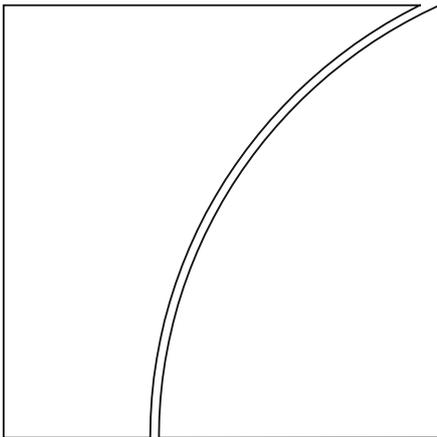


Basel Committee on Banking Supervision

Consultative Document

General guide to account opening



July 2015



BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

© *Bank for International Settlements 2015. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISBN 978-92-9197-181-7 (print)

ISBN 978-92-9197-179-4 (online)

Contents

- General guide to account opening 1
- I. Background 1
- II. Introduction..... 1
- III. Natural persons..... 3
 - A. Identification of individuals who are customers or beneficial owners 3
 - B. Information related to the customer’s risk profile..... 3
 - C. Verification of identity of natural persons 4
 - D. Further verification of information on the basis of risks 5
- IV. Legal persons and arrangements and beneficial ownership 5
 - A. Legal persons..... 5
 - 1. Identification of legal persons..... 6
 - 2. Information for defining the risk profile of a customer which is a legal person 6
 - 3. Verification of identity of legal persons..... 7
 - 4. Verification of identity of authorised signatories and of beneficial owners of the customer. 8
 - B. Legal arrangements 8
 - 1. Identification of legal arrangements..... 8
 - 2. Information for defining the risk profile of a customer which is a legal arrangement..... 8
 - 3. Verification of information..... 9
 - 4. Verification of identity of authorised signatories and of beneficial owners of the legal arrangement 9
 - C. Focus on specific types of customer 9
 - 1. Retirement benefit programmes..... 9
 - 2. Mutuels/friendly societies, cooperatives and provident societies 10
 - 3. Professional intermediaries..... 10

General guide to account opening

I. Background

1. In 2013, the Basel Committee on Banking Supervision (the Basel Committee) reviewed two of its publications on anti-money laundering and countering financing of terrorism (AML/CFT). In January 2014, it published the guidelines for a *Sound management of risks related to money laundering and financing of terrorism* (hereafter “the guidelines”). This document revised, updated and merged two previous publications of the Basel Committee, issued in 2001 and 2004.

2. As part of its continuous effort to keep its publications up-to-date, the Basel Committee is now proposing a revised version of the *General guide to account opening and customer identification* first issued in 2003. This revised version takes into account the significant enhancements to the Financial Action Task Force (FATF) Recommendations and related guidance. It builds in particular on the February 2012 version of the FATF Recommendations, as well as on two supplementary FATF publications specifically relevant for this guide: the *Guidance for a risk-based approach the banking sector* and the *Transparency and beneficial ownership*, both issued in October 2014.

3. The Basel Committee deems it worthwhile to keep this guide as an annex to the guidelines. Most bank-customer relationships start with an account opening procedure. The customer information collected and verified at this stage is crucial to the bank in order for it to fulfil its AML/CFT obligations, both at the inception of the customer relationship and thereafter. All banks need to establish policies and procedures for account opening and these policies and procedures have to reflect AML/CFT obligations.

4. As for the remainder of the guidelines, the content of the proposed guide is in no way intended to strengthen, weaken or otherwise modify the FATF standards. Rather, it aims to support banks in implementing the FATF standards and guidance, which requires the adoption of specific policies and procedures, in particular on account opening.

5. The proposed document expands on the discussion in Section II.3 (paragraphs 35–41 in particular) of the guidelines, entitled “Customer and beneficial owner identification, verification and risk profiling”. It should be read in conjunction with the guidelines. More specifically, the document will be included as an annex to the guidelines, in addition to the three existing annexes that address:

- Using another bank, financial institution or third party to perform customer due diligence;
- Correspondent banking; and
- List of relevant FATF standards.

II. Introduction

6. This annex is a general guide detailing the principles set out in the main body of these guidelines (paragraphs 35–41). This guide focuses on account opening. It is not intended to address every eventuality, but instead to focus on some of the mechanisms that banks can use in developing an effective customer identification and verification programme. It also sets out the information that should be gathered at the time of account opening and which will help the bank to complete the customer risk profile.

7. For the purpose of this Annex, an account is defined as any formal banking or business relationship established by a bank to provide or engage in products, services, dealings, or other financial transactions. This includes demand deposits, savings deposits, or other transaction or asset accounts, or credit accounts or other extension of credit. In keeping with the scope of the original document issued by the Basel Committee in 2003, this guide only covers the opening of new accounts and not the conducting of occasional transactions.

8. The guidance set out in this annex may be adapted for specific application by banks in respect of their AML/CFT policies and procedures and by national financial supervisors seeking to further enhance the effectiveness of customer identification and verification programmes and of customer risk profiles. Supervisors recognise that any customer identification/verification programme should reflect the risks associated with the different types of customer, types of banking product and the varying levels of risk resulting from a customer's relationship with a bank. Higher-risk customer relationships and transactions, such as those associated with politically exposed persons (PEPs)¹ or other higher-risk customers, will clearly require greater scrutiny than relationships and transactions associated with lower-risk customers. Therefore, the provisions in this guide should be read in conjunction with the main body of the guidelines, and in particular with the provisions related to assessing and understanding risks (see paragraphs 15 or 16 of the guidelines) and should be adapted for identified specific (higher- or lower-) risk situations.

9. Guidance and best practice established by national financial supervisors should be commensurate with the risks present in the jurisdiction as well as those associated with categories of customers, products and services that are most prevalent in the particular bank. For this reason, customer identification and verification policies and procedures are expected to vary between countries.

10. In designing and implementing customer identification programmes and establishing a customer's risk profile, banks should take into account the risks associated with each type of financial product or service that is utilised by the customer in this relationship as well as the delivery channel and the geographical area. According to this risk-based approach, jurisdictions may allow simplified customer due diligence measures to be applied for lower-risk situations. For example, some jurisdictions have either taken or supported actions to encourage financial inclusion by promoting lower-risk financial products (such as an account associated with a limited set of services for specific types of customer). Conversely, in cases where there is higher-risk (as may be the case for products featuring non face-to-face or anonymity of certain transactions,² or that are vulnerable to fraud), banks should apply enhanced due diligence.

11. According to the FATF standards,³ banks should always identify the customer and verify its identity. When doing so, banks should be conscious that some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the validity of the document(s) presented, the verification requirement should be enhanced and the information provided by the customer should be verified through additional inquiries or other sources of information.

¹ See in particular the *FATF Guidance on Politically Exposed Persons* (recommendations 12 and 22), www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

² Anonymous accounts are prohibited by the FATF but some products (prepaid cards, virtual currencies) could open the way for anonymous transactions.

³ See recommendation 10.

12. The rest of this annex is divided into two sections covering different aspects of customer identification. Section III describes what types of information should be collected and verified for natural persons seeking to open accounts. Section IV describes what types of information should be collected and verified for legal persons and legal arrangements.

III. Natural persons

A. Identification of individuals who are customers or beneficial owners

13. For natural persons, the bank should collect the following information for identification purposes

At a minimum⁴	Potential additional information (on the basis of risks)
Legal name (first names and last name);	Any other names used (such as marital name, former legal name or alias);
Complete permanent address, whenever applicable;	Professional address, post office box number, e-mail address and landline or mobile telephone numbers;
Nationality, an official personal identification number or other unique identifier ;	Resident status;
Date and place of birth.	Gender.

B. Information related to the customer's risk profile

14. When the account opening is the start of a customer relationship, further information should be collected with a view to developing an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

⁴ Not all this information may be required in lower-risk situations according to the results of the national risk assessment. The list does not include other basic requirements that are not specifically AML-related, such as collecting the signatures of the account holders.

Key attributes⁵	Potential additional information (on the basis of risks)
Occupation, public position held;	Name of employer, where applicable;
Income;	Sources of customer's wealth;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Sources of funds passing through the account;
Financial products or services requested by the customer.	Destination of funds passing through the account.

C. Verification of identity of natural persons

15. The verification should be proportionate to the risk posed by the customer and to the types of document produced. The bank should verify the information, collected according to paragraph 13 and related to the identity of the customer, using reliable, independently sourced documents, data or information. The bank should take reasonable measures to verify the identity of the customer's beneficial owner. Examples are given below. They are not the only possibilities. In some jurisdictions, there may be other documents or verification processes of an equivalent nature that could be used to satisfactorily confirm a customer's identity.

(a) *Documentary verification procedures*

- confirming the identity of the customer or the beneficial owner from an unexpired official document (eg passport, identification card, residence permit, social security records, driver's licence) that bears a photograph of the customer;
- confirming the date and place of birth from an official document (eg birth certificate, passport, identity card, social security records);
- confirming the validity of official documentation provided through certification by an authorised person (eg embassy official, public notary); and
- confirming the permanent address (eg utility bill, tax assessment, bank statement, letter from a public authority).

(b) *Non-documentary verification procedures*

- contacting the customer by telephone or by letter to confirm the information supplied, after an account has been opened (eg a disconnected phone, returned mail etc should warrant further investigation);
- checking references provided by other financial institutions; and
- using non-documentary verification methods, such as public and private databases.

⁵ These key attributes are useful in establishing the first step of the customer's risk profile; they might not be required in lower-risk situations, depending on the results of the national risk assessment.

16. Banks should verify that any person purporting to act on behalf of the customer is so authorised. If so, banks should identify and verify the identity of that person. In such a case, the bank should also verify the authorisation to act on behalf of the customer (a signed mandate, an official judgment or equivalent document).

D. Further verification of information on the basis of risks

17. Particular attention needs to be focused on those customers assessed as having higher-risk profiles (eg PEPs). Additional sources of information and enhanced verification procedures may include:

- evidence of an individual's permanent address utilising official papers, a credit reference agency search, or through independent verification by home visits;
- personal reference (ie by an existing customer of the same bank);
- prior bank reference (including banking group reference) and contact with the bank regarding the customer;
- verification of income sources, funds and wealth identified through appropriate measures; and
- verification of employment and of public positions held.

18. If national law allows for non-face-to-face account opening, banks should take into account the specific risks associated with this method. Customer identification and verification procedures should be equally effective and similar to those implemented for face-to-face interviews. In particular, banks should (i) establish that the customer exists; and (ii) establish that the person the bank is dealing with is that customer.

19. As part of its broader customer due diligence measures, the bank should consider, on a risk-sensitive basis, whether the information regarding sources of wealth should be corroborated.

IV. Legal persons and arrangements and beneficial ownership

20. The underlying principles of customer identification for natural persons can be applied equally to identifying and verifying customers who are legal persons and arrangements. Accordingly, the procedures discussed previously in Section III (paragraphs 13–19) are similarly applicable to legal persons and arrangements. Banks should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure, with a view to establishing a customer risk profile.

A. Legal persons⁶

21. The term legal person includes any entity (eg business or non-profit organisation, distinct from its officers and shareholders) that is not a natural person or a legal arrangement. In considering the

⁶ FATF definition: "legal persons" refers to any entities other than natural persons that can establish a permanent customer relationship with a bank or otherwise own property. This can include companies, bodies corporate, foundations, *Anstalt*-type structures, partnerships, or associations and other relevantly similar entities.

customer identification guidance for the different types of legal persons, particular attention should be given to the different levels and nature of risk associated with these entities.

1. Identification of legal persons

22. For legal persons, the following information should be obtained for identification purposes:

At a minimum ⁷	Potential additional information (on the basis of risks)
Name, legal form, status and proof of incorporation of the legal person;	
Permanent address of principal place of the legal person's activities;	
Official identification number (company registration number, tax identification number);	Legal entity identifier (LEI) if available;
Mailing and registered address of legal person;	Contact telephone and fax numbers.
Identity of natural persons who have authority to operate the account and who exercise control of the legal person through ownership or other means. In the absence of a natural person, the identity of the relevant person who is the senior managing official.	Identity of relevant persons holding senior management positions.
Identity of the beneficial owners ⁸ (according to relevant FATF standards and paragraph 13 of this annex); ⁹	
Powers that regulate and bind the legal person.	

2. Information for defining the risk profile of a customer which is a legal person

23. When the account opening is the start of a customer relationship, further information should be collected with a view to developing an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

⁷ Not all this information may be required in lower-risk situations depending on the results of the national risk assessment. The list does not include other basic requirements that are not specifically AML-related, such as collecting the signatures of the account holders.

⁸ The term "beneficial owner" is used in this annex in a manner consistent with the definition and clarifications provided in the FATF standards. For reference, the FATF defines a "beneficial owner" as the natural person(s) who ultimately owns or controls a customer and/or natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

⁹ See *Interpretative note to recommendation 10* of the FATF. See also FATF, *Transparency and beneficial ownership*, October 2014, www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

At a minimum ¹⁰	Potential additional information (on the basis of risks)
Nature and purpose of the activities of the legal entity and its legitimacy;	Financial statements of the entity;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Sources of funds paid into the account and destination of funds passing through the account.

3. Verification of identity of legal persons

24. The bank should verify the identity of the customer using reliable, independent source documents, data or information. The verification should be proportionate to the assessment of risk tied to the customer and to the types of document produced by the customer. The bank should obtain:

- a copy of the Certificate of Incorporation and Memorandum and Articles of Association, or Partnership agreement (or any other legal document certifying the existence of the entity, eg abstract of the registry of companies/commerce);

25. Examples of other verification include:

(a) *Documentary verification*

- for established corporate entities – reviewing a copy of the latest financial statements (audited, if available).

(b) *Non-documentary verification*

- undertaking a company search and/or other commercial enquiries to ensure that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (eg lawyers, accountants);
- validating the LEI and associated data in the public access service;
- obtaining prior bank references;
- visiting the corporate entity, where practical; and
- contacting the corporate entity by telephone, mail or e-mail.

26. The list of examples included in paragraph 25 is not exhaustive. In some jurisdictions, there may be other documents of an equivalent nature, such as procedures or sources of information, which may be produced, applied or accessed as satisfactory evidence of a customer's identity.

¹⁰ Not all this information may be required in lower-risk situations depending on the results of the national risk assessment. The list does not include other basic requirements that are not specifically AML-related, such as collecting the signatures of the account holders.

4. Verification of identity of authorised signatories and of beneficial owners of the customer

27. Banks should verify that any person purporting to act on behalf of the legal person is so authorised. If so, banks should verify the identity of that person. This verification should entail verification of the authorisation to act on behalf of the customer (a signed mandate, an official judgment or equivalent document).

28. Banks should undertake reasonable measures to verify the identity of the beneficial owners, in accordance with the FATF definition referenced in footnote 9 and the due diligence procedures for natural persons outlined in Section III above.

B. Legal arrangements¹¹

1. Identification of legal arrangements

29. For legal arrangements, the following information should be obtained:

At a minimum¹²	Potential additional information (on the basis of risks)
Name of the legal arrangement and proof of existence;	Contact telephone and fax numbers.
Address, and country of establishment;	
Nature, purpose and objects of the legal arrangement (eg is it discretionary, testamentary etc);	
The names of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (including through a chain of control/ownership);	The names of the relevant persons having a senior management position in the legal arrangement, if relevant.

2. Information for defining the risk profile of a customer which is a legal arrangement

30. When the account opening is the start of a customer relationship, further information should be collected with a view to develop an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

¹¹ The term “legal arrangements” is used in this annex consistently with the definition provided by the FATF standards. As a reminder, the FATF defines “legal arrangements” as express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include *fiducie*, *Treuhand* and *fideicomiso*.

¹² Not all this information may be required in lower-risk situations depending on the results of the national risk assessment. The list does not include other basic requirements that are not specifically AML-related, such as collecting the signatures of the account holders.

At a minimum ¹³	Potential additional information (on the basis of risks)
Description of the purpose/activities of the legal arrangement (eg in a formal constitution, trust deed);	Source of funds;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Destination of funds passing through the account.

3. Verification of information

31. The bank should verify this information, at least by obtaining a copy of documentation confirming the nature and legal existence of the account holder (eg a deed of trust, register of charities). Other procedures of verification could include:

- obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- obtaining prior bank references; and
- accessing or searching public and private databases or other reliable independent sources.

32. Banks should undertake reasonable measures to verify the identity of the beneficial owners of the legal arrangements, in accordance with Section III above.

4. Verification of identity of authorised signatories and of beneficial owners of the legal arrangement

33. Banks should verify that any person purporting to act on behalf of the legal arrangement is so authorised. If so, banks should verify not only the identity of that person but also the person's authorisation to act on behalf of the legal arrangement (by means of a signed mandate, an official judgment or another equivalent document).

34. Banks should undertake reasonable measures to verify the identity of the beneficial owners.

C. Focus on specific types of customer

1. Retirement benefit programmes

35. Where an occupational pension programme, employee benefit trust or share option plan is an applicant for an account, the trustee and any other person who has control over the relationship (eg administrator, programme manager or account signatories) can be considered as beneficial owners and the bank should take steps to identify them and verify their identities.

¹³ Not all this information may be required in lower-risk situations depending on the results of the national risk assessment. The list does not include other basic requirements that are not specifically AML-related, such as collecting the signatures of the account holders.

2. Mutuals/friendly societies, cooperatives and provident societies

36. Where these entities are applicants for accounts, those persons exercising control or significant influence over the organisation's assets should be considered the beneficial owners and therefore identified and verified. This will often include board members as well as executives and account signatories.

3. Professional intermediaries

37. When a professional intermediary opens a customer account on behalf of a single customer that customer must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities. Where funds held by the intermediary are not co-mingled but "sub-accounts" are established which can be attributed to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the bank should look through to the beneficial owners. However, there may be circumstances – which should be permitted by law and set out in supervisory guidance – where the bank may not need to look beyond the intermediary (eg when the intermediary is subject to the equivalent due diligence standards in respect of its customer base as the bank, such as could be the case for broker-dealers).

38. Where such circumstances apply and an account is opened for an open or closed-end investment company, unit trust or limited partnership that is subject to customer due diligence requirements which are equivalent to those applying to the bank itself, the bank should treat this investment vehicle as its customer and take steps to identify:¹⁴

- the fund itself;
- its directors or any controlling board where it is a company;
- its trustee where it is a unit trust;
- its managing (general) partner where it is a limited partnership;
- account signatories; and
- any other person who has control over the relationship eg fund administrator or manager.

39. Where other investment vehicles are involved, the same steps should be taken as in paragraph 38 where it is appropriate to do so. In addition, in cases when no equivalent due diligence standards apply to the investment vehicle, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.

40. Intermediaries should be treated as individual customers of the bank and the standing of the intermediary should be separately verified by applying the appropriate methods listed in paragraphs 22–26 above.

¹⁴ When the domestic AML requirements do not require all this information to be collected but, as a minimum, only one of the items mentioned, the account-opening bank should consider collecting the other items as additional information.