting for and on behalf of Service Users and/or the Beneficial Owners of Service User transactions based on data, information and/or documents from independent and reliable sources;
   c. conducting ongoing due diligence and updating the data, information and/or documents concerning the Service User; and

d. understanding the purpose and intention of business relationships or transactions processed as well as the funding sources used.

6. Based on Article 14, Article 29 and Article 31 of the PBI AML/CFT as well as FATF Recommendation 10 (CDD), there are three types of customer due diligence, namely simplified CDD, standard CDD and enhanced CDD (Table 1.1).

Table 1.1 CDD Types

Process	Simplified CDD	Standard CDD	Enhanced CDD
Conditions	Under CDD with low risk: Service Users in the form of Public Companies or State Institutions; Products with limited transactions and features	Service Providers undertake business relationships with Service Users under standard conditions	Under CDD with high risk: Service Users in the form of Politically Exposed Persons (PEP); Products/Services using high-value cross-border transfers or unlimited online transactions
Identification	Simplified request for information and supporting documents to identify name, ID number, address, place/date of birth and signature.	Identification through request for information and supporting documents (name, ID number, address, place/date of birth, nationality, telephone number, employment details, gender and signature).	Standard identification procedure with additional information on source of funds/wealth, asset value/income, position/business activity.
Verification	Verify the accuracy of the identity after establishing a business relationship while the transaction limit is restricted.	Verify the accuracy of the identity before establishing a business/transaction relationship	Verify the accuracy of the identity before establishing a business/transaction relationship through a face-to-face meeting
Ongoing Due Diligence	Reduce the frequency of ongoing due diligence and data updates	Periodic due diligence and data updates	Tighter due diligence and deeper analysis, while increasing the frequency of data updates
Understanding the purpose and intention of the business relationship	Understand the purpose and intention of the business relationship with a Service User based on specific analysis of transactions and/or products/services as determined by the Service Provider	Direct request by the Service Provider for information regarding the purpose and intention of the business relationship /transaction and funding sources to the Service User or collect such information through other relevant means if the accuracy can be verified.	Collect additional information regarding the purpose and intention of the business relationship /transaction Collect additional information regarding source of funds and wealth

7. Based on Article 15 of the PBI AML/CFT as well as FATF Recommendation 10 (CDD), Service Providers are required to conduct CDD procedures when:
   a. establishing a business relationship with a Service User or Potential Service User;
   b. processing a financial transaction denominated in rupiah and/or a foreign currency exceeding Rp100 million or equivalent;
   c. processing a Funds Transfer transaction;
   d. receiving indications of a Suspicious Financial Transaction relating to Money Laundering and/or Terrorism Financing; or
   e. there is doubt to the veracity of the information submitted by a Potential Service User, Service User, Authorised Party and/or Beneficial Owner.
8. Based on FATF Recommendation 15 (New Technologies), Service Providers are required to:
   a. identify and analyse risks of money laundering and terrorism financing that may emerge before a product launch or when using a product due to business practices or new technologies; and
   b. manage and mitigate the risks.
9. Based on the elucidation of Article 16, paragraph (1) of the PBI AML/CFT, data and information for the identification process may be submitted directly or electronically.
10. Based on Article 21, paragraphs (1) and (2) of the PBI AML/CFT, the verification process for CDD is as follows:
    a. Direct face-to-face or virtual meeting;
    b. Other appropriate methods or technologies accompanied by effective risk mitigation procedures and policies. Other appropriate methods include the use of biometric data and photographs submitted online in real-time. Other technologies and communication media can be used to verify the identity of Service Users.
11. Electronic Customer Due Diligence (electronic CDD) may be performed through online and mobile channels.

1.2. Purpose for Compiling the Guidelines

A prerequisite for enhancing the effectiveness of Customer Due Diligence is a universal perception and understanding amongst Service Providers, Service Users, relevant institutions and law enforcement concerning the implementation of conventional and electronic CDD. In general, the procedures and mechanisms of CDD implementation are regulated in accordance with the Bank Indonesia Regulation (PBI) on Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT). To facilitate greater understanding amongst Service Providers in terms of meeting and conducting customer due diligence as mandated by the

PBI on AML/CFT, CDD guidelines are required as a reference for Service Providers to conduct conventional and electronic CDD.

The CDD guidelines are a reference that must be followed by non-bank money changers (KUPVA BB), non-bank fund transfer service providers (PTD BB), non-bank card-based payment instruments (APMK BB), non-bank e-money issuers (UE BB) and non-bank e-wallet service provider (DE BB) limited to the funds held in the corresponding electronic wallet.

CHAPTER 2
Identification

Chapter 2 | Identification

2.1. Identification Procedure

1. Identification is achieved by a Service Provider through a request for data and information from the Potential Service User and Service User as elaborated in Table 2.1.

Table 2.1 Data and Information for Identification of Potential Service Users

No	Type of (Potential) Service User	Data and Information
1	Individual	1. Full Name, including aliases, and ID Number; 2. Residential address on ID document and other residential address if applicable; 3. Place and Date of Birth; 4. Nationality; 5. Telephone number; 6. Employment details; 7. Gender; and 8. Signature or biometric data.
2	Corporate	1. Name of corporation; 2. The form of legal entity or business entity; 3. Place and date of incorporation; 4. Business licence number; 5. Domicile address; 6. Type of business activities; 7. Telephone number; 8. Name of board of directors and board of commissioners; 9. Shareholders names; and 10. Information and data of natural person authorized to act for and on behalf of the Corporation.
3	Legal Arrangements	1. Name; 2. Licence number of authorised institution if applicable; 3. Domicile address; 4. Form of legal arrangements; and 5. information and data of natural person authorized to act for and on behalf of the other legal arrangements

2. For the identification of Potential Service Users and Service Users, Service Providers may request the identification documents detailed in Table 2.2

Table 3.4 Identification Document of Potential Service Users

No	Type of (Potential) Service User	Documents
1	Individual	1. Identification card (KTP); 2. Driving licence (SIM); 3. Passport; or 4. Documentation issued by a Government Institution.
2	Corporate	1. Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws with amendments if applicable; 2. Business license or other licence issued by relevant authority; 3. Taxpayer identification card (NPWP) for Service Users as required in accordance with prevailing laws and regulations; and 4. dentification documents of a natural person authorized to act for and on behalf of the Corporation
3	Legal Arrangements	1. Statement of registration at authorised institution; 2. Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws if applicable; 3. Individual identification documents: a. For trust law: i. A natural person authorized to act for and on behalf of the other legal arrangement; ii. Settlor; iii. Trustee; iv. Protector, if applicable; v. Beneficiary or class of beneficiary; and vi. Trustor; b. For other legal arrangements (excluding trust), in the form of a natural person identity having a position equal to or equivalent to a party in the trust referred to in Point a.

3. For the identification of Potential Service Users and Service Users initiating transactions of less than Rp100 million by a walk-in customer (no continuous business relationship), the Service Provider may request the Potential Service User or Service User to submit the data and information presented in Table 2.3. For the identification of Potential Service Users and Service Users detailed in the tables above, the Service Provider may request the Potential Service User or Service User to submit the identification documents detailed in Point 2.

Table 5.3 Data and Information for Identification of Walk-In Customers

No	Type of (Potential) Service User	Data and Information
1	Individual	1. Full Name, including aliases; 2. ID document number; 3. Residential address on ID document and other residential address if any; 4. Place and Date of Birth; and 5. Signature or biometric data.
2	Corporate	1. Name of corporation; 2. Address of registered office, if applicable; 3. Information and data of a natural person authorized to act for and on behalf of the Corporation.
3	Legal Arrangements	1. Name; 2. Address of registered office; and 3. Information and data of a natural person authorized to act for and on behalf of the other legal arrangements.

4. Service Provider may require Potential Service Users and Service Users to submit additional supporting data, information and/or documentation beyond that referred to in Points 1, 2 and 3 if there is doubt concerning the identity of the Potential Service User or Service User.
5. Identification of a Potential Service User or Service User in the form of a state institution, government institution, international institution or foreign representative is achieved by the Service Provider by requesting the Potential Service User or Service User to submit data, information and/or documentation in the form of institution or representative name and domicile. Documentation for the institution or representative is an appointment letter from a party authorised to represent the institution or representative in a business relationship.

2.2. Electronic Identification Procedure

1. Electronic identification is achieved, amongst others, through completion of an electronic form together with submission of softcopy documentation via the website or application of the Service Provider.
2. Through electronic identification, the Service Provider may collect additional data, information and/or documentation as required to electronically identify the Potential Service User or Service User, including email and selfie photo. Example data, information and documents that may be requested by the Service Provider to electronically identify a Potential Service User or Service User is presented in the following table.

Table 6.4 Data, Information and Documentation for Electronic Identification

No	Type of (Potential) Service User	Data, Information and Documentation
1	Individual	1. Full Name; 2. Email address; 3. Telephone number; 4. Softcopy of ID document (KTP, SIM, Passport, other official document issued by a government institution); 5. Selfie Photo.
2	Corporate	1. Name of corporation; 2. Email address; 3. Telephone number; 4. Softcopy of Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws with amendments if applicable; 5. Softcopy of business license or other licence issued by relevant authority; 6. Softcopy of taxpayer identification card (NPWP) for Service Users as required in accordance with prevailing laws and regulations; 7. Softcopy of management names and structure; 8. Softcopy of controlling shareholders' ID documentation; 9. Name, email address, telephone number, selfie photo and softcopy of ID documentation of a natural person authorized to act for and on behalf of the Corporation
3	Foundation Legal Arrangements	1. Name of corporation; 2. Email address; 3. Telephone number; 4. Softcopy of foundation operating license; 5. Description of foundation activities; 6. Softcopy of management names and structure; 7. Name, email address, telephone number, selfie photo and softcopy of ID documentation of a natural person authorized to act for and on behalf of the Foundation Legal Arrangements.
4	Non-foundation incorporated or unincorporated business entity	1. Name of corporation; 2. Email address; 3. Telephone number; 4. Softcopy of license issued by authorised institution; 5. Softcopy of Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws with amendments if applicable; 6. Name, email address, telephone number, selfie photo and softcopy of ID documentation of a natural person authorized to

No	Type of (Potential) Service User	Data, Information and Documentation
		act for and on behalf of the Non-foundation incorporated or unincorporated business entity.
5	Other Legal Arrangements	1. Name; 2. Legal arrangement; 3. Softcopy of license issued by authorised institution if applicable; 4. Softcopy of Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws with amendments if applicable; 5. Name, email address, telephone number, selfie photo and softcopy of ID documentation for the following individuals: a. For trust law: i. Individual identification documents of Person in Charge (PIC) of the legal arrangement; ii. Settlor; iii. Trustee; iv. Protector, if applicable; v. Beneficiary or class of beneficiary; and vi. Trustor; b. For other legal arrangements (excluding trust), individual identification documents, consisting of name, email address, telephone number, selfie photo and softcopy of ID documentation of a natural person authorized to act for and on behalf of other legal arrangements equivalent to the respective positions under trust law referred to in Point a.
6	State Institution, Government Institution, International Institution, Foreign Representative	1. Softcopy of name and address of institution or representative; 2. Softcopy of power of attorney document for a party authorised to represent the institution or representative in a business relationship; 3. Name, email address, telephone number, selfie photo and softcopy of ID documentation of party authorised to represent the institution or representative in a business relationship;

3. Specific to issuer of electronic money, the electronic identification process is necessary for Potential Service Users and Service Users intending to use registered electronic money or convert unregistered to registered electronic money.

CHAPTER 3
Verification

Chapter 3 | Verification

3.1. Verification

1. Based on the identity submitted by the Potential Service User or Service User during the identification process, the Service Provider is required to verify the accuracy of the information submitted by the Potential Service User or Service User as well as identify any irregularities or concerns based on the documents and/or other independent and trusted sources, while ensuring that the data submitted by the Potential Service User or Service User is up-to-date. The verification process assesses the accuracy of:

   a. identification documents issued by a government institution;
   b. population data and information administrated by a government institution; and/or
   c. biometric or electronic data only if the Service Provider can ensure data validity and reliability.

   In addition, during the verification process, the Service Provider must also refer to the List of Suspected Terrorists and Terrorist Organisations (DTTOT), List of Funding of the Proliferation of Weapons of Mass Destruction, Politically Exposed Person (PEP) data and/or other independent and trusted databases.

2. The verification process referred to in Point 1 can be executed through:

   a. Face-to-face meetings; and
   b. other methods.

   Direct meetings can be conducted face-to-face or through virtual meetings using video call technology, while other methods include photograph submission online and in real time.

3. Other verification methods referred to in Point 2 must be reported by the Service Provider to Bank Indonesia, accompanied by clarification concerning the verification method and technology used as well as the effective risk management policies and procedures implemented.

4. In the event of doubt, the Service Provider shall request the Potential Service User or Service User to provide more than one identification document issued by an authorised party to ensure accuracy.

5. The verification process must be completed by the Service Provider prior or during the establishment of a business relationship or settlement of a transaction with a Potential Service User or Service User.

6. The Service Provider may complete the verification process after establishment of a business relationship with a Potential Service User or Service User providing:
    a. the risk of Money Laundering and Terrorism Financing is effectively managed;
    b. such an arrangement is a common business practice; and
    c. the verification process can be promptly completed.

3.2. Electronic Verification

1. Service Providers implementing an electronic identification process must take measures to ensure the data and information is verifiably submitted by a Potential Service User or Service User, for instance using a One-Time Password (OTP) sent through Short Message Service (SMS) or email to the Potential Service User or Service User.
2. For electronic verification, the Service Provider is required to utilise the following technology:
    a. biometric technology to verify the Potential Service User or Service User against identification data issued by the Government;
    b. fraud detection technology to ensure the authenticity of the identification data and confirm verification of the Potential Service User or Service User;
    c. motion detection technology to ensure the Potential Service User or Service User is genuine with no attempt to impersonate another identity (during a video call);
    d. other information systems or technology, such as artificial intelligence or algorithms electronically paired to a database.
3. For issuer of electronic money, an electronic verification process is required for requests to use registered electronic money or to convert unregistered to registered electronic money.
4. The following aspects must be considered when converting unregistered to registered electronic money:
    a. If the electronic verification process fails, the Service User is still eligible to use unregistered electronic money;
    b. Upon electronic verification failure, the Service Provider is required to investigate whether there are elements of fraud or suspicious financial transactions. If fraud or suspicious financial transactions are detected, the Service Provider must submit a Suspicious Financial Transaction Report to the Indonesian Financial Transaction

Reports and Analysis Centre (PPATK) and initiate enhanced due diligence of the Service User's transactions.

CHAPTER 4
Identification and Verification of Beneficial Owners

Chapter 4 | Identification and Verification of Beneficial Owners

4.1. Identification and Verification of Beneficial Owner

1. The Service Provider is required to ensure the Potential Service Users or Service Users are acting for themselves or for the benefit of Beneficial Owner.
2. If a Potential Service User or Service User is acting on behalf of a Beneficial Owner, the Service Provider is required to identify and verify the Beneficial Owner.
3. If a Potential Service User or Service User is a Cooperation, the Beneficial Owner shall be determined by virtue of majority ownership in the Corporation.
4. In addition to identification and verification referred to in Point 2, the Service Provider is required to:
   a. examine the legal relationship between the Service User and Beneficial Owner;
   b. request a written statement from the Service User regarding the true identity and source of funds of the Beneficial Owner;
   c. request a written statement from the Beneficial Owner that the Beneficial Owner concerned is the true owner of the funds of the Service User.
5. The Service Provider may determine a Corporate Beneficial Owner beyond the purview of Point 2 in the event of:
   a. There is a doubt that an individual who owns a majority share is a Corporate Beneficial Owner; or
   b. no individual is found to have a majority share.
6. If the Corporate Beneficial Owner cannot be determined under the scope of Point 5, the Service Provider is required to identify and verify the identity of individuals appointed as Board of Directors or equivalent positions in the corporation. For a non-limited liability corporation, such as a foundation or collective, or a corporation not using shares as a measure of ownership, the Beneficial Owner is an individual assessed by the Service Provider with absolute authority or control over the corporation.
7. Identification of the Beneficial Owner is not required for the following Potential Service Users or Service Users:
   a. State or government institutions;
   b. majority state-owned enterprises; or
   c. public listed companies or issuers.

Table 4.1 Data, Information and Documentation for Identification and Verification of Beneficial Owner

No	Beneficial Owner of (Potential) Service User	Data, Information and Documentation
1	Individual	1. Name, telephone number, identification document of Beneficial Owner. For instance, for Service Users in the form of a student or housewife, the head of the household can be identified as the Beneficial Owner of the Service User; 2. A statement concerning the legal relationship between the Potential Service User or Service User with the beneficial owner, including family card, proof of employment, power of attorney authority to act as intermediary; 3. A written statement from the Potential Service User or Service User regarding the true identity and source of funds of the Beneficial Owner; 4. A written statement from the Beneficial Owner that the Beneficial Owner concerned is the true owner of the funds of the Potential Service User or Service User
2	Corporate	1. For a Beneficial Owner as an individual: Name, telephone number, identification document and tax file number (NPWP) of the Beneficial Owner; 2. For a Beneficial Owner as a corporation: Name of corporation, Telephone number, Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws, or business license of the Beneficial Owner; 3. A statement concerning the legal relationship between the Potential Service User or Service User with the beneficial owner, including family card, proof of employment, power of attorney authority to act as intermediary; 4. A written statement from the Potential Service User or Service User regarding the true identity and source of funds of the Beneficial Owner; 5. A written statement from the Beneficial Owner that the Beneficial Owner concerned is the true owner of the funds of the Potential Service User or Service User
3	Other Legal Arrangements	1. For other legal arrangements in the form of trust law: Name, telephone number, identification documents of the following individuals: a. Settlor; b. Trustee; c. Protector, if applicable; d. Beneficiary or class of beneficiary; and

No	Beneficial Owner of (Potential) Service User	Data, Information and Documentation
		e. Trustor; 2. For other legal arrangements (excluding trust): Name, telephone number, identification documents of individuals equivalent to the respective positions under trust law referred to in Point 1

4.2. Electronic Identification and Verification of Beneficial Owners

1. If a Service Provider implements electronic identification and verification of a Beneficial Owner, the process must refer to the electronic identification and verification process described in these guidelines.
2. To find out whether a Potential Service User or Service User is acting on behalf of a Beneficial Owner, the Service Provider may ask additional questions on the electronic form about whether the Potential Service User or Service User is acting in its own interest or on behalf of a Beneficial Owner.
3. Example data, information and documents requested by a Service Provider for the electronic identification and verification process of a Beneficial Owner are presented in the following table.

Table 4.2 Data, Information and Documentation for Electronic Identification and Verification of Beneficial Owner

No	Beneficial Owner of (Potential) Service User	Data, Information and Documentation
1	Individual	1. Name, telephone number, selfie photo and softcopy of identification document of Beneficial Owner. For instance, for Service Users in the form of a student or housewife, the head of the household can be identified as the Beneficial Owner of the Service User; 2. Softcopy of a statement concerning the legal relationship between the Potential Service User or Service User with the beneficial owner, including family card, proof of employment, power of attorney authority to act as intermediary; 3. Softcopy of a written statement from the Potential Service User or Service User regarding the true identity and source of funds of the Beneficial Owner; 4. Softcopy of a written statement from the Beneficial Owner that the Beneficial Owner concerned is the true owner of the funds of the Potential Service User or Service User

No	Beneficial Owner of (Potential) Service User	Data, Information and Documentation
2	Corporate	1. For a Beneficial Owner as an individual: Name, email address, telephone number, selfie photo, softcopies of identification document and tax file number (NPWP) of the Beneficial Owner; 2. For a Beneficial Owner as a corporation: Name of corporation, email address, telephone number, Deed of Establishment (DoE) and/or Articles of Association (AoA) and corporate bylaws, or softcopy of business license of the Beneficial Owner; 3. Softcopy of a statement concerning the legal relationship between the Potential Service User or Service User with the beneficial owner, including family card, proof of employment, power of attorney authority to act as intermediary; 4. Softcopy of a written statement from the Potential Service User or Service User regarding the true identity and source of funds of the Beneficial Owner; 5. Softcopy of a written statement from the Beneficial Owner that the Beneficial Owner concerned is the true owner of the funds of the Potential Service User or Service User
3	Other Legal Arrangements	1. For other legal arrangements in the form of trust law: Name, email address, telephone number, selfie photo, softcopy of identification documents of the following individuals: a. Settlor; b. Trustee; c. Protector, if applicable; d. Beneficiary or class of beneficiary; and e. Trustor; 2. For other legal arrangements (excluding trust): Name, email address, telephone number, selfie photo, softcopy of identification documents of individuals equivalent to the respective positions under trust law referred to in Point 1

CHAPTER 5
Ongoing Due Diligence

Chapter 5 | Ongoing Due Diligence

5.1 Ongoing Due Diligence

1. Ongoing due diligence is a process conducted by the Service Provider on the Service User to ensure transactions are in accordance with the profile of the Service User.
2. Service Providers conduct ongoing due diligence in terms of Enhanced Due Diligence through enhanced monitoring of the business relationship or transactions, including the determination of transaction criteria required for further analysis.
3. Service Providers are required to maintain adequate procedures to conduct ongoing due diligence as referred to in Point 1.
4. Service Providers with complex business scale and services are required to operate an effective due diligence system. Complex business scale and services are determined based on total office network, total Service Users as well as product variety and features. Ongoing due diligence can involve information systems or other monitoring methods.
5. Ongoing due diligence concerning Service User transactions and profiles includes the following activities:
    a. ensuring complete information and supporting documents from the Service User;
    b. effectively identifying, analysing, monitoring and reporting the profile, characteristics and/or usual transaction patterns of the Service User;
    c. tracing each transaction, as required, including the identity of the Service User, type of transaction, transaction date, transaction total and denomination as well as source of funds;
    d. analysing all transactions, particularly Suspicious Financial Transactions, including complex transactions, unusual totals or patterns, as well as ambiguous economic intentions;
    e. ongoing due diligence, including:
        i. transactions of Service Users engaged in a business relationship with a Service Provider without opening an account; and
        ii. transactions processed through the system or network of a Service Provider, for instance funds transfers.
    f. post-transaction due diligence is permitted within a certain period.

g. investigate and clarify any resemblance or similarity between the names and identities of the Service Users and those names and identities listed on the:
   i. List of Suspected Terrorists and Terrorist Organisations (DTTOT);
   ii. List of Funding of the Proliferation of Weapons of Mass Destruction;
   iii. Politically Exposed Person (PEP) data;
   iv. Suspects or defendants published in the mass media or by authorised parties; and
   v. Other independent and trusted databases.

h. If the name of a Potential Service User or Service User appears on the List of Suspected Terrorists and Terrorist Organisations (DTTOT) or List of Funding of the Proliferation of Weapons of Mass Destruction, referred to in Point g, the Service Provider is required to immediately freeze all funds and submit a Suspicious Financial Transactions Report, while taking the necessary follow-up actions in accordance with prevailing laws.

6. The Service Provider is required to administrate and update the List of Suspected Terrorists and Terrorist Organisations as well as the List of Funding of the Proliferation of Weapons of Mass Destruction in accordance with prevailing regulations concerning the prevention of terrorism financing and proliferation of weapons of mass destruction.

7. The Service Provider is required to evaluate/analyse its ongoing due diligence efforts to ensure elements of suspicious financial transactions are present.

8. The Service Provider may request information concerning the background and destination of any transactions that are unusual based on the Service User's profile in accordance with anti-tipping off legislation as stipulated in laws and regulations concerning the prevention and eradication of money laundering.

9. The Service Provider is required to submit a Suspicious Financial Transactions Report (LTKM) to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) upon detection of a suspicious financial transaction pursuant to PPATK regulations.

10. The Service Provider is required to administrate the results of its ongoing due diligence as well as evaluation/analysis efforts reported and unreported to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) in written form through formal documents, such as a memorandum or letter, as well as informal documents, such as email correspondence.

5.2 Updating Data as a Follow-Up Action to Ongoing Due Diligence

1. The Service Provider is required to update data, information and/or documents on Service Users, including the data, information and/or documents relating to customer due diligence (CDD).
2. The data, information and/or documents must be required in the event of:
   a. changes in the data, information and/or documents of the Service User or party authorised to represent the institution or representative;
   b. changes in the patterns of transactions, unusual transactions based on the Service User's profile or a significant increase in Service User risk; and/or
   c. suspicions of money laundering or terrorism financing.
3. The Service Provider must conduct CDD procedures concerning Service Users to update the data based on materiality and level of risk. The CDD is executed based on the duration of previous CDD and scope of the data collected.
4. The Service Provider must ensure that the data, information and/or documents collected during the CDD process remain up-to-date and relevant by reviewing the data, information and/or documents in possession, particularly for high-risk Service Users.
5. The data, information and/or documents of Service Users must be updated using a risk-based approach, including updating the Service User's profile and pattern of transactions. The data, information and/or documents are updated based on a priority scale.
6. When determining the priority scale, the Service Provider must prioritise the following criteria:
   a. high-risk Service Users;
   b. large and/or unusual transactions based on the Service User's profile (red flag);
7. The data, information and/or documents must be updated periodically based on the risk level of the Service User or transaction. For example, the data for high-risk Service Users must be updated biannually, or annually for medium-risk Service Users and biennially for low-risk Service Users.
8. All activities associated with updating the data, information and/or documents must be administrated by the Service Provider.

5.3 Ongoing Due Diligence and Updating Data Electronically

1. Ongoing due diligence and updating the data can be performed electronically by a Service Provider in order to increase the efficiency and effectiveness of the process.

2. Ongoing due diligence and updating the data electronically is relevant for Service Providers with complex business scale and services based on total office network, total Service Users as well as product variety and features.
3. Ongoing due diligence and updating the data electronically can be achieved using information systems or other monitoring methods in order to:
    a. effectively identify, analyse, monitor and report on the profile, characteristics and/or usual patterns of transaction of the Service User; and
    b. trace each transaction, as required, including the identity of the Service User, type of transaction, transaction date, transaction total and denomination as well as source of funds;
4. Other ongoing due diligence methods include the use of algorithms, specific parameters, artificial intelligence and regulatory technology (RegTech).
5. Service User data can be updated by through special features or notifications in the application to ensure the Service User updates its own data and information prior to the subsequent transaction.

CHAPTER 6
Enhanced Due Diligence

Chapter 6 | Enhanced Due Diligence (EDD)

1. Service Providers are required to conduct Enhanced Due Diligence for high-risk Potential Service Users, Service Users and Beneficial Owners.
2. Potential Service Users, Service Users and Beneficial Owners are considered high risk based on the following factors:
   a. Service User;
   b. country or geographic area;
   c. products or services; and
   d. delivery channels.
3. Service Providers are required to maintain policies and procedures to determine high-risk Potential Service Users, Service Users and Beneficial Owners.
4. Service Providers are required to maintain policies and procedures to recognise Potential Service Users, Service Users and Beneficial Owners categorised as Politically Exposed Persons (PEP).
5. Enhanced due diligence is required for PEP, at least in the form of identification and verification referred to in Chapters 2, 3 and 4 as well as:
   a. any measures necessary to determine source of funds; and
   b. enhanced monitoring with additional criteria concerning transaction patterns for further analysis.
6. If a Potential Service User, Service User or Beneficial Owner is categorised as a Politically Exposed Person (PEP), the Service Provider is required to conduct enhanced due diligence (EDD). EDD is applicable to foreign and domestic PEP as well as PEP in international organisations or with a prominent function in an international organisation, such as the International Monetary Fund (IMF), World Bank, United Nations (UN), Organisation for Economic Co-operation and Development (OECD), Asian Development Bank (ADB) and Islamic Development Bank (IsDB). EDD is also applicable to family members and close associates of the PEP.
7. Service Providers are required to appoint a Director or Executive Officer to be responsible for business relationships with high-risk Potential Service Users, Service Users and Beneficial Owners.
8. An example of enhanced due diligence (EDD) referred to in Point 1 is as follows:
   a. seek additional information concerning the high-risk Service User, Service User or Beneficial Owner in terms of:

i. employment, wealth or other publicly available information through the internet and periodically update the identity data of the high-risk Service User and/or Beneficial Owner;
ii. purpose of the business relationship and destination of previous and new financial transactions;
iii. source of funds or source of wealth.

b. regularly update identification data;
c. enhanced monitoring of business relationships or transactions, including the determination of transaction criteria for further analysis; and
d. request approval from the Director or Executive Officer to:
   i. approve or reject a high-risk Service User, Service User or Beneficial Owner;
   ii. decide whether to continue or terminate a business relationship with a high-risk Service User, Service User or Beneficial Owner.

9. Service Providers are required to maintain a list of Service Users subject to EDD.
10. In the event that the Service Provider conducts business relationships with Service User and/or conducts transactions originating from high risk countries published by the Financial Action Task Force on Money Laundering (FATF) for counter measures, the Service Provider is obliged to perform EDD by requesting confirmation and clarification to the relevant authorities.
11. Enhanced due diligence (EDD) referred to in Point 1 is also required if a Service Provider performs transactions with a Service User suspected of not having a licence from the relevant authority to conduct Funds Transfers and foreign currency exchange activities as well as provide other financial services.
12. If EDD of a high-risk Service User reveals unusual transactions based on Service User profile but a clear purpose or underlying asset is provided, ongoing due diligence should be conducted based on prevailing procedures. If no clear purpose or underlying asset is provided, the transaction must be reported as a Suspicious Financial Transaction and subject to enhanced due diligence.
13. The attributes, quality and quantity of information concerning high-risk Service Users and/or Beneficial Owners collected through enhanced due diligence (EDD) must provide a clear picture of the risks that may emerge from the business relationship.
14. The information collected must be verified and support the genuine profile of the high-risk Service User and/or Beneficial Owner.
15. Prevailing regulations for PEP, as referred to in Points 2, 3 and 4, are also applicable to family members and close associates of the PEP.

16. If a Service Provider conducts enhanced due diligence electronically, the process must refer to the electronic identification, verification, monitoring and data updating procedures described in these guidelines.

CHAPTER 7
Simplified CDD

Chapter 7 | Simplified CDD

1. Service Providers can conduct simplified customer due diligence for low-risk Potential Service Users, Service Users and Beneficial Owners.
2. Simplified CDD is conducted as follows:
   a. simplified requests for data and information concerning the identity of the Service User;
   b. verification of Service User identity after initiating a business relationship;
   c. verification of Service User identity upon reaching a balance or transaction threshold;
   d. lower updating frequency for Service User data;
   e. monitoring (on-going due diligence) of Service Users with a specific balance or transaction total; and/or
   f. understanding the purpose and intention of the business relationship with the Service User based on analysis of specific transactional patterns or product/service types as determined by the Service Provider.
3. The CDD procedure must be conducted proportionally to the low risk factors.
4. Service Providers are required to maintain policies and procedures to determine low-risk Potential Service Users, Service Users and Beneficial Owners based on the following factors:
   a. Service User;
   b. country or geographic area;
   c. products or services; and
   d. delivery channels.
5. Service Providers with effective risk mitigation policies and procedures may conduct simplified CDD. AML/CFT policies and procedures must contain criteria to determine low risk as well as procedures for simplified CDD.
6. Simplified CDD is not applicable in cases of suspected Money Laundering, Terrorism Financing and/or Financing the Proliferation of Weapons of Mass Destruction.
7. A list of Service Users eligible for simplified CDD must be maintained by the Service Provider. The list must contain information concerning the reasons and criteria for the low-risk designation.
8. Service Providers in the form of issuer of electronic money are not required to implement identification and verification when issuing electronic money:
   a. up to a specific value threshold, thus obviating the need to record the identification data of electronic money holders in accordance with Bank Indonesia regulations concerning electronic money; and

b. if not engaged in funds transfer activities.

9. If a Service Provider is conducting simplified CDD electronically, the process must refer to the electronic identification, verification, monitoring and data updating procedures described in these guidelines.

CHAPTER 8
Rejection and Termination of Business Relationships

Chapter 8 | Rejection and Termination of Business Relationships

1. Service Providers are required to reject business relationships and transactions, cancel transactions and/or terminate business relationships if:
   a. the Potential Service User, Service User and/or Beneficial Owner fails to meet data and information submission requirements in the identification process;
   b. the Service Provider knows or suspects that the Potential Service User, Service User and/or Beneficial Owner has used a fictitious name and/or alias; and/or
   c. the Service Provider is doubtful concerning the accuracy of the identity of the Potential Service User, Service User and/or Beneficial Owner.
2. Service Providers must document the identity of Potential Service Users, Service Users and/or Beneficial Owners referred to in Point 1 as supporting documentation for the Suspicious Financial Transactions Report (LTKM) submitted to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK).
3. Service Providers must report Potential Service Users, Service Users and/or Beneficial Owners referred to in Point 1 as part of the Suspicious Financial Transactions Report (LTKM).
4. The Service Providers' right to reject, cancel and/or terminate a business relationship with a Service User referred to in Point 1 must be stipulated in the account opening agreement and known to the Service User.
5. If a Service Provider terminates a business relationship referred to in Point 1, the Service Provider is required to provide a written notification to the Service User concerning the termination.
6. After notification referred to in Point 1 has been received, the Service User may not access the remaining funds held at the Service Provider, which will be settled in line with prevailing laws and regulations, including conveyance to the Insolvency and Public Trustees Office.
7. If a Service Provider suspects a transaction may be linked to Money Laundering or Terrorism Financing, and is confident that CDD implementation may result in violations of anti-tipping off regulations, the Service Provider:
   a. can suspend CDD implementation; and
   b. must report the transaction as a Suspicious Financial Transaction to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK).

8.1 Rejection and Termination of Business Relationship concerning Account-Based Fund Transfer Activities

1. A Provider may also reject a business relationship, reject a transaction, cancel a transaction and/or terminate a business relationship in the event of an incoming transfer to a beneficiary, however only after the Beneficiary Provider has conducted CDD and based on information from the Originating Provider that the beneficiary account contains proceeds of crime in accordance with prevailing laws on the prevention and eradication of Money Laundering.
2. If a business relationship is rejected/terminated in terms of funds transfer transactions, the rejection/termination procedure is implemented in accordance with prevailing laws concerning funds transfers.
3. The rejection or cancellation of a transaction in a beneficiary account containing proceeds of crime may be accompanied by a refund to the originator if the following requirements are met:
    a. upon receipt of a report from the originator to the Originating Provider complete with supporting documentation, such as a report to the police;
    b. the identity of the beneficiary is known to be fictitious and/or forged documents are suspected to have been used;
    c. the funds remain in the beneficiary's account;
    d. the transaction from the originator account was conducted through funds transfer;
    e. part or all of the funds stored in the beneficiary account originated from the originating account;
    f. the account or balance of funds in the beneficiary account have not been frozen or confiscated by an authorised institution; and
    g. the account opening agreement contains a clause concerning the obligation of a Service Provider to reject a transaction, cancel a transaction and/or terminate a business relationship with the Service User.
4. The refund referred to Point 3 is processed by debiting the funds from the beneficiary account and crediting the funds to the originator account.
5. The refund referred to in Point 4 is conducted in accordance with the following provisions:
    a. If only one originator submits a refund request, the funds returned to the originator are the funds of the originator still stored in the beneficiary account; or
    b. If more than one originator submits a refund request and the Service Provider is confident the funds in the beneficiary account:

i. originated from all originators and total funds are adequate to refund to all originators, the Service Provider may return the funds;
ii. only originated from some of the originators and total funds are adequate, the Service Provider may return the funds to some of the originators the Service Provider considers as the source of funds in the beneficiary account;
iii. originated from all originators but total funds are inadequate to return to all originators, the funds shall be returned based on an agreement between the originators. If no agreement can be reached, the funds shall be returned based on a court decision instructing the Service Provider to return the funds to the rightful parties; or
iv. only originated from some of the originators but total funds are inadequate, the funds shall be returned to each originator whose funds the Service Provider considers still to be in the beneficiary account based on an agreement between the originators. If no agreement can be reached, the funds shall be returned based on a court decision instructing the Service Provider to return the funds to the rightful parties.

6. When the funds have been returned to the originator, the Originating Provider will create a refund notification signed by the officer at the Originating Provider and the originator.
7. The refund process referred to in Point 6 is not applicable if the beneficiary's and/or originator's name appear on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).
8. In this case, the account is an account that can store funds as well as send and receive funds transfers, for example a server-based electronic money account with funds transfer features.

CHAPTER 9
Third-Party CDD Implementation

Chapter 9 | Third-Party CDD Implementation

1. If a Service Provider cooperates with a third party, the Service Provider is required to ensure AML/CFT implementation, as referred to in Chapter 1.1.1 Point 3, by the third party.
2. A Service Provider may cooperate with a third party to conduct CDD referred to in Point 1 above. If a Service Provider cooperates with a third party, the Service Provider is required to ensure AML/CFT implementation by the third party.
3. A Service Provider may utilise the results of CDD conducted by a third party.
4. A third party referred to in Point 1 includes:
   a. a party representing the Service Provider acting for and on behalf of the Service Provider in a direct relationship with a Potential Service User or Service User, namely agents working with the Service Provider, such as marketing agents, cash deposit agents for funds transfers and digital financial services (DFS) agents for issuer of electronic money;
   b. other Service Providers that have conducted CDD on a Potential Service User or Service User in the form of Other Financial Services Providers regulated and supervised by Bank Indonesia or other relevant authorities; or
   c. an entity under the same corporate/business group as the Service Provider.
5. Service Providers are required to report the results of third-party CDD to Bank Indonesia.
6. Service Providers are responsible for the results of third-party CDD.
7. If a Service Provider works with a third party to conduct electronic CDD, the Service Provider must:
   a. provide information concerning CDD procedures and ensure the third party understands the core principles of CDD, including the basic procedures associated with identification, verification and ongoing due diligence;
   b. ensure the third party applies CDD procedures in accordance with the procedures of the Service Provider; and
   c. identify and verify the Service Users and Beneficial Owners, as well as understand the reasons and intention for the business relationship or transaction and the source of funds.
8. If a Service Provider uses the results of third-party CDD referred to in Point 4 letter a, the following conditions apply:
   a. the Service Provider is deemed to have conducted CDD itself as part of the policies, procedures and internal control system determined by the Service Provider;

b. the Service Provider is required to immediately collect the results of CDD, including the identity documents of the Service User and other supporting documents;
c. the Service Provider is responsible for ensuring third-party compliance to the provisions in Bank Indonesia regulations and/or the AML/CFT policies and procedures determined by the Service Provider as follows:
    i. detail the third-party compliance obligations to Bank Indonesia regulations as well as Service Provider AML/CFT policies and procedures in a written agreement;
    ii. provide education and socialisation activities to a third party concerning Bank Indonesia regulations as well as Service Provider AML/CFT policies and procedures; or
    iii. conduct periodic monitoring and evaluation of a third party in terms of compliance to Bank Indonesia regulations and/or Service Provider AML/CFT policies and procedures.

9. For use of CDD results conducted by another Service Provider, as referred to in Point 4 letter b, or business entity within the same corporate group, as referred to in Point 4 letter c, the Service Provider is required to:
    a. maintain a business relationship with the third party based on a written agreement;
    b. immediately collect the CDD results;
    c. ensure the availability of copies of Service User identity documents and other supporting CDD documents upon request;
    d. ensure that the third party is supervised by a relevant authority in terms of compliance to AML/CFT regulations in the home country; and
    e. ensure the home country of the third party is not considered a high-risk country.
10. Service Providers are required to ensure the third party maintains CDD security and confidentiality.

CHAPTER 10
Fund Transfer

Chapter 10 | Funds Transfer

1. Funds Transfer Providers, in addition to meeting the provisions stipulated in Chapter 1.1.1 Point 3, are also required to have the following Funds Transfer policies and procedures:
   a. funds transfer sending and/or receiving;
   b. ensure complete information in terms of the Funds Transfer and follow-up actions: and
   c. transfer of funds to the beneficiary.
2. Identification and verification of Service Users in Funds Transfer activities must be conducted by:
   a. The Originating Service Provider on the originator; and
   b. The Beneficiary Service Provider on the beneficiary.
3. The information submitted by the Originating Service Provider to the Intermediary Provider or Beneficiary Service Provider must include:
   a. the identity of the originator, including name and address, accompanied by other information such as identity document number, place and date of birth as well as other information in accordance with prevailing laws;
   b. originator account number or unique transaction reference number;
   c. originator source of funds;
   d. name of beneficiary;
   e. beneficiary account number or unique transaction reference number;
   f. transfer total and currency; and
   g. transaction date.
4. For cross-border Funds Transfers of less than Rp10 million or equivalent, the identity of the originator referred to in Point 3 Letter a is the name of the originator.
5. For domestic Funds Transfers, the information submitted by the Originating Service Provider to the Intermediary Provider or Beneficiary Service Provider includes the following:
   a. originator account number or unique transaction reference number; and
   b. beneficiary account number or unique transaction reference number, while the account number or unique transaction reference number can be used to trace the identity of the originator and beneficiary.
6. All funds transfer activities must be documented.

7. In the event of a request for information from a relevant authority, the Service Provider must submit the information referred to in Point 3 – Point 5 no later than three working days upon receipt of the request.
8. Originating Service Providers failing to meet the provisions referred to in Point 3 – Point 7 are proscribed from executing the Funds Transfer order from the originator.
9. Intermediary Service Providers are required to ensure complete information is submitted to the originating Service Provider, including post-event due diligence or real-time due diligence if possible.
10. All information received by the originating Service Provider must be documented in accordance with prevailing laws and regulations concerning document administration.
11. Intermediary Service Providers are required to have and implement follow-up policies and procedures, including in cases when incomplete information is submitted. Follow-up actions include:
    a. processing transactions;
    b. rejecting transactions;
    c. suspending transactions;
    d. other actions as required, including reporting the transactions to a relevant authority in accordance with prevailing regulations.

    Follow-up actions are determined based on the level of risk faced.
12. The actions taken by the Intermediary Service Provider referred to in Point 11 are accompanied by appropriate follow-up actions, including enhanced due diligence and/or reporting the transaction as a Suspicious Financial Transaction.
13. Intermediary Service Providers are required to send all information referred to in Point 9 to other Intermediary Service Providers and the Beneficiary Service Provider.
14. Intermediary Service Providers must administrate all information referred to in Point 9.
15. Beneficiary Service Providers are required to ensure complete information is submitted to the Originating Service Provider or Intermediary Service Provider, including post-event due diligence or real-time due diligence if possible.
16. All information received must be documented in accordance with prevailing laws and regulations concerning document administration.
17. Beneficiary Service Providers must have and implement follow-up policies and procedures, including in cases when incomplete information is submitted. Follow-up actions include:
    a. processing transactions;
    b. rejecting transactions;
    c. suspending transactions;

d. other actions as required, including reporting the transactions to a relevant authority in accordance with prevailing regulations.

Follow-up actions are determined based on the level of risk faced.

18. Actions taken by the Originating Service Provider referred to in Point 17 are accompanied by appropriate follow-up actions, including enhanced due diligence and/or reporting the transaction as a Suspicious Financial Transaction.
19. If the Beneficiary Service Provider receives a transfer order from the Originating Service Provider within the Indonesian region that is not accompanied by complete information as referred to in Point 3 yet only includes the originator account number or unique transaction reference number, the Beneficiary Service Provider may submit a written request for information as required to the Originating Service Provider.
20. An Originating Provider simultaneously acting as a Beneficiary Service Provider must consider and analyse all information concerning the originator and beneficiary when compiling a Suspicious Financial Transactions Report (LTKM) for submission to the relevant authority.
21. The provisions stated in Points 3-19 are not applicable to:
    a. transactions using debit cards, ATM cards, credit cards or electronic money (traceable using the card number) when used for the payment of goods or services, excluding payments for goods or services such as person-to-person (P2P) funds transfers; and
    b. funds transfers between Service Providers in the interest of the Service Provider.
22. When transferring funds, an Originating Service Provider facilitating cross-border funds transfer services is required to:
    a. reject working with a shell bank; and
    b. ensure that the third party has not licensed an account used by a shell bank.

CHAPTER 11
Document Administration

Chapter 11 | Document Administration

1. Service Providers are required to administrate all domestic and international data and documents for a minimum of five years:
   a. documents relating to Service Users since:
      i. the end of the business relationship or transactions with the service user; or
      ii. the discovery of unusual transactions based on the risk profile of the service user; and
   b. documents relating to the financial transactions of the Service User in accordance with prevailing laws on corporate documents. Documents relating to the financial transactions of Service Users, including account numbers, transaction journals, account opening, funds transfer orders (FTO), receipts and/or proof of transaction of the Service User. The financial transaction documents of the service user are administrated in a way to facilitate transaction tracing and reconstruction as required by Bank Indonesia, law enforcers and/or other relevant authorities.

   Documents can be administrated in the form of originals, copies, electronic documents, microfilm, or other documents in accordance with prevailing laws, which can be used as legal evidence.

2. Documents relating to the Service User's data as follows:
   a. identity of the Service User, including supporting documents;
   b. evidence of Service User data verification;
   c. the results of ongoing due diligence and analysis;
   d. correspondence with the service user; and
   e. documents relating to the Suspicious Financial Transactions Report (LTKM) as applicable.
3. Service Providers are immediately required to provide the data, information and/or documents administrated as requested by Bank Indonesia, law enforcement and/or other authorities in accordance with prevailing laws and regulations.
4. The duration of administration referred to in Point 1 may be extended for specific cases and/or as requested by Bank Indonesia, the relevant authorities and/or law enforcement in accordance with prevailing laws and regulations.

GLOSSARY

GLOSSARY

Term	Definition
AML/CFT	Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT), namely efforts to prevent and eradicate money-laundering and terrorism financing
PEP Family Member	A second-degree relative (SDR) horizontally or vertically of the PEP as follows: a. biological/step/adopted parents; b. biological/step/adopted siblings; c. biological/step/adopted children; d. biological/step/adopted grandparents; e. biological/step/adopted grandchildren; f. biological/step/adopted aunts and uncles; g. spouse; h. in-laws; i. spouse of biological/step/adopted children; j. grandparents of spouse; k. spouse of biological/step/adopted grandchildren; l. biological/step/adopted sibling of husband; and/or m. husband and wife or wife of sibling. For the criteria of a Politically Exposed Person (PEP), family member or close associate of a PEP, refer to an independent and trusted source, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) or other relevant authority.
Anti-Tipping Off	Directors, Commissioners, Managers and/or Employees of a Service Provider are prohibited from tipping off a Service User or third party, directly or indirectly, regarding a Suspicious Financial Transactions Report (LTKM) under preparation or submitted to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK).
Beneficial Owner (BO)	The Beneficial Owner is each individual or collective, directly or indirectly, as the actual owner of the funds, controlling transactions of the service user, controlling the corporation or other legal arrangement; and/or with power of attorney to perform a transaction.
Customer Due Diligence (CDD)	Customer due diligence includes the identification, verification and monitoring of customers to ensure that transactions are performed in accordance with the respective profile of the Potential Service User, Service User or Beneficial Owner.
DTTOT	List of Suspected Terrorists and Terrorist Organisations
Enhanced Due Diligence (EDD)	Enhanced due diligence is additional customer due diligence used to deepen the profile of the high-risk Potential Service Users, Service Users or Beneficial Owners.
Electronic Customer Due Diligence	Electronic Customer Due Diligence is remote customer due diligence performed using electronic devices and media to minimise costs and increase efficiency, including online channels and mobile channels.
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an intergovernmental organisation that functions to combat money laundering and terrorism financing globally.
Government Institution	A collective term for government organisational units with the following functions: a. coordinating ministry; b. government ministry; c. ministry d. non-ministerial state institution; e. provincial government; f. city government; g. municipal government; h. state institution established based on prevailing laws; and i. state institutions implementing a government function using the state or regional government budget.
Low-Risk Delivery Channels	Low-risk delivery channels include low-value transactions through direct meetings.
High-risk delivery channels	High-risk delivery channels include high-value online transactions.

Term	Definition
	High-risk criteria refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities, including the results of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA).
KUPVA BB	Non-bank money changers, namely legal entities licensed to exchange foreign currencies in accordance with prevailing Bank Indonesia regulations concerning non-bank money changers.
State Institution	An institution with executive, judicial or legislative authority.
Digital Financial Services (DFS)	Digital financial services are payment system and financial services performed in cooperation with a third party using mobile or web-based technology towards financial inclusion.
Suspicious Financial Transactions Report (LTKM)	The Suspicious Financial Transactions Report (LTKM) contains suspicious financial transactions in accordance with prevailing laws and regulations on the prevention and eradication of money laundering and terrorism financing.
Cash Financial Transaction Report (LTKT)	The Cash Financial Transaction Report contains all financial transactions using banknotes and/or coins.
International Financial Transaction Report (LTKL)	The International Financial Transaction Report contains all incoming and outgoing international funds transfers.
Low-risk country or geographic area	Low-risk countries or geographic areas include: 1. countries maintaining a high level of good governance as determined by the World Bank; and/or 2. countries with a low corruption risk as identified by the Transparency's International Corruption Perception Index.
High-risk country or geographic area	High-risk countries or geographic areas include: 1. jurisdictions identified as failing to adequately implement the FATF recommendations based on an evaluation by the Financial Action Task Force on Money Laundering (FATF), Asia-Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Eastern and Southern Africa Anti-Money Laundering Group (ESAmlG), The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), The Grupo de Accion Financiera de Sudamerica (GAFISUD), Intergovernmental Anti-Money Laundering Group in Africa (GIABA) or Middle East & North Africa Financial Action Task Force (MENAFATF); 2. countries identified as uncooperative or tax havens by the Organisation for Economic Co-operation and Development (OECD); 3. countries with a low level of governance as determined by the World Bank; 4. countries with a high corruption risk as identified by the Transparency's International Corruption Perception Index; 5. countries widely accepted as producers or centres of the illegal drug trade; 6. countries subject to UN sanctions, embargos or similar measures; 7. countries or jurisdictions identified by trusted institutions as funders or supporters of terrorism; High-risk criteria refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities, including the results of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA).
Unique Transaction Reference Number	A UTR number is a unique traceable reference code attached to every funds transfer or payment transaction consisting of letters, numbers and/or symbols that replace the account number.
Tax File Number (NPWP)	A tax file number given to all taxpayers for tax administration purposes used to identify the taxpayer in terms of rights and responsibilities.
One-Time Password (OTP)	A one-time password is a series of numeric or alphanumeric characters generated automatically that is valid for only one transaction or login session.
Bank Indonesia Regulation (PBI)	Regulations formulated and issued by Bank Indonesia.
Beneficiary	The party stated on the Funds Transfer Order as the recipient of the transferred funds in

Term	Definition
	accordance with prevailing laws on funds transfers.
Originator	The party issuing a Funds Transfer Order in accordance with prevailing laws on funds transfers.
Low-Risk Service User	Low-risk service users include the following: 1. state or government institution; 2. majority state-owned enterprise; 3. public company or issuer subject to laws and regulations concerning financial transparency; and 4. service users of products or services for government poverty alleviation programs.
High-Risk Service User	High-risk service users include the following: 1. PEP, family of PEP and close associates of PEP; 2. high-risk business owners; 3. appointing a third party to establish a business relationship; 4. named on the List of Suspected Terrorists and Terrorist Organisations (DTTOT) or List of Funding of the Proliferation of Weapons of Mass Destruction. High-risk criteria refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities, including the results of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA).
Beneficiary Provider	A Funds Transfer Provider performing a payment or sending transferred funds to the beneficiary in accordance with prevailing laws on Funds Transfers. The Beneficiary Provider disburses the payment in cash or equivalent, directly or through an agent, intermediary or cashier.
Intermediary Provider	A Funds Transfer Provider other than the Originating Provider and Beneficiary Provider in accordance with prevailing laws concerning funds transfers.
Originating Provider	A Funds Transfer Provider receiving a funds transfer order from the originator to pay or instruct another Funds Transfer Provider to pay a specific amount of funds to the beneficiary in accordance with prevailing laws concerning funds transfers.
Close Associates of PEP	Close associates of PEP include: a. legal entities owned or managed by a PEP; or b. parties publicly known to share a close relationship with a PEP, for instance a driver, personal assistant and personal secretary. The criteria for a PEP, family of PEP and close associates of PEP refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities.
P2P	Person-to-person
PEP	Politically Exposed Person
Foreign PEP	A person with a prominent function in another country, such as a head of state or government, senior politician, senior government official, military officer, law enforcement officer, senior manager of a state-owned company, or prominent member of a political party. The criteria for a PEP, family of PEP and close associates of PEP refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities.
Domestic PEP	A person with a prominent function in the country, such as a head of state or government, senior politician, senior government official, military officer, law enforcement officer, senior manager of a state-owned company, or prominent member of a political party. The criteria for a PEP, family of PEP and close associates of PEP refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities.
PEP in an International Organisation	A person with a prominent function in an international organisation, including senior management, such as a director, deputy director, board member or equivalent function. The criteria for a PEP, family of PEP and close associates of PEP refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities.

Term	Definition
PJSP SB	Nonbank payment system service provider, namely a nonbank legal entity licensed to perform payment system services activities in accordance with Bank Indonesia regulations on the payment system.
Low-Risk Products or Services	Low-Risk Products or Services include the following: 1. products or services that support government programs to increase financial inclusion, raise public prosperity, alleviate poverty and/or intended for people living with disabilities, limited in terms of amount and use; and/or 2. products or services with limited purposes, uses, features, Service Users, balance or restrictions along with effectively mitigated risk of money laundering and terrorism financing.
High-Risk Products or Services	High-Risk Products or Services include the following: 1. private banking or similar business relationship; 2. anonymous transactions, especially in cash; or 3. payments received by unknown or unaffiliated beneficiary. High-risk criteria refer to independent and trusted sources, including Bank Indonesia, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) and other relevant authorities, including the results of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA).
SMS	Short Messaging Service is a text messaging service to send or receive (exchange) short messages.
Shell Bank	A shell bank is an established and licensed financial institution but with no physical presence in the country and/or not subject to consolidated regulation and supervision by the authorities.
TC	Technical compliance
TPT	Cashier, namely a third party cooperating with a Service Provider to disburse allocated funds to the beneficiary.
TPPU	Money Laundering, namely any criminal acts stipulated in money laundering laws.
TPPT	Terrorism financing, namely any criminal acts stipulated in terrorism financing laws.
Funds Transfer	A series of activities, starting with a funds transfer order from the originator, to transfer money to the Beneficiary named in the Funds Transfer Order, until the money is received by the Beneficiary.
Cross-Border Funds Transfer	A funds transfer where at least one of the Providers, namely the Originating Provider, Beneficiary Provider or Intermediary Provider, is located outside of the Republic of Indonesia.

Department of Policy and Payment System

June 2020