GLOBAL INVESTIGATIONS & COMPLIANCE

ELLEN ZIMILES
Managing Director
Financial Services Advisory and Compliance Segment Leader
Head of Global Investigations & Compliance
212.554.2602
ellen.zimiles@navigant.com

ALMA ANGOTTI
Managing Director
202.481.8398
alma.angotti@navigant.com

BRANDY SCHINDLER
646.227.4881
brandy.schindler@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

BCBS REVISED GENERAL GUIDE TO ACCOUNT OPENING:

PROTECTING AGAINST MONEY LAUNDERING AND COUNTER FINANCING THREATS WITH A RISK-BASED APPROACH

I. OVERVIEW

On February 4, 2016, the Basel Committee on Banking Supervision ("BCBS") issued a revised version of its *General guide to account opening ("Revised Guide")*.[1] The Revised Guide replaces BCBS's *General Guide to Account Opening and Customer Identification*, issued in February 2003, and emphasizes a risk-based approach to an institution's account opening process.

1. The full General guide to account opening is available as Annex 4 here: https://www.bis.org/bcbs/publ/d353.pdf

The key differences between the two guides are summarized in the table below.

ACCOUNT OPENING PROCEDURES	REVISED GENERAL GUIDE TO ACCOUNT OPENING (2016)	GENERAL GUIDE TO ACCOUNT OPENING AND CUSTOMER IDENTIFICATION (2003)
Build a Customer Risk Profile	The Customer's Risk Profile must be: A. Established before an account is opened; and B. Based on the following: a. Product or service, b. Delivery Channel and geography, c. Type of customer.	The Customer's Risk Profile must be: A. Established after account is opened and initial documentation is received; and B. Based on the following: a. Type of customer and b. Relationship with the Institution.
Collect Documentation	Document collection should be guided by the following principles: A. Documentation received should be analyzed; this analysis will drive a customer's risk profile. B. Documentation should be collected for: a. Identifying the customer and b. Building a customer's risk profile. C. The quantity and type of documentation collected should be based on a customer's risk profile.	The identification of a customer should be made through the collection of specific documentation. Higher risk transactions and relationships requires greater scrutiny of the documentation.
Verify Documentation	When verifying documentation, an institution should: A. Use reliable, independently sourced documents; B. Use verification measures proportionate to the customer's risk; and C. If necessary, use both documentary and non-documentary procedures.	Verification of the documentation should be made by using at least one of the methods listed in the Guide.
Identify the Natural Persons behind Legal Persons	For legal persons opening an account, an institution must: A. Verify the identity of the beneficial owners; and[2] B. For natural persons acting on behalf of the legal person, an institution must: a. Verify his or her authorization to act on behalf of the legal person and b. Verify the identity of the natural person.	For legal persons opening an account, an institution must: A. Verify the identity of shareholders, signatories or others who inject a significant proportion of capital or financial support, or who otherwise exercise control; and B. Take reasonable steps to verify the identity and reputation of any agent that opens the account, if the agent is not an officer of the corporation
Identify the Natural Person behind Legal Arrangements	For legal arrangements opening an account, an institution must: A. Identify the natural persons who are authorized to operate the account or the identity of the relevant person who is the senior managing official; and B. Identify the beneficial owners.	For legal arrangements opening an account, an institution must identify the principals, partners and/or immediate family members that have ownership control.

2. Beneficial owners is defined as the natural person(s) who ultimately owns or controls a customer and/or the 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 arrangements. This definition has been sourced from the FATF Recommendations' General Glossary.

As institutions bring innovative products and services to market, it is imperative that they identify and mitigate any additional compliance risks they may pose. The account opening process is an institution's first line of defense against money laundering and terrorist financing schemes, as the accurate classification of a customer's risk profile is essential to fulfilling an organization's anti-money laundering ("AML") and countering financing of terrorism ("CFT") responsibilities. Accurate classification, and the subsequent application of simplified or enhanced due diligence ("EDD"),[3] ensures proper resource allocation within an effective compliance program.

The Revised Guide is published as an annex to the Sound management of risks related to money laundering and financing of terrorism[4] and heavily reflects the following Financial Action Task Force publications:

A. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2012);* [5]

B. *Guidance for a Risk-Based Approach: The Banking Sector (2014);*[6] and

C. *FATF Guidance: Transparency and Beneficial Ownership (2014).*[7]

Senior compliance staff should review the Revised Guide as soon as possible to confirm that account opening procedures identify and verify customers based on AML/CFT risk. To provide additional direction and support, Navigant has summarized key takeaways from the Revised Guide.

II. II. RISK ASSESSMENT FACTORS PRIOR TO ACCOUNT OPENING

An institution should begin building a customer risk profile even before substantive documentation is collected at account opening. This initial risk profile should be based on a combination of factors. At a minimum, the following factors should be considered when developing the customer risk profile prior to account opening:[8]

A. Customer Risk;

B. Country or Geographic Risk; and

C. Product, Service, Transaction or Delivery Channel Risk.

The risk assessment undertaken prior to account opening will inform the identification and verification procedures that follow.

III. BUILDING A CUSTOMER RISK PROFILE THROUGHOUT THE ACCOUNT OPENING PROCESS

Once an initial customer risk profile is developed, the institution can begin the identification and verification process. It is important to note that this is a dynamic process: as an institution gathers information, it will be in a better position to evaluate the risks presented. If a customer is perceived to present greater risk, supplementary identification information should be gathered at account opening.

Since different types of customers require unique identification and verification procedures, the Revised Guide discusses the following entities separately: natural persons, legal persons, legal arrangements and specific types of customers. This alert will follow the same format.

A. Natural Persons [9]

1. Identification Procedures

   The Revised Guide provides a table which highlights the data types required to identify natural persons as it relates to meeting an organization's AML/CFT requirements.[10] Examples of the identification types listed include: legal name, address and date of birth.[11] Not all data types listed will be required all of the time, however, as the information collected for identification should be driven by the customer risk profile.

3. Additional information regarding enhanced due diligence can be found in the FATF's Interpretive Note to Recommendation 10
4. The full Sound management of risks related to money laundering and financing of terrorism is available here: https://www.bis.org/bcbs/publ/d353.pdf
5. The full International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations is available here: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
6. The full Guidance for a Risk-Based Approach: The Banking Sector is available here: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf
7. The full FATF Guidance: Transparency and Beneficial Ownership is available here: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf
8. The risk factors listed have been sourced from FATF's Interpretive Note to Recommendation 10
9. In this context, natural persons can be defined as individuals, not business entities, non-profits, or other legal persons
10. Other information may be collected as part of the regular account opening process that is not relevant to combating AML/CFT, such as customer signature
11. This is not the full list and serves only to provide an illustration of the types of information recommended for collection

It is important for an institution to be aware that when a customer is legitimately unable to provide certain information, the customer's access to the formal banking sector should not be impeded. Instead of refusing to serve the customer, the Revised Guide recommends institutions find alternative methods of identification or implement additional risk mitigation techniques, such as heightened account monitoring.

2. Risk Profile

A customer's risk profile should be enhanced throughout the account opening process. The Revised Guide suggests the following information be collected to form the key elements of a customer's risk profile:

a. Occupation/public position held;

b. Income, expected use of the account; and

c. Financial products or services requested by the customer.

Additional information that may be collected based on the institution's risk assessment includes:

a. Name of employer;

b. Source of wealth; and

c. Sources and destinations of funds.

3. Verification

According to the Revised Guide, verification of a natural person should be made using "reliable, independently sourced documents, data or information."[12] Compliance officers should be aware that some documentation is more susceptible to fraud than others, such as counterfeit and stolen passports. In order to mitigate this risk, both documentary (e.g. passport, driver's license, utility bill) and non-documentary (e.g. attempt to contact the customer via telephone, fax or email) verification procedures should be put into place.

Similar to the identification process, the intensity of the verification process should reflect the risk posed by the customer.

B. Legal Persons[13]

1. Identification Procedures

The Revised Guide provides a table highlighting data types required to identify legal persons for the purpose of fulfilling an institution's AML/CFT requirements. Examples of the identification types listed include:[14] name, address and official identification number. Not all data types will be required in every instance. The information collected for identification should be driven by the customer risk profile.

When a legal person requests an account, it is imperative that information is also collected on the natural persons behind the application. This includes natural persons who are authorized to operate the account or who manage the legal person, as well as any beneficial owners.[15]

2. Risk Profile

A legal person's risk profile should be developed throughout the account opening process. The Revised Guide suggests institutions collect the following information to form the key elements of a customer's risk profile:

a. Nature and purpose of the legal persons activities, as well as the activities' legitimacy; and

b. Expected use of the account.

Additional information that may be collected based on the institution's risk assessment includes:

a. Financial situation of the legal person; and

b. Sources and destination of funds.

12. Bank for International Settlements, Feb. 2016. Sound Management of Risks Related to Money Laundering and Financing of Terrorism. Available at: < http://www.bis.org/bcbs/publ/d353.pdf > [Accessed 11 February 2016]

13. Legal Persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships,

14. This is not the full list and serves only to provide an illustration of the types of information recommended for collection

15. According to the FATF's Guidance on Transparency and Beneficial Owner, 'beneficial owners refers to the natural person(s) who ultimately owns or controls a customer and/or the 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.'

3. Verification

According to the Revised Guide, verification of a legal person should be made using "reliable, independently sourced documents, data or information."[16] As with natural persons, institutions should verify legal persons using both documentary and non-documentary evidence. Documentary evidence may include review of financial statements and non-documentary evidence may include an attempt to contact or prior bank references.

The natural persons behind the legal persons should be identified and verified based on the natural person process described in Section A. It should also be verified that the natural persons have the authorization to act on behalf of the legal person.

As with the verification of natural persons, the verification process for legal persons should correspond to the customer risk profile. Higher risk customers should be held to a higher degree of scrutiny.

C. Legal Arrangements[17]

1. Identification Procedures

The Revised Guide provides a table which highlights the data types required to identify legal arrangements as it relates to meeting an organization's AML/CFT requirements. Examples of the identification types listed include: name, country of establishment, proof of existence and purpose of arrangement.[18] Not all data types listed in the table will be required in every circumstance, as the information collected for identification should be driven by the customer risk profile.

When an account is requested for a legal arrangement, it is imperative that information is also collected on the natural persons behind the application. This includes natural persons who are managers, settlors, trustees, protectors, signatories, beneficiaries and those who have ultimate effective control over the legal arrangement.

2. Risk Profile

A legal arrangement's risk profile should be developed throughout the account opening process. The revised guide suggests the following information be collected to form the key elements of a customer's risk profile:

a. Description of the purpose/activities of the legal arrangement; and

b. Expected use of the account.

Additional information that may be collected based on the institution's risk assessment includes:

a. Source of funds; and

b. Origin and destination of funds.

3. Verification

Verification of a legal arrangement should be made using "reliable, independently sourced documents, data or information" and compliance officers should be aware that some documentation is more susceptible to fraud than others.[19] In order to mitigate this risk, both documentary (e.g. collecting a copy of the deed of trust) and non-documentary (e.g. prior bank references) verification procedures should be put into place.

The natural persons behind the legal arrangements should be identified and verified based on the natural person process described above in section A. Institutions should also verify that the natural persons have the authorization to act on behalf of the legal arrangement.

Institutions should take a risk-based approach to the verification process corresponding to the risk profile of the legal arrangement.

16. Bank for International Settlements, Feb. 2016. Sound Management of Risks Related to Money Laundering and Financing of Terrorism. Available at: < http://www.bis.org/bcbs/publ/d353.pdf > [Accessed 11 February 2016]

17. Legal arrangements refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso. This definition has been sourced from the FATF Recommendations' General Glossary.

18. This is not the full list and serves only to provide an illustration of the types of information recommended for collection

19 Bank for International Settlements, Feb. 2016. Sound Management of Risks Related to Money Laundering and Financing of Terrorism. Available at: < http://www.bis.org/bcbs/publ/d353.pdf > [Accessed 11 February 2016]

D. Specific Customer Types

The Revised Guide further highlights specific customers types and makes recommendations related to an institution's account opening procedures on behalf of these customers. The customers highlighted in the revised guide include:

1. Retirement Benefit Programs;

2. Mutual/friendly societies, cooperatives and provident societies;

3. Professional Intermediaries; and

4. Investment Company, Unit Trust or Limited Partnership.

The Revised Guide emphasizes it can be difficult to identify the natural person behind the account in the listed customer types. Nevertheless, it is important institutions take "all reasonable steps should be taken to verify the identity of the beneficial owners and those who have control."

IV. KEY CONSIDERATIONS FOR SENIOR COMPLIANCE OFFICERS

Senior compliance officers should review their own account opening procedures to ensure that they meet the expectations of the Revised Guide. Institutions should understand the risks inherent in their own products, delivery channels and geographies even before opening an account for a new customer. As the account opening process proceeds, standard documentation is sufficient for customers that are low risk; additional resources should be allocated towards collecting and verifying supplementary documentation for high-risk customers.

V. HOW NAVIGANT CAN HELP

A. Risk Assessment

Navigant can conduct a comprehensive review of your organization and assess the potential risks associated with customers, products and services, delivery channels and geographic locations.

B. Development and Delivery of Training and Educational Programs

Navigant can help your financial institution develop and deliver training materials that clearly and concisely interpret applicable legal, regulatory, policy and procedural requirements as well as the possible ramifications associated with non-compliance.

C. Customer Reviews

Navigant can perform Know Your Customer ("KYC") and EDD file remediation.