GUIDELINES ON CUSTOMER DUE DILIGENCE (CDD)

MESSAGE FROM PRESIDENT

SOUTH ASIAN FEDERATION OF ACCOUNTANTS (SAFA)

The development of this comprehensive document on "Customer Due Diligence" underscores SAFA's continuous commitment to maintaining the highest standards in anti-money laundering practices and reinforces our dedication to safeguarding the integrity of the financial system in the region.

The meticulous efforts invested in developing this document reflect the collective expertise and diligence of our committee members representing the SAFA member countries. Customer Due Diligence is a critical aspect of the anti-money laundering framework, and this document serves as a robust guide to navigating the complexities associated with this process. By setting forth clear guidelines and best practices, we aim to enhance the efficiency and effectiveness of our due diligence procedures.

In an evolving regulatory landscape, it is imperative that we, as accountants, stay ahead of the curve in our efforts to combat financial crimes. Therefore, this document not only aligns with current regulatory requirements but also anticipates future challenges, providing a foundation for sustained compliance and risk mitigation.

I would like to express my gratitude to the SAFA AML Committee members for their commitment and spirit of cooperation in creating this significant document, which will undoubtedly be very beneficial for all of our members throughout South Asia, and for further advancing and bolstering accountability, integrity, and transparency.

Here's to a future marked by continued success and unwavering dedication to the principles of combating anti-money laundering and counter-terrorism financing.

CA. Heshana Kuruppu
President
South Asian Federation of Accountants (SAFA)

MESSAGE FROM VICE PRESIDENT

SOUTH ASIAN FEDERATION OF ACCOUNTANTS (SAFA)

Having had the privilege of serving as a founding member of the SAFA Anti-Money Laundering (AML) Task Force, formed in the year 2020, I also had the honor of assuming the role of the inaugural Convener of this pivotal initiative within SAFA. This unique opportunity allowed me to contribute to the establishment and strategic direction of the task force, marking the beginning of a journey dedicated to fortifying our organization against the multifaceted challenges posed by money laundering.

Under my leadership as the Convener, a detailed exercise was carried out, analyzing AML legislations of various member countries of SAFA and determining compliance information/requirements related to Designated Non-Financial Businesses and Professions (DNFBPs), including Accountants. This booklet was called the "Anti–Money Laundering Best Practices for Accountants".

The measures put forth by the AML Task Force were instrumental in cultivating a culture of vigilance within SAFA. Subsequently, a proactive stance emerged, setting the stage for future endeavors such as the development of a formal SAFA AML Committee. Today, as I reflect upon the journey, I take great pride in witnessing the culmination of the SAFA AML Committee's collective efforts, embodied in the form of this comprehensive Customer Due Diligence (CDD) document that aligns with the principles contained in the best practices booklet.

Comprised of dedicated professionals, the SAFA AML Committee has labored diligently to refine and elevate our approach to customer due diligence. This achievement underscores the Committee's dedication to upholding the highest standards in the fight against money laundering, showcasing a proactive and vigilant approach that aligns seamlessly with SAFA's mission and values.

I would like to convey my sincere gratitude to the SAFA AML Committee for their steadfast dedication and invaluable expertise throughout the developmental phase. Their unwavering commitment to upholding excellence has played a pivotal role in shaping this notable document for SAFA.

Ashfaq Tola, FCA
President
South Asian Federation of Accountants (SAFA)

MESSAGE FROM CHAIRMAN

SAFA COMMITTEE ON ANTI – MONEY LAUNDERING

I am delighted to present the comprehensive document on "Guidelines on Customer Due Diligence (CDD) for the member countries of the South Asian Federation of Accountants (SAFA). This latest addition builds upon the groundwork laid out in two previous documents issued in 2023, reflecting our commitment to providing comprehensive and up-to-date guidance in field of AML/CFT.

This document encompasses the Financial Action Task Force (FATF) Recommendations pertaining to customer due diligence and outlines the suggested processes through which the Accountants of the member bodies can ensure compliance with this crucial aspect within the overarching Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Regime.

This comprehensive document aims to aid member bodies in comprehending the obligations of Customer Due Diligence under the FATF Regime. It is anticipated that the member bodies of SAFA will diligently work towards ensuring compliance with the FATF recommendations, contributing to the collective effort to combat Money Laundering and Terrorism Financing, and fortifying the compliance regime across the entire region.

The member countries are required to effectively implement the FATF recommendations (commonly known as FATF Standards on AML / CFT). These standards set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

I would like to express my gratitude for the cooperation of the Committee members in providing feedback related to this crucial aspect of AML/CFT. Additionally, I extend my appreciation for the efforts of Ms. Noureen Merchant, Secretary SAFA AML Committee, in formulating this comprehensive guideline.

Khalid Rahman, FCA
Chairman

SAFA Committee on AML

INTRODUCTION

Risk-Based Customer/Client Due Diligence (CDD) is a crucial element in the effective implementation of anti-money laundering and counter-terrorism financing (AML/CFT) measures. It requires a significant shift in how Reporting Firms (RFs) approach customer engagement, focusing on assessing the risk associated with each customer. While some aspects of CDD are standard, such as collecting customer information, other requirements, like verifying customer identity and beneficial ownership, as well as assessing the source of funds, may be new and necessitate additional time and resources before accepting a new customer or engagement.

LEGAL OBLIGATION

1. The South Asian countries are under legal obligation to implement the FATF Recommendations on CDD, on account of being a responsible member of the United Nations.
2. To fulfill these obligations, these countries rely on various legal provisions found within their respective Laws and Regulations related to Anti-Money Laundering, which can vary from one country or organization to another.

KEY STATUTORY REQUIREMENTS FOR CDD

1. Identification and verification of customer and beneficial owner.
2. The option to rely on third parties for conducting CDD.
3. Completion of CDD prior to providing specified services or terminating the customer relationship.
4. Prohibition of anonymous business relationships and transactions.
5. Mandatory CDD requirements for reporting firms, encompassing customer and beneficial owner identification.
6. Provisions for delayed verification under certain conditions.
7. Ongoing due diligence on existing customers, involving transaction scrutiny and the updating of CDD records.
8. Enhanced due diligence for higher-risk customers, such as Politically Exposed Persons (PEPs) and individuals closely associated with them.
9. Application of countermeasures for high-risk countries.
10. The option for simplified due diligence after identifying lower risks through risk assessments.

WHO TO CONDUCT CDD ON

1. Your customer:

   Any person seeking the services of a reporting firm for specific purposes, as defined in the Guidelines.
2. Beneficial owner of a customer:

   This refers to the natural person who ultimately owns or controls the customer or a person on whose

behalf a transaction is conducted, or a person who exercises ultimate effective control over a legal entity.

3. Any person acting on behalf of a customer:

   This category includes individuals who represent customers but may not be beneficial owners themselves. For instance, individuals with power of attorney, legal guardians acting on behalf of minors, or employees authorized to act on behalf of a company.

TIMING OF CDD

1. For new customers:

   The CDD process should commence during initial discussions but must be completed before the reporting firm agrees to provide services or accepts the customer or new engagement. Identification of a new customer should occur before acceptance.

2. For existing customers:

   There may be instances where CDD is required if there are significant changes in the nature of the business relationship, ownership, or control structure. In such cases, CDD should be conducted promptly. For other existing customers with no changes, there is no fixed deadline for updating CDD.

Overall, Risk-Based Customer Due Diligence is a comprehensive framework that assists in identifying and mitigating financial crime risks while adhering to legal requirements and ensuring sanctions for non-compliance. It targets customers, beneficial owners, and individuals acting on behalf of customers, and its timing depends on the nature of the engagement and the need for verification or updating of information.

CDD COMPONENTS

The key components of Customer Due Diligence (CDD) provide the foundation for effective anti-money laundering and counter-terrorism financing efforts. These components apply on a global scale and are not specific to any particular region or country. Here's a summary of the essential elements of CDD:

1. Identify Legal Identity and Address:

   Reporting firms are required to identify the legal identity of customers, which can be individuals, legal entities like companies or non-profit organizations, or legal arrangements such as trusts. This includes obtaining key information like date of birth, address, or date of formation, and the address should be a physical one.

2. Verify Legal Identity and Address:

   Verification of customer identity, including name, date of birth/formation, and address, must be conducted using reliable and independent source documents, data, or information. Acceptable verification documents are detailed in a separate section.

3. Identify and Verify Beneficial Ownership:

   Identifying and verifying beneficial ownership is a significant requirement under AML/CFT legislation. For individuals, the person is typically considered both the legal and beneficial owner. In cases of non-

complex company structures, the natural person director(s) may also be the beneficial owner(s). However, complex ownership structures or discretionary trusts may involve multiple layers of legal ownership, necessitating identification and verification of the ultimate beneficial owner. This is a complex process, and guidelines provide further details.

4. Identify and Verify Authorized Representatives:

   Reporting firms must identify and verify the identity of individuals authorized to act on behalf of the customer. This does not require identifying and verifying the beneficial owner in this situation. Examples of such representatives include employees acting on behalf of a company, trustees, individuals with power of attorney, or legal guardians representing minors. The process is similar to Steps 1 and 2 for individual customers, with the additional requirement of obtaining evidence of the appointment and specimen signature.

5. Information on Purpose and Nature of the Relationship:

   Reporting firms must obtain information regarding the purpose and intended nature of the business relationship. This information should be documented, especially when dealing with high-risk customers. There is no requirement to verify this information.

6. Establish or Obtain Information on the Source of Wealth or Funds:

   Regulations require reporting firms to obtain information on the source of wealth or funds, particularly for higher-risk customers, including Politically Exposed Persons (PEPs) and their close associates. Accountants, given their professional services, are well-positioned to acquire this knowledge.

7. Ongoing Customer Due Diligence:

   Reporting firms must conduct ongoing due diligence for continuing business relationships. This includes monitoring transactions and ensuring that the services provided align with the firm's understanding of the customer, their business, and their risk profile, including the source of funds.

   These CDD components are essential in combating money laundering and the financing of terrorism and apply to financial institutions and reporting firms globally. They are a fundamental part of fulfilling international obligations and maintaining the integrity of financial systems.

CUSTOMER VERIFICATION DOCUMENTS

These verification requirements apply across various regions and are not specific to any particular country:

1. Individuals (as customers, authorized representatives, and beneficial owners):

   Acceptable documents include a government-issued photo identification document, such as a passport, national identity card, or any equivalent official document with a photograph. In the case of foreign nationals, a passport with a valid visa or other proof of legal stay is required.

2. Sole Proprietors:

   Verification documents include the proprietor's government-issued photo identification, business registration certificates, tax identification numbers, proof of membership in relevant trade bodies, and a declaration of sole proprietorship on official business letterhead.

3. Partnership:

   Verification involves the government-issued photo identification of all partners, the partnership agreement, registration certificate with the relevant government authority, and an authorization letter from all partners allowing individuals to represent the partnership in the business relationship.

4. Legal Persons (e.g., limited companies/corporations):

   Documents required include the resolution of the board of directors, the company's articles of incorporation, registration certificate with the official business registry, a list of directors, and government-issued photo identification of all directors, beneficial owners, and authorized persons. Additional documents, such as annual accounts and financial statements, may be requested for risk assessment.

5. Legal Arrangements:

   Verification involves the document creating the legal arrangement, registration records, by-laws, rules, regulations, authorization documents, and government-issued photo identification of authorized persons, beneficial owners, and members of governing bodies or committees. Additional documentation may be requested for risk assessment.

6. NGOs/NPOs/Charities:

   Verification includes registration certificates, by-laws or governing documents, resolutions from the governing body or trustees authorizing the business relationship, government-issued photo identification of authorized persons and members of the governing body or trustees, and any additional documents providing insight into the organization's activities, sources of funds, and fund utilization for risk assessment.

7. Government Institutions and Entities:

   Verification requires government-issued photo identification of authorized individuals representing the institution and a letter of authorization from the relevant governmental authority for the designated individual acting on behalf of the institution.

Original documents should be sighted, photocopied, and attested by the reporting firm for verification. In cases where original documents cannot be produced, certified true copies by an independent and qualified person (such as a notary public or an external law firm) may be considered, but the original certified true copy must be provided, not just a photocopy. Alternatively, electronic verification may be undertaken using various subscription services.

Overall, these document and data verification requirements are essential for maintaining the integrity of

financial systems and ensuring compliance with international anti-money laundering and counter-terrorism financing standards, regardless of the specific country or region.

IDENTIFYING AND VERFIYING BENEFICIAL OWNERS

Beneficial ownership refers to identifying and verifying the individuals or entities that ultimately own or control a customer or a transaction. It plays a crucial role in anti-money laundering (AML) and counter-terrorist financing (CFT) regulations and is essential for mitigating financial risks.

1. Definition of Beneficial Ownership:

   Beneficial ownership refers to a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is conducted. It can also include a natural person who exercises ultimate effective control over a legal entity or arrangement.

2. Reasonable Measures for Verification:

   Reporting firms are required to identify and take reasonable measures to verify the identity of beneficial owners. The requirement to take "reasonable measures" acknowledges the challenges involved in this process.

3. Legal Definitions and Tests:

   Different legal entities (e.g., individuals, legal persons, legal arrangements) may require distinct methods for identifying and verifying beneficial ownership. Legal definitions and tests, such as controlling ownership tests, control through other means tests, senior management tests, may be used to determine beneficial ownership. These tests are cascading and are applied in succession when the previous test doesn't identify the beneficial owner.

4. Natural Persons:

   For individuals, beneficial ownership is generally the same as legal ownership, but exceptions exist in cases like when a son/daughter manages an account for their parents.

5. Legal Persons (e.g., Companies):

   Beneficial ownership may differ from legal ownership, especially in cases of multiple shareholders. The legal definitions of beneficial ownership may involve thresholds, indirect ownership, and control through various means.

6. Legal Arrangements (e.g., Trusts):

   Identifying beneficial ownership in trusts can be complex, as it involves parties with different roles, rights, and obligations. All parties to a trust, such as settlors, trustees, protectors, and beneficiaries, are treated as beneficial owners. Verification may require understanding trust deeds, agreements, and other relevant documentation.

7. Publicly Listed Companies:

   Simplified due diligence may apply to publicly listed companies, depending on the outcome of a customer risk assessment. Verification of beneficial ownership may not be required for publicly listed companies if they meet specific criteria and are deemed low risk.

8. Enhanced Due Diligence:

   For complex or high-risk cases where beneficial ownership cannot be easily verified, enhanced due diligence measures may be necessary.

9. International Considerations:

   Beneficial ownership regulations may vary by country, and international reporting firms should be aware of and comply with the AML and CFT requirements of their jurisdiction. In conclusion, identifying and verifying beneficial ownership is essential for ensuring the integrity of the financial system and preventing illicit activities. The specific methods and criteria for determining beneficial ownership may vary by jurisdiction and depend on the legal entity in question. Reporting firms should adopt a risk-based approach to comply with global AML and CFT regulations effectively.

POLITICALLY EXPOSED PERSONS (PEPs)

1. Who is a PEP?

   Politically Exposed Persons (PEPs) are individuals who, due to their prominent roles in public life, are susceptible to corrupt activities. The definition of a PEP varies across regulations, but generally includes individuals who have held or currently hold significant positions domestically or internationally. This encompasses heads of state or government, senior politicians, government officials, judicial or military authorities, executives of state-owned enterprises, and political party members. PEPs can be affiliated with foreign, domestic, or international organizations.

2. Why are family members and close associates included?

   Family members and close associates of PEPs are also considered within the PEP framework because corrupt PEPs often use them to facilitate money laundering. Family members include spouses, descendants, ascendants, and siblings, while close associates are individuals with joint beneficial ownership, close business relations, or any social or professional connection to a PEP.

3. Enhanced due diligence on PEPs, family members and close associates

   Enhanced due diligence is required for PEPs, their family members, and close associates. Reporting firms must have risk management systems in place to identify PEPs and assess whether they are beneficial owners of any legal entities.

4. Is enhanced due diligence applicable to PEPs (and family member and close associate) in all circumstances?

   Enhanced due diligence is applied to PEPs and their associates under specific circumstances, such as during customer onboarding. However, there is flexibility for reporting firms to apply enhanced due diligence even when not explicitly mandated by law, given the importance of a risk-based approach.

5. Procedures to identify a PEP (and family member and close associates)

   - Asking customers to declare their status,
   - Conducting independent background checks, and
   - Utilizing databases and reports from commercial service providers.

   These procedures aim to identify PEPs during the customer acceptance stage and through ongoing monitoring, especially if a customer's role changes or if there are alterations in company ownership.

   Overall, the definition of PEPs is broad and encompasses various roles and affiliations, and enhanced due diligence is a critical element in anti-money laundering efforts to mitigate the risks associated with corrupt individuals in public life.

SOURCE OF WEALTH & FUNDS

Source of wealth and source of funds are crucial elements in the due diligence process for customer relationships.

1. Source of wealth

   It pertains to the origin of a customer's total assets and provides insights into their wealth's volume and how it was acquired. This information can be gleaned from general sources, like commercial databases and open data available on the internet.

2. Source of funds

   It, on the other hand, focuses on the origin of specific funds or assets involved in the business relationship between the customer and the reporting firm.

3. Enhance Due diligence

   The requirement to obtain information on the source of wealth and source of funds is generally reserved for customers subject to enhanced due diligence. While supporting documentation is typically not mandated, it might be requested if doubts arise regarding the provided information or if there's an associated risk.

4. PEPs

   Politically Exposed Persons (PEPs) undergoing enhanced due diligence have additional obligations, particularly related to establishing the source of wealth and source of funds. However, not all PEPs are

automatically deemed high risk, and the level of due diligence varies depending on the risk assessment. There's no explicit requirement for source verification for all PEPs, but in cases of negative news reports or heightened risk, additional due diligence may be necessary.

When in doubt about the accuracy of the stated source of wealth or funds, reporting firms may request documents for confirmation, such as financial statements or taxation returns. These documents typically do not need to be original or certified copies unless doubts about their veracity exist.

Examples of acceptable sources for information and verification of source of wealth or funds include:

a. Employment Income:

- Recent pay slips
- Annual salary and bonus history
- Confirmation from the employer of annual salary
- Income tax returns/wealth statements

b. Business Income/Profits/Dividends:

- Latest audited financial statements
- Board of Directors approvals
- Rental statements
- Dividend statements

c. Savings/Deposits/Assets/Property:

- Statements from financial institutions
- Bank statements
- Tax returns
- Accountant's statements
- Property ownership certificates
- Share certificates

d. Inheritance:

Succession certificate

e. Sale of Property/Business:

Copy of sale agreement/Title Deed

f. Loan:

Loan agreement

g. Gift:

- Gift Deed

- Source of donor's wealth
- Certified identification documents of the donor

h. Other income/wealth sources:

   Details of income, amount, date received, and the source, with supporting documentation where available

ENTERPRISE RISK ASSESSMENT & CUSTOMER RISK ASSESSMENT

Enterprise risk assessment and customer risk assessment are fundamental components of anti-money laundering (AML) and counter-terrorist financing (CFT) regulations globally. These assessments are essential for businesses and financial institutions to evaluate and mitigate potential risks associated with their customers and operations.

The enterprise risk assessment provides a macro-level view of risks within an organization, covering various aspects like customer risks, geography, products, services, and delivery channels. In contrast, the customer risk assessment offers a micro-level perspective by evaluating the risk posed by individual customers. Once an enterprise risk assessment is conducted, it informs subsequent customer risk assessments.

These assessments are distinct because not all risks are customer-related. Some risks may arise from products, services, or delivery channels, such as handling cash payments, which inherently carry higher risks. Organizations may choose to mitigate these risks through measures like limiting cash transactions, which apply to all customers regardless of their individual risk profiles.

CUSTOMER RISK ASSESSMENT & RISK BASED CDD

Customer risk assessments follow a risk assessment methodology that considers threats, vulnerabilities, likelihood, and consequences to determine risk levels. Customers are categorized into risk groups, including:

- Lower Risk: Typically, publicly listed companies, financial institutions regulated by relevant authorities, or welfare recipients.
- Medium Risk: Standard customer due diligence, representing the most common risk category.
- Higher Risk: Applied to Politically Exposed Persons (PEPs) and their close associates, and for customers from countries identified by the Financial Action Task Force (FATF) as high-risk jurisdictions.

The responsibility for conducting customer due diligence (CDD) and assigning risk ratings usually falls to business line or customer-facing staff, with approval from relevant authorities. Enhanced due diligence may require senior management's involvement.

Indicators for higher risk customers include PEPs, discretionary trusts, companies with complex ownership structures, NGOs, companies with nominee shareholders, and cash-intensive businesses, among others.

THREE CATEGORIES OF CDD

CDD requirements vary based on risk levels, and simplified due diligence is typically applied to lower-risk customers. Standard CDD applies to customers without specific high-risk indicators. Enhanced CDD is mandatory for PEPs, their families, close associates, and transactions involving high-risk countries or other high-risk factors.

The level of due diligence, including verification of the source of wealth and income, is dependent on the customer's risk category. Risk assessments are critical for businesses to understand their customers and to take the appropriate steps to mitigate financial crime risks.

The document provides examples of customer risk assessments, highlighting different risk scenarios and the corresponding due diligence steps, from standard CDD for common businesses to enhanced CDD for high-risk situations.

PROHIBITED CUSTOMERS & RISK SCREENING

International Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) standards are applied to prevent financial systems from being misused by criminals and terrorists. These standards are seen worldwide, although specific regulations may vary by country. In many countries, regulations are in place to prohibit providing services to certain individuals and entities:

1. Prohibition by Government Orders:

   Regulations, akin to Statutory Regulatory Orders (SROs), issued by relevant authorities such as the Ministry of Foreign Affairs, National Counter Terrorism Authority, and Ministry of Interior, designate or proscribe individuals, entities, and their beneficial owners for various reasons, often related to national security.

2. Obligation to Screen New Customers:

   It is a global practice to require financial institutions and businesses, including reporting firms, to screen all new customers against these designated or proscribed lists. The aim is to prevent any association with potentially risky or illegal entities.

3. Ongoing Screening of Existing Customers:

   Ongoing checks are essential. It's an international standard to regularly update and screen existing customer lists each time there are updates to the sanctions lists. This continuous screening helps ensure that relationships with any prohibited entities are detected promptly and necessary action is taken.

4. Legal Person Verification:

   A widely accepted practice is to verify whether a customer, particularly a legal entity, is still registered as a legitimate entity. If a company has been deregistered, businesses are generally not allowed to accept them as new customers, as the legal person effectively ceases to exist.

5. Reputational Risk Screening:

While not mandated in all AML/CFT legislations, it is a global best practice for reporting firms to conduct reputational risk screening, especially for higher-risk customers. This may involve checking for adverse reports in media, information about fines, punishments, or allegations of corruption. Reputational risk screening helps in identifying potential issues, but it can be time-consuming, particularly if a reporting firm does not have access to commercial risk screening providers. Even without such subscriptions, conducting this screening, especially for Politically Exposed Persons (PEPs), remains an important risk management measure.

DELAYED VERIFICATION

1. General CDD Timing:

CDD measures are typically expected to be completed before establishing a business relationship with a customer. However, there are scenarios where a short extension for verifying beneficial ownership, source of wealth or funds may be acceptable, especially when most required information is already collected before the relationship begins.

2. Conditions for Delayed Verification:

Regulations often provide for delayed verification subject to specific conditions. These conditions are meant to manage risks and prevent money laundering or terrorist financing.

3. No Delay for Identity and Address:

Generally, there should be no delay in verifying the identity and address of the customer, as this is fundamental and legally mandated in most AML/CFT legislations.

4. Risk Management:

In the event of delayed verification, risk management procedures must be in place. This includes completing the verification as soon as reasonably practicable, ensuring normal business operations are not disrupted, and effectively managing money laundering/terrorist financing risks.

5. Rare and Limited Instances:

Delayed verification should be a rare and limited exception, as prompt CDD completion is crucial to maintain the integrity of financial systems.

6. Risk Mitigation Measures:

To minimize risks during delayed verification, actions may include not fully completing company formation, limiting funds transfers for managed accounts, and more.

7. Clear Communication:

It is essential to communicate clearly with the customer. If CDD cannot be completed, the customer should be made aware that the reporting firm may have to terminate the business relationship to avoid contractual disputes.

UNABLE TO COMPLETE CDD

1. Prohibition on Opening Accounts:

Global AML/CFT standards explicitly state that if a reporting firm is unable to complete the CDD process, it should not open an account, commence business relations, or perform transactions. This is to prevent the potential misuse of the financial system by those not adequately identified.

2. Potential Suspicious Transaction Reporting:

In cases where CDD cannot be completed, the reporting firm should promptly consider filing a Suspicious Transaction Report (STR) in relation to the customer. This aligns with international efforts to detect and report suspicious activities.

3. Circumstances for Incomplete CDD:

There are common circumstances in which CDD may remain incomplete. These can include a prospective customer refusing to provide necessary identity evidence, the reporting firm finding the information provided unsatisfactory for the customer's higher risk profile, or the risk of tipping off the customer.

CDD & TIPPING OFF

If continued CDD may tip off the customer and if there is a suspicion of money laundering or terrorist financing, international AML/CFT standards advise that the reporting entity should not proceed with CDD but should file an STR.

ONGOING MONITORING OF NEW CUSTOMERS

While specific regulations vary by country, there are common principles and practices applicable worldwide:

1. Ongoing CDD Components

a. Scrutinizing Transactions:

After completing initial CDD, there's no need to repeat the entire process every time a customer returns. Ongoing CDD typically involves scrutinizing transactions, which includes assessing whether

transactions align with the customer's business profile, risk profile, and the source of wealth and funds, when necessary.

b. Updating Customer Information and Records:

Customer information and verification documents must be kept up-to-date. There's also a stronger focus on conducting more frequent checks for customers rated as higher risk compared to those categorized as medium or lower risk.

2. Variability Based on Services Provided

The extent to which a reporting firm conducts ongoing CDD depends on the services provided. For firms managing customer funds, assets, or properties (e.g., banks), scrutinizing transactions becomes an integral part of ongoing CDD. Meanwhile, the component involving information and record updates applies to all customers but varies based on the level of risk.

3. Importance of Ongoing CDD

Ongoing CDD is essential to keep customer information current. This ensures that the risk assessment can be updated promptly when there's a change in circumstances, potentially shifting a customer from medium to high risk. It also enables the implementation of further due diligence measures if necessary.

4. Event-Driven Reviews:

a. Triggering Events:

Event-driven reviews occur in response to specific triggers, such as changes in a customer's identity, beneficial ownership, or the services they receive. Other triggers include information inconsistent with what's known about the customer, suspicions of money laundering or terrorist financing (ML/TF), or the start of a new engagement.

b. Additional Triggers:

Event-driven reviews can also be initiated when planning recurring engagements, restarting previously stalled engagements, a significant change in key office holders, the involvement of a politically exposed person (PEP), a significant change in the customer's business activity (e.g., expanding into new countries), or when there's knowledge, suspicion, or cause for concern, such as doubts about the accuracy of provided information. Care must be taken to avoid disclosures that could be considered tipping off, especially if a Suspicious Transaction Report (STR) has been filed.

5. Periodic Reviews:

a. Routine Assessment:

Routine periodic reviews are conducted at intervals (e.g., annually) to update the CDD information. The frequency of these updates is risk-based, relying on the reporting firm's risk assessment, and considering changes in the customer's circumstances or services required.

b. Differing Procedures:

CDD procedures for event-driven or periodic reviews may differ from the initial customer onboarding stage, as there may already be a substantial amount of existing information. Ongoing CDD often involves collecting less new information than what was required during customer onboarding.

EXISTING CUSTOMERS

1. Regulatory Requirements:

Reporting firms are required to apply Customer Due Diligence (CDD) measures to existing customers based on materiality and risk. They must conduct due diligence at appropriate times, considering whether CDD measures were previously undertaken and the adequacy of data obtained.

2. Definition of Existing Customers:

Existing customers are those who were customers of the reporting firm before new Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) CDD requirements came into effect. Specific dates for this transition may vary by jurisdiction.

3. Centralized Customer Database:

It is recommended, especially for larger firms, to maintain a centralized database containing all customer information. This centralization facilitates access to customer data by all staff interacting with customers, preventing redundancy and enhancing customer satisfaction.

4. Classification of Existing Customers:

Existing customers fall into two categories - active and dormant. For dormant accounts, a senior management decision should be made regarding whether they should be considered existing customers or treated as new customers from an AML/CFT perspective. This decision may hinge on the duration of dormancy (e.g., treating accounts as new customers if dormant for a certain period to mitigate risks).

5. Periodic Review:

It's crucial to periodically review existing customers, especially those classified as higher risk.

RELIANCE ON THIRD PARTY TO CONDUCT CDD

1. Outsourcing CDD Measures:

Reporting firms can outsource some or all of their Customer Due Diligence (CDD) measures to third parties. The reporting firm may rely on these third parties, subject to their agreement, to complete the CDD process.

2. Legal Framework:

   Regulations outline the principle of relying on third parties for conducting CDD. These principles are detailed in relevant AML/CFT regulations and may differ by jurisdiction.

3. Conditions for Reliance:

   Conditions for relying on third parties to conduct CDD are typically specified in the regulations. Reporting firms must ensure that these conditions are met, and they may have to obtain CDD information and verification documents from these third parties.

4. Corporate Group Considerations:

   If the third party is part of the same corporate group as the reporting firm, some requirements related to third-party reliance may be deemed fulfilled.

5. Types of Third Parties:

   Third parties capable of conducting CDD may include banks, law firms, or even other accounting firms, especially if the customer maintains relationships with multiple entities subject to AML/CFT regulations.

FEW OF THE FATF RECOMMENDATIONS RELATED TO CDD

1. Recommendation 10 - Customer Due Diligence:

   Objective:

   Recommendation 10 outlines the necessity for financial institutions and designated non-financial businesses and professions (DNFBPs) to conduct CDD. The primary goal is to understand the customer's identity, risk profile, and the purpose of the business relationship.

   Key Provisions:

   - Obtain and verify customer identity information.
   - Understand the nature and purpose of the business relationship.
   - Conduct ongoing monitoring to detect suspicious activities.

   Relevance to CDD:

   Recommendation 10 is the cornerstone of CDD requirements, emphasizing the need for robust processes to identify, verify, and monitor customers.

2. Recommendation 11 - Record Keeping:

Objective:

Recommendation 11 focuses on the maintenance of records. It requires financial institutions and DNFBPs to keep records of customer identification data and transaction information for a specified period.

Key Provisions:

- Maintain customer records for at least five years.
- Ensure records are readily available for competent authorities.

Relevance to CDD:

Adequate record-keeping is crucial for CDD processes as it enables institutions to track and verify customer information over time, aiding in due diligence and investigations.

3. Recommendation 12 - Politically Exposed Persons (PEPs):

Objective:

Recommendation 12 addresses the risk posed by Politically Exposed Persons (PEPs) who hold prominent public positions. It emphasizes enhanced CDD measures for PEPs.

Key Provisions:

- Implement measures to identify and verify the identity of PEPs.
- Assess the source of wealth and funds related to PEPs.
- Continuously monitor PEP relationships.

Relevance to CDD:

Recommendation 12 extends CDD requirements by specifying enhanced due diligence measures for a high-risk category, PEPs, ensuring thorough scrutiny of their financial activities.

4. Recommendation 22 - Beneficial Ownership:

Objective:

Recommendation 22 focuses on transparency of legal persons and arrangements. It requires countries to ensure access to accurate and up-to-date beneficial ownership information.

Key Provisions:

- Maintain accurate records of beneficial ownership.

- Allow competent authorities access to beneficial ownership information.
- Impose sanctions for non-compliance.

Relevance to CDD:

Accurate identification of beneficial owners is a crucial part of CDD, and Recommendation 22 reinforces this by emphasizing transparency and access to beneficial ownership information.

GLOSSARY	
CDD	Customer/Client Due Diligence
EDD	Enhanced Due Diligence
AML	Anti-Money Laundering
CFT	Counter-Terrorism Financing
RFs	Reporting Firms
FATF	Financial Action Task Force
PEPs	Politically Exposed Persons
NGOs/NPOs	Non-Governmental Organizations/Non-Profit Organizations
STR	Suspicious Transaction Report