OVERVIEW

No. RADAR
5926

Responsible level
EU

Competent authority
EBA – European Banking Authority

Standard designation
Guidelines on strategies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services

Title of Standard
Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services

Abbreviation (standard)

Short Title

Abbreviation (standard)
EBA/GL/2023/04

Abbreviation
EBA/GL/2023/04

Implementation status of the standard
published

Industry relevance
Banking, insurance

category
08. Anti-money laundering and financial sanctions

Document type
Guideline

Management Summary
The EBA analyzed the scope and impact of de-risking in the EU. De-risking refers in this context to decisions by credit and financial institutions not to enter into or to terminate business relationships with individual customers or customer categories that pose a higher risk of money laundering and terrorist financing (ML/TF). Certain customer groups, such as non-profit organizations (Not for

Profit Organisations (NPOs) and refugees were identified as particularly vulnerable to unjustified de-risking.

Against this background, these Guidelines establish new principles, procedures and controls that credit and financial institutions should implement to mitigate and effectively manage ML/TF risks in accordance with Article 8(3) of the *Directive (EU) 2015/849 (dataset 897)*. This also includes situations to which the provisions of Article 16 of the *Directive 2014/92 (Payment Accounts Directive (PAD, dataset 955)* which govern the right of individuals to open and maintain a payment account with basic features.

Management Summary

EBA analyzed the scale and the impact of de-risking in the EU. De-risking refers, in this context, to decisions made by credit and financial institutions to refuse to enter into, or to terminate, business relationships with individual customers or categories of customers associated with higher money laundering/financing of terrorism (ML/TF) risk. EBA highlighted certain categories of customers as particularly vulnerable to unwarranted derisking, including refugees and Not-for-Profit organizations (NPOs).

Against this background, the present guidelines set out policies, procedures and controls credit and financial institutions should have in place to mitigate and effectively manage ML/TF risks in accordance with Art. 8(3) of *Directive (EU) 2015/849 (dataset 897)*. The specification includes situations where provisions in Art. 16 of *Directive (EU) 2014/92 (PAD, dataset 955)* apply, which provide the right of individuals to open and maintain a payment account with basic features.

CONTENTS

Main content

1. Credit and financial institutions should set up their strategies, controls and procedures in a way that enables them to identify the relevant risk factors and to assess the risks of money laundring and financing of terrorism (ML/TF) in accordance with the requirements of the EBA Guidelines (EBA/GL/2021/02) pursuant to Article 17 and Article 18(4) of the *Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, amending Regulation (EU) No 648/2012 (4th Anti-Money Laundering Directive, Dataset 897)* on due diligence obligations and the factors that credit and financial institutions should take into account when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions ("The Guidelines on risk factors for money laundering and terrorist financing"), repealing and replacing the *Guidelines JC/2017/37 (Dataset 4032*) is possible.

2. Ensure that the implementation of the policies, procedures and controls does not lead to

blanket rejection or termination of business relationships with entire customer categories whose ML/TF risk was assessed as higher.

3. Before credit and financial institutions reject a customer due to high ML/TF risks, policies, procedures, and controls should specify mitigating options for the higher ML/TF risks, which should be considered before a negative decision is taken. These options should include, at a minimum, adjusting the scope and intensity of monitoring and, where permitted by national law, applying targeted restrictions on products and services. The policies and procedures should clearly specify in which cases these mitigating measures are appropriate.

4. Before taking a decision to reject or terminate a business relationship, credit and financial institutions should ensure that they have considered all possible risk mitigation measures that could reasonably be applied in that specific case, taking into account the MT/TF risk associated with the existing or future business relationship.

5. For the purposes of the reporting obligations under Article 33 of Directive (EU) 2015/849, institutions should set out in their procedures grounds for considering a suspicion or attempt to commit ML/TF.

6. Credit and financial institutions should document and justify any decision to reject or terminate a business relationship. Furthermore, they should be prepared to make these documents available to their competent authority upon request.

7. With regard to the right of access to a payment account with basic features pursuant to Article 16(2) and Article 17 of the*Directive 2014/92/EU of the European Parliament and of the Council on comparability of payment account fees, payment account switching and access to payment accounts with basic features (Payment Accounts Directive, PAD, dataset 955)*Credit institutions that are required to offer such basic accounts should set out in their account opening policies and procedures how they can adapt their customer due diligence measures to take account of the fact that the limited features of a basic account help to mitigate the risk of misuse of these products and services by the customer for financial criminal purposes.

8. When ensuring non-discriminatory access to a basic payment account within the meaning of Article 15 of Directive 2014/92/EU, credit institutions should ensure that digital solutions for establishing a business relationship also comply with that Directive and these Guidelines and that the digital solutions do not generate automatic rejections that are contrary to that Directive and these Guidelines.

9. Credit and financial institutions should, over time and as their understanding of the ML/TF risk associated with individual business relationships grows, update the individual customer risk assessment and adjust the level of monitoring and the type of products and services for which the customer is eligible.

II. Adjustment of the intensity of monitoring measures (Title 2)

1. Credit and financial institutions should set out in their policies and procedures how they adapt the scope and intensity of monitoring to the ML/TF risk associated with the customer, in accordance with EBA/GL/2021/02 on risk factors. To effectively manage the ML/TF risk associated with a customer, monitoring should include at least the following steps:

- Establishing expectations regarding customer behavior, such as the type and amount, source and recipient of transactions, so that the institution is able to detect unusual transactions;

- Ensuring regular review of the customer account to determine whether changes to the customer's risk profile are justified;

- Ensure that any changes to the previously obtained CDD information that may affect the institution's assessment of the ML/TF risk associated with the individual business relationship are taken into account.

2. The policies and procedures of credit and financial institutions should include guidelines for the treatment of applications from persons who, for credible and legitimate reasons, are unable to present traditional forms of identification. These should specify at least the following aspects:

- the steps to be taken if the client is an asylum seeker and cannot provide the credit and financial institution with conventional identification documents such as passports or identity cards (see source for details). Institutions' policies and procedures should specify which alternative, independent documents are accepted to meet customer due diligence obligations, where permitted by national law. These documents should be sufficiently reliable, i.e., current, issued by a national or local authority, and contain, at a minimum, the applicant's full name and date of birth.

- the measures to be taken if the customer is vulnerable and cannot provide conventional identification documents or has no fixed address, for example, because they are a refugee or homeless (see source for details). Institutions' policies and procedures should specify which alternative, independent documents they can rely on. These documents may include expired identity documents and, where permitted by national law, documents provided by an official authority such as the social welfare office or an established non-profit organization acting on behalf of official authorities (e.g., the Red Cross).

- A similar approach should be taken with applications from persons who do not have an EU residence permit but whose expulsion is impossible. In such cases, credit and financial institutions should take into account in their policies and procedures certificates or documents provided by an official authority, or an organisation acting on its behalf, that provides assistance or legal aid to such persons, where permitted by national law. These authorities may include social services, ministries of the interior, or migration services. These documents can be used as evidence that the person concerned cannot be expelled under EU law;

- In cases where the support for vulnerable customers referred to in points a, b and c is paid out in the form of prepaid cards and the conditions for simplified due diligence measures set out in Guidelines 4.41, 9.15 and 10.18 of EBA/GL/2021/02 are met, a note may be provided stating that credit and financial institutions may defer the application of the initial customer due diligence measures to a later date;

- In cases where customers identified as having a low ML/TF risk request access to a payment account, the alternative means of customer identification accepted by the institution and the possibilities for deferring the fulfilment of full customer due diligence obligations after the establishment of the business relationship shall be specified.

III. Targeted and proportionate restrictions on access to products or services (Title 3)

1. The policies and procedures of credit and financial institutions should, to the extent permitted by national law, include options and criteria for risk-sensitive and individualised adaptation of the features of the products or services offered to a particular customer. These should include the following options:

- Offering payment accounts with basic features, provided that a credit institution is obliged to do so in accordance with the national implementation of Directive 2014/92/EU or
- Imposing targeted restrictions on financial products and services, for example on the amount or number of person-to-person transfers or the amount of transactions to and from third countries, in particular where those third countries involve a higher ML/TF risk, where permitted by national law.

2. With regard to ML/TF risks of particularly vulnerable customers such as refugees and homeless people, credit and financial institutions should ensure that potential product or
Service restrictions within the meaning of paragraph 20b of these Guidelines (see III. 1, second indent above) should be applied, taking into account the individual client's personal situation, the associated ML/TF risk, and their basic financial needs. In these cases, the procedures should include an assessment of the following risk mitigation options:

- no granting of loans or overdrafts;
- monthly turnover limits (unless the reasons for higher or unlimited turnover can be explained and justified);
- Limitation of the amount and/or number of transfers from person to person (additional or larger transfers are possible on a case-by-case basis);
- Limiting the amount of transactions to and from third countries (taking into account the cumulative effect of frequent lower-value transactions within a given period), in particular where those third countries are associated with a higher ML/TF risk;
- Limiting the amount of deposits;
- Limiting third-party payments to payments made by the authority supporting vulnerable customers;
- Limiting the amount of payments received from third parties that have not been verified by the Institute, and
- Prohibition of cash withdrawals from third countries.

IV. Information on complaint mechanisms (Title 4)

In the event of a customer's rejection or termination of a business relationship, credit and financial institutions should ensure in their policies and procedures that customers are informed of their right to lodge a complaint with the relevant supervisory or resolution authorities. For this purpose, the customer must be provided with the relevant contact details (alternatively, the web link https://www.eba.europa.eu/consumer-corner/how-to-complain is sufficient).

CATEGORIZATION

Keywords

Rejection, ID, basic account, CDD, customer due diligence, non-discriminatory access, third country, refugee, money laundering, business relationship, basic function, account opening policy, customer due diligence, termination, ML/TF, ML/TF risk, homeless person, prepaid card, risk factor, risk mitigation, vulnerable customer, terrorism, transfer, overdraft, suspicious transaction reporting obligation, payment account

Legal and information bases

- EBA Guidelines (EBA/GL/2021/02) pursuant to Article 17 and Article 18(4) of Directive (EU) 2015/849 on due diligence measures and the factors that credit and financial institutions should consider when assessing the risk of money laundering and terrorist financing associated with individual business relationships and occasional transactions (The Guidelines on money laundering and terrorist financing risk factors repealing and replacing Guidelines JC/2017/37, Dataset 4032)

- Directive 2014/92/EU (Payment Accounts Directive, PAD, dataset 955)
- Directive (EU) 2015/849 (dataset 897)
- Regulation (EU) No 1093/2010 (Dataset 245)

Related Standards

- Directive 2014/92/EU (PAD, dataset 955)
- Directive (EU) 2015/849 (dataset 897)
- Regulation (EU) No 1093/2010 (Dataset 245)

Target group – credit institutions

Yes

Target group – financial services institutions

Yes

Target group – Other companies in the financial sector

Yes

Target group – payment institutions

Yes

Target group – insurance companies

Yes

Target group – supplement

These guidelines are addressed to competent authorities within the meaning of Article 4(2)(iii) of Regulation (EU) No. 1093/2010. They also address credit and financial institutions within the meaning of Article 3(1) and (2) of Directive (EU) 2015/849, which are financial sector operators within the meaning of Article 4(1a) of Regulation (EU) No. 1093/2010.

Comments

These guidelines are addressed to competent authorities as defined in Art. 4(2) point (iii) of Regulation (EU) No 1093/2010. They are also addressed to credit and financial institutions as defined in Art. 3(1) and 3(2) of Directive (EU) 2015/849, which are financial sector operators as defined in Art. 4 (1a) of Regulation (EU) No 1093/2010.

Statement by (date)

Implementation status Explanation

Status – Further Details

Date of entry into force/publication

03.08.2023

Entry into force estimated?

No

Date of first application

November 3, 2023

Application appreciated?

No

Date Standard repealed

Remark (Entry into force/Publication)

Competent authorities must notify, in all official EU languages, within two months of the publication of the guidelines (publication on 3 August 2023), whether they comply or intend to comply with the guidelines, or give reasons why they do not comply or intend not to comply (comply-or-explain).

The guidelines shall apply three months after their translation into all official EU languages.

Comments

Competent authorities must notify the EBA within two months after the publication (publication on 3 August 2023) of the translations as to whether they comply or intend to comply with these guidelines, or otherwise state their reasons for non-compliance (comply-or-explain).

These Guidelines will apply three months after publication in all EU official languages.

Sources

The sources are not shown in this working paper.