EBA-Op-2016-07

12 April 2016

Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories

Introduction and legal basis

The European Banking Authority (EBA)'s competence to deliver an opinion is based on Article 29(1) (a) of Regulation (EU) No 1093/2010,[1] as anti-money laundering and countering the financing of terrorism (AML/CFT) relate to the EBA's area of competence.

In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors,[2] the Board of Supervisors has adopted this Opinion.

This Opinion is addressed to competent authorities (CAs) as defined in Article 4(2) letter (ii) of Regulation (EU) 1093/2010.

Summary

This Opinion is addressed to competent authorities. It sets out the EBA's view on the application of Customer Due Diligence (CDD) measures to customers who are asylum seekers from higher-risk third countries or territories when they first enter into a business relationship with a credit or financial institution and supports the development of a consistent approach throughout the European Union.

The scale of the current migrant movement, the level of money laundering and terrorist financing (ML/TF) risk associated with many asylum seekers' countries and territories of origin and concerns over the reliability and robustness of some asylum seekers' identity documentation create unique compliance challenges for credit and financial institutions. At the same time, providing asylum seekers with access to at least basic financial products and services is not only a prerequisite for their participation in modern economic and social life, it is also central to the fight against ML/TF:

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

[2] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 27 November 2014 (EBA/DC/2011/01 Rev4).

lack of access can drive financial transactions underground, which makes the detection and reporting of suspicious transactions more difficult.

In this Opinion, the EBA sets out how credit and financial institutions can strike the right balance between providing asylum seekers from higher-risk third countries and territories with access to financial products and services on the one hand, and complying with EU Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) requirements on the other hand. European Union law is sufficiently flexible to permit a proportionate and effective response and the EBA believes that there will be relatively few cases where it will be necessary for a credit or financial institution to decline a business relationship with an asylum seeker from a higher-risk third country or territory on ML/TF grounds. ML/TF risks can in most cases be managed effectively by offering a more limited range of services and/or setting up stricter monitoring controls, which will be conducive to early intervention in the event of suspicion.

The EBA believes that national guidance on this matter is important and calls on competent authorities to consider taking steps to clarify how the views expressed in this Opinion apply under their legal and regulatory framework.

Background and rationale

During 2015, more than one million people made their way to Europe to seek asylum. The majority are fleeing from war and terrorism in their countries of origin, including Syria and Afghanistan.[3] European governments therefore have to find ways to manage large numbers of asylum seekers, provide them with means of subsistence, and ultimately, integrate them into European society.

The financial inclusion of asylum seekers is an important component of wider integration efforts, as access to basic payment services is a prerequisite for participating fully in modern economic and social life.[4] At the same time, financial inclusion is central to the fight against ML/TF: this is because lack of access to financial services can drive financial transactions underground and away from effective AML/CFT controls and oversight.[5]

The success of EU Member States' integration and financial crime prevention efforts therefore depends at least in part on the extent to which credit institutions and financial institutions ('institutions') provide asylum seekers with access to financial products and services.

[3] European Migration Network- Policy Brief on migrants' movements through the Mediterranean (http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-informs/xemn_policybrief_movementsmediterranean_final.pdf)

[4] European Commission (2009): Financial Inclusion: Ensuring Access to a Basic Bank Account. Consultation Document (http://ec.europa.eu/internal_market/consultations/docs/2009/fin_inclusion/consultation_en.pdf) See also Recital 3 and Article 16(2) of Directive 2014/92/EU, which establishes a right to access a basic payment account for all consumers who are legally resident in the Union.

[5] Financial Action Task Force (2013): Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (http://www.fatf-gafi.org)

Providing asylum seekers with access to financial products and services can create challenges for institutions where the identity of asylum seekers cannot be verified on the basis of 'traditional' forms of identification like passports or ID cards, or where there are doubts about the veracity of the information contained in the documentation provided. These challenges can be exacerbated where asylum seekers originate from countries or territories that are associated with higher ML/TF risk, including those where groups committing terrorist offences are known to be operating.[6] This is because institutions are under an ongoing legal obligation to comply with applicable AML/CFT and financial sanctions legislation.

This Opinion sets out what institutions can do under the European Union's legal framework to facilitate the financial inclusion of asylum seekers from higher-risk third countries and territories when they first apply for a financial product or service. It acknowledges that due to a combination of country risk and uncertainty over the robustness of applicants' identity documentation, the ML/TF risk associated with these customers is unlikely to be low, but suggests that this risk can be managed effectively.

The focus of this Opinion is on the establishment of a business relationship between an institution and a customer who is an asylum seeker from a higher-risk third country or territory. Many of the issues addressed in this Opinion will apply in a similar way in relation to occasional transactions, but institutions should be mindful that their ability to identify, assess and manage ML/TF risk on the basis of customer identification and verification measures alone will be limited in those circumstances and take steps to address these risks adequately.

The EBA welcomes the effort competent authorities of some EU Member States have made to clarify how institutions can provide asylum seekers with access to financial products and services under the existing legal framework and calls on others to consider taking similar steps.

The EBA's views expressed in this Opinion are based on an analysis of European Union law. They may also inform wider efforts by Member States financially to include other members of society. Institutions should ensure that any action they take is in line with their national legal and regulatory requirements. Nothing in this Opinion overrides or otherwise invalidates EU law, national legislation or the risk-based approach to AML/CFT.

[6] Article 1(1) of the Council Framework Decision of 13 June 2002 on combating terrorism defines 'terrorist offences' as 'intentional acts', which, 'given their their nature or context, may seriously damage a country or an international organisation' and are 'committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.'

Definitions

Unless otherwise specified, the terms used in this Opinion have the same meaning as those defined in Directive (EU) 2015/849. In addition, for the purpose of this Opinion, the following definitions apply:

- *Asylum seeker* means persons seeking asylum under the Geneva Convention of 28 July 1951 Relating to the Status of Refugees, the Protocol thereto of 31 January 1967 and other relevant international treaties.[7]

- *Higher-risk third country or territory* means any country or territory that is associated with significant ML/TF risk as a result of the prevalence of groups committing terrorist offences, terrorist finance and predicate offences to money laundering. This term is different from the term 'high risk third countries' with strategic deficiencies in their AML/CFT regime targeted by Article 9 of Directive (EU) 2015/849.[8]

Legal obligations

Institutions' AML/CFT obligations are set out in national law transposing the applicable EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML/CFT Directive).[9] These texts lay down measures that institutions within their scope must take to prevent and detect ML/TF.

The AML/CFT Directives make the successful application of risk-sensitive CDD controls to all customers and their beneficial owners a condition for the establishment of a business relationship. Where institutions cannot comply with these obligations, they cannot enter into, or maintain, a business relationship. The AML/CFT Directives also require institutions to take adequate measures to manage ML/TF risk, which include measures that enable institutions to identify and report suspicious transactions.

These obligations apply also in situations where Directive 2014/92/EU on payment accounts (PAD) [10] creates a right for all consumers who are legally resident in the European Union, including asylum seekers, to obtain a basic payment account and protects them from discrimination on the basis of their nationality, place of residence or any ground referred to in Article 21 of the

[7] See Article 2 (2) of Directive 2014/92/EU

[8] The European Supervisory Authorities' Joint Guidelines on simplified and enhanced customer due diligence and the factors institutions should consider when assessing the ML/TF risk associated with individual business relationships and occasional transactions, which are currently being finalised, set out how institutions can assess the ML/TF risk associated with a country or territory.

[9] Directive (EU) 2015/849 has to be transposed by 26 June 2017. Until then, many Member States' legislation will reflect similar provisions in Directive 2005/60/EC. Regulation (EU) 2015/847 may also be relevant in this context; this Regulation entered into force on 26 June 2015 and will apply from 26 June 2017. Until then, Regulation (EC) No 1781/2006 applies.

[10] Directive 2014/92/EU of the European Parliament and the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (OJ L257, 28.8.2014, p.214). This Directive will have to be transposed into national law by 18 September 2016.

Charter.[11] A basic bank account offers those services that are necessary in daily life.[12] The PAD is clear that the right to open and use a basic payment account applies only to the extent that credit institutions can comply with their AML/CFT obligations.[13]

Identification and Verification

The AML/CFT Directives require institutions to apply CDD measures before entering into a business relationship. This is so that institutions know who their customers are.

CDD includes measures to verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. Institutions often use official documents, like passports, national identity cards or driving licences, to verify a customer's identity; the recourse to such documents may be mandatory in some EU Member States'national legal orders.

European Union law does not specify what 'reliable and independent sources' are. To the extent permitted by national legislation, institutions may therefore have some flexibility in relation to the application of CDD measures, including in situations where a customer may be unable to provide traditional forms of identity documentation.

Many asylum seekers will have legitimate reasons for being unable to provide traditional forms of identity documentation when first arriving in an EU Member State, and national authorities may be unable to verify that an asylum seeker is who they claim to be even where such documentation exists. This is because of the large number of applications authorities currently have to process, political instability in asylum seekers' countries and territories of origin, and suggestions of a thriving trade in fake passports from some of the countries affected.[14] For example, there is evidence from last year's terrorist attacks in Paris suggesting that some perpetrators took advantage of the movement of migrants, obtained false Syrian passports and assumed the identity of a refugee to enter EU Member States.

All asylum seekers will have been issued with official identity documents by an EU Member State to confirm their status and their right to reside in that EU Member State. The EBA considers that these official identity documents are likely to satisfy the verification requirement in both Article 8 of Directive 2005/60/EC and Article 13 of Directive (EU) 2015/849, provided that they are

- current (i.e. unexpired);
- issued by an official national or local authority; and

[11] Charter of the Fundamental Rights of the European Union (OJ,C 326, 26.10.2012, p.391)

[12] Article 17 of Directive 2014/92/EU

[13] Articles 1(7) and 16(4) of Directive 2014/92/EU.

[14] Frontex: Risk Analysis for 2016
http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf

- listing the applicant's full name and date of birth.

Where this is Member State practice or a national requirement, these documents should also contain additional information, for example

- a unique identity or registration number;
- the applicant's photograph; and
- the address at which the applicant is registered. This may be a temporary address or the address of a resettlement office, refugee asylum or similar.

The EBA acknowledges that the content and look of these documents can differ significantly even within one Member State. This can make it difficult for institutions to be reasonably satisfied that such identity documents are genuine and may mean that the non-face to face verification of identity will not be appropriate. Where the issue and content of these identity documents is not harmonised, competent authorities may wish to work with national authorities to provide guidance to institutions on how to assess the veracity of the documentation provided; such guidance could also give reassurance to institutions that unless they have reasonable grounds to know or suspect that the documentation provided is forged, it should be enough to satisfy the AML/CFT Directives' verification requirements. Where institutions cannot verify an asylum seeker's identity on the basis of documents, data or information such as those described above, the AML/CFT Directives require that they must not enter into the business relationship.

Similar considerations apply also in relation to institutions' duty to comply with applicable financial sanctions regimes. The EBA recognises that in light of the uncertainty associated with many asylum seekers' identity, institutions may have very limited means of establishing whether such customers are who they claim to be. This means that unless an institution

- should have had specific grounds for knowing or suspecting that a customer is subject to a financial sanctions regime or otherwise known or suspected to be linked to terrorist activity, or
- can be shown otherwise to have deliberately or negligently failed to apply adequate CDD or other AML/CFT measures, which include measures to identify and report suspicious transactions

enforcement action will be very unlikely.[15]

[15] See for example Article 28 in Regulation 36/2012.

Risk mitigation

The type of evidence of identity an institution chooses to accept as evidence of an asylum seeker's identity will affect its assessment of the ML/TF risk associated with an individual business relationship or occasional transaction and determine the most appropriate way to manage that risk effectively.

Limiting ML/TF risk through monitoring

In line with provisions in national law transposing the applicable EU AML/CFT Directive, institutions must monitor their business relationships as part of their CDD obligations. Monitoring includes both transaction monitoring to ensure that transactions are consistent with the credit or financial institution's knowledge of the customer and ensuring that the CDD information the institution holds remains up to date.

EU AML/CFT Directives require institutions to adjust the extent of monitoring on a risk-sensitive basis. This means that institutions must ensure that the level and intensity of monitoring is set in a way that is commensurate to the ML/TF risk associated with the customer, including the risk that the customer may not be who they claim to be. The European Supervisory Authorities' Joint Guidelines on simplified and enhanced customer due diligence and the factors institutions should consider when assessing the ML/TF risk associated with individual business relationships and occasional transactions, which are currently being finalised, set out how institutions can do this.

In the situation described in this Opinion, ongoing monitoring of both transactions and the business relationship is key to the effective mitigation of ML/TF risk. Monitoring measures that may be particularly relevant include:

- Setting expectations of the customer's behaviour, such as the likely nature, amount, source and destination of transactions, to be able to spot unusual transactions and considering what might constitute a suspicious transaction.

  In addition to obtaining information from individual customers about the purpose and intended nature of the business relationship or transaction, including, for example, the expected source and amount of payments from third parties, institutions may be able to draw on their experience of existing or previous asylum seekers' account usage to inform this process and liaise with other institutions to share experiences where appropriate. For example, when building a customer risk profile and setting alert thresholds, institutions may find it useful to take account of specificities of the asylum process, such as frequent relocations or frequent low value transfers to asylum seekers' countries of origin, which by themselves may not give rise to suspicion. It may also be useful to understand common parameters, such as the amount and source of state benefits; access to information from national authorities and law enforcement may be particularly helpful in this context.

The EBA acknowledges that language barriers may make it more difficult for an institution to establish the purpose and intended nature of a business relationship with an individual customer, but considers that generic parameters such as those described above*, together with a careful targeting of basic financial products and services*, will allow institutions to make reasonable assumptions about the purpose and intended nature of the business relationship. Competent authorities may wish to work with other national authorities and institutions to provide further guidance on when the purpose and intended nature of a business relationship can be assumed and how to ensure that language barriers do not stand in the way of asylum seekers being aware of their rights as consumers. The EBA notes that a number of institutions in some Member States, for example in Italy, employ staff with specific language skills to service local communities whose first language is not the Member State's and that others, for example in Germany, have opened branches specifically for asylum seekers with staff that possess the necessary expertise and foreign language skills to process applications. The EBA considers that this can be an effective way forward in some cases.

- Ensuring that in line with an institution's general ML/TF risk management policies and procedures, asylum seekers' accounts are reviewed both regularly and after trigger events such as unusual or unexpected transactions to understand whether changes to the customer's risk profile are warranted.

  Where the customer's behaviour or transactions give rise to suspicion, institutions must report this to the Financial Intelligence Unit (FIU). Should suspicion arise before a transaction is carried out, institutions must refrain from carrying out the transaction until they have informed the FIU and awaited instructions from the FIU on how to proceed.

- Taking steps to ensure that the institution becomes aware of any changes to the CDD information previously obtained that might affect its assessment of the ML/TF risk associated with the individual business relationship. This may be particularly important where an asylum seeker's identity was verified on the basis of a provisional document with limited validity only. It may be helpful to ensure that such accounts can be easily identified, for example, by indicating the nature of the account in the institution's onboarding system.

  The EBA considers that as part of their obligation to keep the CDD data or information up to date, where identification was based on temporary identity documentation, institutions should take risk-sensitive measures to verify the customer's identity on the basis of a permanent European identity document as soon as reasonably possible, or once the claim for asylum has been processed (whichever occurs first).

- Taking steps to ensure that the institution can identify cases where an asylum seeker no longer resides in the institution's Member State to safeguard against the account being used fraudulently, in particular where a third party has signatory rights to the account.

Other measures to mitigate ML/TF risk

Limiting ML/TF risk through the products or services offered

Upon arrival in an EU Member State, asylum seekers will have specific financial needs. These can often be met through basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes. Such basic products and services may also make it easier for institutions to identify unusual transactions or patterns of transactions, including the unintended use of the product; but it is important that any limits be proportionate and do not unreasonably or unnecessarily limit asylum seekers' access to financial products and services.

To the extent permitted by national legislation, examples of limits institutions might impose on a risk-sensitive basis include, for example:

- no provision of credit or overdraft facilities;
- monthly turnover limits (unless the rationale for larger or unlimited turnover can be explained and justified);
- limits on the amount of person to person transfers (further or larger transfers are possible on a case by case basis);
- limits on the amount of transactions to and from third countries (while considering the cumulative effect of frequent smaller value transactions within a set period of time), in particular where these third countries are associated with higher ML/TF risk;
- limits on the size of deposits and transfers from unidentified third parties, in particular where this is unexpected; and
- prohibiting cash withdrawals from third countries.

Some of these limits may also be appropriate in the context of basic payment accounts to the extent that this is necessary to manage the ML/TF risk associated with an individual business relationship.

After 18 September 2016, where asylum seekers intend to use a payment account with basic features, the PAD will apply. This means that credit institutions will be unable to refuse the opening of the account unless the opening of the account or its subsequent use would result in a breach of national law transposing the applicable AML/CFT Directive, for example, because the credit institution cannot manage the ML/TF risk associated with the business relationship.

The EBA considers it unlikely that the condition for refusal would be met generally or solely on the basis that a prospective customer originates from a higher-risk country or territory and/or has legitimate reasons for providing less robust evidence of identity; this would likely be incompatible with the PAD and not be in line with the risk-based approach set out in the AML/CFT Directives. But while in standard situations a basic payment account must allow for the execution of an unlimited number of operations in relation to the services included in Article 17(1) of the PAD,

credit institutions will be able to limit a basic payment account's services on a case by case basis where that this is necessary to manage the ML/TF risk they have identified. However, to ensure compliance with the PAD, it is important that such limits only apply to the extent that they would also apply to other customers and accounts in similar risk scenarios.[16] Where credit institutions decide to refuse or limit the services of a basic payment account for AML/CFT compliance purposes, they should document their reason for so doing and stand prepared to demonstrate to their competent authority that these steps were appropriate and commensurate to the ML/TF risk associated with the individual business relationship.

Policies, procedures and record-keeping

EU AML/CFT Directives require institutions to identify and assess ML/TF risk and put in place policies and procedures to manage that risk, including in relation to CDD. The EBA considers that institutions should be in a position to demonstrate to their supervisor that the AML/CFT measures they take in relation to asylum seekers from higher risk country or territory are adequate if

- this category of customers is explicitly addressed in the business-wide risk assessment;
- the policies and procedures clearly state which controls staff may consider applying, on a case-by-case and risk-sensitive basis, in relation to such customers; and
- any decision to refuse a business relationship or to apply risk-mitigating measures is clearly documented.

The EBA considers that staff training is essential to ensure the consistent and effective application of these policies and procedures.

Conclusion

The current influx of asylum seekers from higher risk third countries and territories poses unique and complex challenges to EU Member States and, by implication, institutions providing their services in the EU. While most asylum seekers will be arriving in an EU Member State because they are fleeing from war or terrorism rather than to commit crimes, the risk remains that those seeking to perpetrate acts of terrorism might use the movement of refugees to further their illicit goals. It is therefore important that efforts to provide asylum seekers with access to financial products and services go hand in hand with robust AML/CFT controls, and that institutions, competent authorities and law enforcement work together to share information that will help inform an effective AML/CFT regime; specific guidance by competent authorities on the management of these customers may be particularly useful in this context.

This Opinion shows that the applicable European legal framework is sufficiently flexible to allow institutions to accommodate both governments' demands for the financial inclusion of asylum seekers and effective ML/TF risk management.

[16] Article 17(1) subparagraph 2 of the PAD

Over time, as their understanding of the ML/TF risk associated with individual business relationships with asylum seekers from higher-risk third countries and territories grows, institutions will be able to adjust the extent of monitoring and the type of products and services offered; this is in line with the risk-based approach.

This opinion will be published on the EBA's website.

Done at London, 12 April 2016

[signed]

Andrea Enria

Chairperson
For the Board of Supervisors