

RegCORE Client Alert

European Banking Authority publishes final guidelines on the use of remote customer onboarding solutions

November 2022

Financial Services

European Banking Authority publishes final guidelines on the use of remote customer onboarding solutions

Dr. Michael Huertas

Tel.: +49 160 973 757-60

michael.huertas

@pwc.com

Contact RegCORE Team

de_regcore@pwc.com

QuickTake

On 22 November 2022 the European Banking Authority (**EBA**) published its long-awaited “final report” containing a cost-benefit analysis, summary of the amendments to the draft version of the guidelines and most importantly the final “guidelines on the use of remote customer onboarding solutions” (the **Guidelines**).¹ The Guidelines aim to provide clarity and uniformity in how the counterparty/client/customer due diligence (**CDD**) rules that were set in the EU’s Directives on anti-money laundering, terrorist financing and financial crime efforts (collectively **AML**) should be interpreted and applied.

As assessed in this Client Alert, the EBA’s Guidelines seek to close the gaps by setting common EU standards on the development and implementation of sound, risk sensitive initial CDD processes in the remote customer onboarding context for “standard remote customer onboarding journeys”. Moreover, the Guidelines set out steps that credit and (other types of) regulated financial services firms in scope of the Guidelines will want to consider when choosing remote customer onboarding tools and assessing whether these are fit for purposes in design and effectiveness in meeting their initial CDD obligations. Crucially, the Guidelines are clear that they are technology neutral, namely that “... as long as the conditions set out in these guidelines are met, and to the extent that this is permitted by national law, the choice of individual technological solutions is the credit and financial institutions.”

The Guidelines should also be considered given their relevance for but not direct application to the wider set of “obliged entities” for AMLD purposes that are not credit nor financial institutions and what this might mean in terms of possible options available to EU policymakers, who are at the time of writing hereof, are aiming to comprehensively revise and replace the AMLDs with the forthcoming finalisation of an EU Regulation on the prevention of money laundering, terrorist financing and financial crime (working title at present **AMLR**) and the operationalisation of a proposed EU Anti-Money Laundering Authority (working title at present **AMLA**).

¹ Available [here](#).

Background

The rise of digital finance has raised a need for increased use of remote and/or digital CDD as part of the onboarding process. The COVID-19 pandemic has certainly acted as a further catalyst. The Guidelines follow on from previous efforts of the EBA to drive harmonisation on rules while at the same time trying to foster the use of innovative solutions when conducting CDD.²

In the European Commission's view, as echoed by the introduction to the EBA's Guidelines, the AML rules in Directive (EU) 2015/849 (**AMLD IV**) and the subsequent amendments introduced by Directive (EU) 2018/843 (**AMLD V**) (collectively the **AMLDs**) (as implemented in the EU Member States) do not provide sufficient clarity and certainty on what is and what is not allowed when conducting CDD in a remote and digital context.

This uncertainty has meant that, despite AMLD V's harmonised measures, fragmentation remains both in how national competent authorities (**NCA**s) as well as market participants interpret these rules and thus what solutions exist when conducting CDD on a remote and/or digital basis differ across Member States. Regulatory divergence is not only costly, but also increases AML risks. The AMLDs apply both to regulated financial services firms as well as a host of other "obliged entities".

The EBA has a leading role in preventing AML risks to the EU's financial system and is mandated to lead, monitor and coordinate the EU's financial sector (and NCA)s in identifying, reducing and mitigating AML risks and shortcomings. As with other EBA guidelines, these Guidelines are addressed to NCA)s as well as credit and financial institutions (but not to other "obliged entities" that are subject to the AMLDs.

The Guidelines were previously subject to a public consultation between 10 December 2021 and March 2022. The EBA adopted feedback from market participants in various amendments thus making the final version of the Guidelines. These will now formally enter into force six months after their publication on the EBA website in all EU official languages. Market participants will want to recall that the English language drafting of the Guidelines contain operative provisions using the word "should" often leading to confusion in other languages.³

Following finalisation, NCA)s must inform the EBA whether they comply or intend to comply with the Guidelines or, in the alternative, their reasons for non-compliance. Many NCA)s may (need to) update or introduce their own new standards and/or supervisory guidance on remote and/or digital including "video assisted identification" solutions, which remain the prevailing method across the EU when conducting remote CDD, so as to reflect the outcomes set in the Guidelines.

Affected market participants i.e., whether those credit and financial institutions that have to comply with AML rules and CDD obligations or those that offer such remote and/or digital CDD solutions will want to begin preparing to meet compliance with the Guidelines, principles and supervisory outcomes as soon as possible.

Importantly, as the Guidelines are purposefully technology neutral, they fail to clarify whether certain third-party developed solutions and standards, as they may exist in one or more EU Member States are fit for purpose and may be used to meet CDD standards in other Member States. This is regrettable as precisely this is part of the certainty on uniform standards that many market participants (including a number of NCA)s had called on the EBA to establish as part of their efforts in these Guidelines. It remains to be seen whether this might be achieved in the context of the AMLR and/or AMLA or as a prelude thereto, any further EBA guidance.

² These include:

1. The EBA Opinion on the use of innovation solutions by credit and financial institutions in the CDD process – available [here](#).
2. EBA guidance on collecting identity's evidence for non-face to face situations in its revised Risk Factors Guidelines – available [here](#).

³ In English, certainly in legal drafting as used by EU policymakers, "should" is taken to mean "must". While "should", when used as an auxiliary verb does not denote a requirement that is absolutely mandatory, as with the auxiliary verb "shall" the use of "should" does still denote an absolute obligation with some degree of optionality and/or a strict supervisory expectation. This is nuance is sometimes incorrectly translated into local -non-English versions of EU rulemaking instruments – including EBA guidelines and may falsely lead to the impression that there is a degree of optionality.

The Guideline's key requirements

The Guidelines operative provisions focus on communicating supervisory expectations of credit and financial institutions with respect to their:

- A. **Internal policies and procedures** – notably with respect to remote CDD how and when it can be used (including on an automated basis) and what controls are in place as part of its governance including (i) conducting a pre-implementation assessment of the remote customer onboarding solution that NCAs may request evidence of, in particular where third party service providers are involved; (ii) ensuring that a remote customer onboarding solution is capable of being integrated into the wider internal control system; and (iii) ensuring robust and frequent ongoing monitoring of the remote customer onboarding solution (including with respect to certain triggers for ad hoc reviews);
- B. **Establishing the means of “acquisition of information” i.e., through CDD conducted during onboarding** – notably with respect to identifying the counterparty/client or customer, including the types of documents, data or information that will be used to verify identities and the manners in which that will be done. Notably paras. 24 et seq. of the Guidelines follow measures adopted by some NCAs, in particular Germany's BaFin, in summarising the supervisory expectations that apply to video assisted identification measures.⁴ The Guidelines also require that credit and financial institutions assess, decide and document what information is manually entered by the person subject to CDD, what is automatically captured from that person's documents and what is gathered using internal or external sources. While this offers (welcome) flexibility for firms, it does not truly set a uniform standard across the EU.
- C. **Matching CDD persons' identities as part of the verification process** – unsurprisingly, the Guidelines require that remote CDD onboarding solutions implemented by credit and financial institutions ensure, that as part of their verification process that (i) there is a match between the visible information of the natural person and the documentation provided; (ii) where there is a legal entity, it is publicly registered (where applicable), and (iii) where there is a legal entity, the natural person that represents it, is entitled to act on its behalf.
- D. **Rules and procedures when relying on third parties and outsourcing** – as under previous EBA and other EU rules and supervisory expectations, AML and CDD compliance may be outsourced or delegated to a third party and/or a person with a primary compliance obligation may rely on another person to fulfil those obligations. Similar to the points listed above, a person with a primary compliance obligation must assure themselves and evidence the same that the involvement of another person into the CDD and/or wider AML compliance obligations are suitably qualified and resourced to do so during normal operating conditions as well as in instances of business continuity/recovery events.
- E. **Rules on information communication technology (ICT) and security risk management** – the Guidelines set specific common standards that credit and financial institutions can refer to when dealing with ICT and security risks related to the use of the remote CDD onboarding process, in particular where such processes are outsourced, including to group entities. These rules and supervisory expectations apply in addition to existing requirements set out in a number of other legislative and regulatory rulemaking instruments that exist at the individual Member State as well as EU level including the forthcoming changes to be introduced as part of the EU's Regulation commonly referred to as the Digital Operational Resilience Act (**DORA**).

Outlook ahead

The Guidelines are certainly timely and in parts are welcome in providing clarifications. Where however they fail to go as far as they perhaps could have done, they do little to remove existing and prevent new fragmentation for credit and financial institutions as well as NCAs supervising them.

⁴ The EBA Guidelines state that credit and financial institutions should (i.e. must) ensure that: “a) the information obtained through the remote customer onboarding solution is up-to-date and adequate to meet the applicable legal and regulatory standards for initial customer due diligence; b) any images, video, sound and data are captured in a readable format and with sufficient quality so that the customer is unambiguously recognisable; c) the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected.” While this sets a minimum standard as applicable on pan-EU basis, it should be noted that Germany's BaFin's Circular on video assisted identification (available [here](#) in English and [here](#) in German) goes well beyond these basic overarching items.

This fragmentation also means that technical solutions and other offerings developed for use in one jurisdiction may still continue to be limited in their acceptance for use in other jurisdiction(s). Consequently, this may well mean that video assisted identification will remain the prevailing method for conducting online and remote CDD on a pan-EU basis, with divergences in certain Member States and outliers of a number of alternatives, such as artificial intelligence powered verification of documents/signatures.

All of these issues that the Guidelines fail to resolve detracts from EU's aims set in its Digital Finance Strategy and ultimately ensuring a better, more efficient user experience, for those subject to CDD inasmuch as those needing to complete CDD checks. Ultimately, EU policymakers may want to give this point further consideration as otherwise this area of the Single Market (and not just for financial services) will remain disjointed in this area – both for firms that need to comply with the Guidelines as well as the wider body of obliged entities.

In a wider sense, as stated above, the Guidelines' targeted application to credit and financial institutions as well as those NCAs tasked with AML compliance and supervision of credit and financial institutions certainly makes sense. So too does the centralisation of a number of concepts (many of which have been refined) in core document. What however remains to be seen is how the Guidelines will be adapted to meet the new AMLA (as well as equally the DORA) regime as well as whether similar principles will be documented that the wider set of obliged entities other than credit and financial institutions can make use of.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these developments.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our [website](#).

Dr. Michael Huertas

Tel.: +49 160 973 757-60

michael.huertas@pwc.com

© 2022 PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft. All rights reserved.

In this document, "PwC Legal" refers to PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft, which is part of the network of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.

www.pwclegal.de