



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

*CONSULTATION PAPER
NO. 3 OF 2021*

**PROPOSALS ON DIGITAL
VERIFICATION OF IDENTITY (eKYC)**

23 June 2021



Contents

Introduction.....	3
Why are we issuing this paper?	3
Who should read this paper?	3
How to provide comments	3
What happens next?	4
Comments to be addressed to:	4
Background	5
Updating the regulatory framework for eKYC	6
Advantages of eKYC.....	6
Facilitation of eKYC	6
Inherent risks	8
Mitigation of eKYC risks.....	8
Biometric verification and authentication	10
Miscellaneous amendments.....	11
Conclusion.....	11
Proposed amendments.....	12

*Introduction****Why are we issuing this paper?***

1. The Financial Services Regulatory Authority (“FSRA”) of Abu Dhabi Global Market (“ADGM”) has issued this Consultation Paper to seek views on its proposed updates to the regulatory framework governing the use of non-face-to-face (“NFTF”), digital verification of identity, also known as “electronic Know Your Customer” (“eKYC”), used during the customer due diligence (“CDD”) process. Adopting these proposals would make the FSRA’s requirements in this area both clearer and more closely aligned with the recommendations and guidance issued on the topic by the Financial Action Task Force (“FATF”) as well as the UAE’s Federal Anti-Money Laundering legislation; and guidance¹ issued by the FSRA and other federal authorities in the context of the Covid-19 pandemic (“the Joint Guidance”). The amendments are principally proposed to Anti-Money Laundering and Sanctions Rules and Guidance (“the AML Rulebook”), although some amendments are also proposed to the General Rulebook (“GEN”).

Who should read this paper?

2. This Consultation Paper should be of interest to all entities required to undertake CDD of natural persons², including in relation to Beneficial Owners. Whilst the measures proposed in this paper are principally directed at entities using or considering using eKYC, the majority of these measures also have implications for the wider population of entities undertaking CDD, irrespective of the method used. For example, the FSRA’s proposals on verification of a natural person’s current residential address would apply to all parties undertaking CDD, not just those using eKYC. Further, the FSRA’s guidance on how the business risk assessment and annual compliance review should interlink and interact has general application, rather than being limited to eKYC.

How to provide comments

3. All comments should be made in writing and sent to the address or the email address specified below. If sending your comments by email, please use the Consultation Paper

¹ Central Bank of the UAE (CBUAE), Dubai Financial Services Authority (DFSA), Financial Services Regulatory Authority (FSRA), the Securities and Commodities Authority (SCA), the Insurance Authority (IA), the Ministries of Justice and of Economy “*Joint Guidance on the treatment of financial crime risks and obligations in the UAE in the context of the Covid-19 crisis*” (<https://www.adgm.com/documents/financial-crime-prevention-unit/notices/fsra-fcpu-uae--supervisory-authorities-aml-guidance-covid-english.pdf> May 2020)

² In this Consultation Paper, ‘entity’ means Relevant Person, as defined in the AML Rulebook. The term therefore includes Authorised Persons, Recognised Bodies, Designated Non-Financial Businesses or Professions, and Non-Profit Organisations (all as defined in the AML Rulebook).

number in the subject line. If relevant, please identify the organisation you represent when providing your comments.

4. The FSRA reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise at the time of submitting those comments. Comments supported by reasoning and evidence will be given more weight by the FSRA.

What happens next?

5. The deadline for providing comments on the proposed framework is **29 July 2021**. After receiving your comments, we shall consider whether any modifications are required to the proposals and the Board of ADGM and the FSRA will then proceed to enact the proposals in their final form.
6. You should not act on these proposals until final rules and guidance are issued by the FSRA. We shall issue a notice on our website when that happens.

Comments to be addressed to:

Consultation Paper No. 3 of 2021
Financial Services Regulatory Authority
Abu Dhabi Global Market Square
Al Maryah Island
PO Box 111999
Abu Dhabi, UAE

email: consultation@adgm.com

Background

1. In March 2020, FATF published its Guidance on Digital ID³ (“the FATF Guidance”), which was supportive of the use of “reliable, independent” NFTF digital verification of customer identity (eKYC) during the CDD process. According to the FATF Guidance “reliable, independent” in this context means “*that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results*”. The FATF Guidance outlines how eKYC can support the wider FATF Recommendations⁴, which are the international benchmark for regulatory frameworks for anti-money laundering and combatting terrorist financing (“AML/CTF”).
2. The FATF Guidance does not supersede the FATF Recommendations, instead it supports them by providing guidance on how eKYC systems (the technology and processes used to undertake eKYC) may be used most appropriately to ensure that they help entities comply with existing AML/CTF requirements. The FATF Guidance also recognises that eKYC has the potential to both reduce and be a source of AML/CTF risk, and makes nineteen recommendations to both help facilitate eKYC and mitigate those risks.
3. The FATF Guidance focusses on addressing the risks arising from eKYC in the following areas:
 - initial and on-going CDD;
 - reliance on third parties involved in the CDD process;
 - record-keeping; and
 - the risk-based approach to AML/CTF.
4. The timing of the publication of the FATF Guidance was opportune, as NFTF interaction (including when undertaking CDD) in many cases became a necessity during the global pandemic. In recognition of that and the general trend towards digitalisation of customer interaction with financial institutions, the FSRA and other UAE regulatory authorities published the Joint Guidance in May 2020. This provided guidance on how to mitigate the risks associated with NFTF interaction, including when using eKYC to on-board customers during the pandemic, but also in other areas, such as the monitoring of suspicious transactions.

³ Financial Action Task Force, “*Guidance on Digital ID*”, (<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html> March 2020)

⁴ Financial Action Task Force, “*The FATF Recommendations*”, (<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>, as amended October 2020)

5. The AML Rulebook is 'technology-neutral' and therefore already permits the use of eKYC, however we recognise that it may benefit from additional wording to make this clear. In addition, given the ever-increasing use of eKYC in ADGM, the FSRA believes its regulatory framework should be updated to reflect the key messages of the Joint Guidance and the FATF Guidance. The purpose of the measures proposed in this paper is to ensure that the FSRA's regulatory framework contains the requisite measures to both facilitate eKYC and also to clarify how it expects applicable entities to employ the technology in a manner that mitigates its inherent risks. The FSRA is therefore proposing amendments to its Rulebooks to reflect this and the areas of focus addressed in the FATF Guidance.

Benchmarking

6. In drawing-up its proposals the FSRA has sought to ensure greater alignment with international best practices, including those promoted in the FATF Guidance. We have therefore examined a number of regulatory frameworks governing eKYC in comparable, peer jurisdictions and concluded that the proposals in this consultation paper would make the FSRA's regulatory framework more comprehensive and reflective of current best practices. In addition, the proposed amendments also reflect the evolving practices in relation to eKYC that are employed by entities operating in or from ADGM.

Updating the regulatory framework for eKYC

Advantages of eKYC

7. Reliable and independent eKYC has several benefits. From an AML perspective, it can enhance CDD and thus help to prevent financial crime. In a wider sense, it may also improve customer experience, reduce compliance costs for entities, eliminate manual processing of physical documentation and advance the digitalisation of financial services. Consequently, the FSRA has proposed a number of measures which clarify that eKYC is permitted in ADGM as part of the CDD process, as well as providing a suitable level of flexibility to reduce regulatory burden as and where appropriate.

Facilitation of eKYC

8. Given the advantages of eKYC outlined above and to encourage its use, the FSRA wishes to make it clear to entities that eKYC is permitted in ADGM. It is proposing to do so by amending applicable guidance on CDD in the AML Rulebook and by proposing a number of substantive amendments to help facilitate the adoption of eKYC. The key proposals are in the following areas:

- **Verification of residential address.** The existing requirement in the AML Rulebook is to both obtain and verify the current residential address of a natural person, but verification of residential address can be challenging for eKYC systems in the UAE. This is because documents evidencing address do not lend themselves to being verifiable by automated, digital processes, and typically must be checked by the human eye. Following a review of applicable FATF publications and peers within and outside the UAE, the FSRA proposes removing the hard requirement to always undertake address verification, as long as doing so is consistent with entities' risk-based approaches to AML/CTF and also all applicable Laws and Rules. This position would, we believe, better align our framework with applicable UAE Federal AML legislation⁵ and the published Guidance on it⁶ (which are more flexible on the issue than the AML Rulebook).
- Further, we consider that our proposed amendments would make our framework more consistent with guidance produced by the FATF, which not only comments on the potential for flexibility on the issue of verification of address⁷, but also identifies national legislative frameworks which have provided similar flexibility⁸. Our proposed position does not preclude entities choosing to verify current residential address as a matter of good business practice, for commercial reasons and to assist verifying a customer's identity. Finally, we have proposed amending the AML Rulebook so that all customers subject to Enhanced Customer Due Diligence must be subject to verification of current residential address.
- **Assurance assessments.** In ADGM and elsewhere, eKYC systems tend to be obtained from outsourced service providers, rather than developed in-house. The AML Rulebook requires entities to undertake reviews of the service providers to whom they have outsourced an element of the CDD process. We have made a number of proposed amendments to rules and guidance in the AML Rulebook, to build-upon this existing requirement and therefore strengthen entities' oversight of the outsourced service providers used. However, we are also proposing to provide

⁵ "Cabinet Resolution No. (10) of 2019 Concerning the Implementing Regulations of Federal Decree by Law No. (20) of 2018 Concerning Anti-Money Laundering and Counter Terrorism Financing and Financing of Illegal Organizations" (<https://www.mof.gov.ae/en/lawsAndPolitics/CabinetResolutions/Pages/201910.aspx>, 2019)

⁶ "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations. Guidelines for Financial Institutions" (<https://www.adgm.com/documents/financial-crime-prevention-unit/useful-links/aml-cft-and-illegal-organisations-guidelines-for-financial-institutions.pdf>, March 2021)

⁷ Financial Action Task Force, "Guidance on Digital ID" (see pages 53 and 61) (<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html>, March 2020)

⁸ Financial Action Task Force, "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion", see pages 11, 89, 102 and 104, (<http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf>, November 2017)

some flexibility in this area, and we propose that entities be permitted to place a level of reliance on assurance assessments of eKYC systems performed by third parties. We propose that this reliance extend to assurance assessments conducted by another Group member, an independent third party, or where the eKYC system is government-authorised (a proposal consistent with the FATF Guidance).

- We believe this approach strikes the right balance between requiring entities to exert strong oversight over outsourced service providers licensing their eKYC systems, and allowing entities to place appropriate reliance on reviews undertaken for them by other parties. We detail the conditions for such reliance within our proposals. For clarity, under our proposals we have not changed the requirement for entities using outsourcing arrangements to be entirely responsible for compliance with applicable rules.

1. THE FSRA INVITES COMMENTS ON THE PROPOSALS FOR FACILITATING eKYC IN ADGM.
--

Inherent risks

9. Compared to traditional CDD, eKYC is vulnerable to distinct risks which merit specific consideration. These range from false acceptance rates (a measure of the proportion of individuals who have been on-boarded by an eKYC system, but should not have been) which can vary materially across different eKYC systems, to how criminals can utilise technology themselves to counter eKYC controls, and how technology allows for the scaling of impersonation fraud to levels not possible when it is attempted face-to-face. Furthermore, noting the tendency for eKYC systems to be sourced from third parties, there are distinct risks in placing reliance on those parties for any significant parts of the CDD process, including the gathering and processing of sensitive customer information, cybersecurity and data protection risks. Therefore, eKYC both presents new risks and increases existing risks in a material enough manner so as to merit additional wording (primarily in the form of guidance) within the FSRA's Rulebooks.

Mitigation of eKYC risks

10. Given the risks of eKYC outlined above, the FSRA's proposed amendments to mitigate risks arising from eKYC seek to ensure the following outcomes:

- **A robust, outcomes-based approach to using eKYC for customer on-boarding.** Our proposed guidance on eKYC does not specify granular technical standards on how eKYC systems used in ADGM must verify identity, e.g. which biometric authentication methods must be used. Instead we propose specifying the outcomes that should be achieved. For example, we propose outlining that eKYC should be ‘secure and effective’ and ‘at least as stringent’ as traditional CDD. We also emphasise the requirement for entities to identify, document and address applicable eKYC risks, by utilising those assessments already required by the AML Rulebook. The FSRA’s proposed amendments therefore highlight the business risk assessment, systems and controls review and annual compliance review as particularly important in addressing eKYC risk. Therefore, our proposals place the onus on entities using eKYC to assess and address eKYC risk itself, and subsequently to calibrate their eKYC systems and broader risk management frameworks as appropriate to the risks it has identified.
- **Strong ongoing customer due diligence and anti-financial crime controls.** The proposed amendments seek to ensure that the use of an eKYC system supports other anti-financial crime measures, including suspicious transaction monitoring, mitigation of fraud risk, and on-going measures to address money laundering, terrorist financing and other potential financial crimes after the customer has been on-boarded. Consequently, a number of our proposed amendments outline that entities should duly consider financial crime risks beyond AML/CTF (such as fraud) in their operations, and to remind entities that on-going CDD is an essential component of their anti-financial crime controls. We have also amended GEN to ensure that entities are required to take measures to prevent fraud against customers, as well as themselves (as is the current requirement). Therefore, the measures proposed seek to avoid eKYC becoming the ‘entry point’ for criminals taking advantage of business relationships conducted entirely on an NTF basis to perpetrate financial crime after on-boarding is completed.
- **Existing record-keeping requirements are adhered to.** The FSRA proposes highlighting existing record keeping rules that require CDD records be held securely by both entities and eKYC system providers where third-party eKYC system providers handle sensitive customer data.

2. THE FSRA INVITES COMMENTS ON THE PROPOSALS TO AMEND THE AML AND GEN RULEBOOKS TO HELP MITIGATE EKYC RISK.

Multiple nationalities and residencies

11. We have taken the opportunity to draft miscellaneous guidance which may assist Relevant Persons (“RPs”) on-boarding customers with more than one nationality. The guidance outlines that where a potential or existing customer has more than one nationality the customer risk assessment should take account of that, potentially requiring a background check against all nationalities held by such a customer. The proposed guidance in this area should be of interest to all entities that on-board new customers, including those that use more ‘traditional’ methods than eKYC.

3. THE FSRA INVITES COMMENTS ON THE PROPOSALS TO PROVIDE GUIDANCE ON UNDERTAKING CDD FOR CUSTOMERS WITH MULTIPLE NATIONALITIES.

Biometric verification and authentication

12. The proposals do not specify granular requirements to be followed when using biometric verification as part of eKYC. However, it should be noted that the use of biometrics is in-scope of the recently issued draft ‘Guidelines for Financial Institutions adopting Enabling Technologies’⁹; once finalised, we intend to include guidance in the AML Rulebook outlining that entities should implement them as applicable.

Portability of CDD information

13. We recently enacted our regulatory framework for Third Party Providers (“TPPs”)¹⁰. Whilst not directly connected to the proposals outlined in this paper, we are taking this opportunity to remind entities of one particular obligation brought in by the TPP framework which may have relevance to entities’ use of eKYC. Our TPP framework brought in (via amendments to the AML Rulebook) the obligation on an applicable entity to share CDD information with another in-scope entity, as long as certain conditions were met. The TPP framework and the measures proposed in this paper are part of the ADGM’s ongoing efforts to foster innovation in financial services.

⁹ Central Bank of the UAE (CBUAE), the Securities and Commodities Authority (SCA), the Dubai Financial Services Authority (DFSA) and the Financial Services Regulatory Authority (FSRA) “Guidelines for Financial Institutions Adopting Enabling Technologies”, see pages 25-26, (<https://www.adgm.com/media/announcements/uae-regulatory-authorities-launch-consultation-june-2021>)

¹⁰ “ADGM FSRA introduces a new regulatory framework for Third Party Financial Technology Services” (<https://www.adgm.com/media/announcements/adgm-fsra-introduces-a-new-regulatory-framework-for-third-party-financial-technology-services> April 2021)

Miscellaneous amendments

14. We are taking this opportunity, alongside the consultation on the proposals outlined above, to correct some minor errors, omissions and typos that are present in the current version of the AML Rulebook, separately from the proposals for amendments to take account of eKYC. For example, our miscellaneous amendments include changing reporting deadlines from Calendar Days to Business Days, in line with other parts of our Rulebook. These corrections and amendments are **not** part of the consultation process and will be implemented as they stand in Appendix 4.

Conclusion

15. We believe that the proposals in this paper clarify that eKYC is permitted in ADGM and will help facilitate its adoption, whilst highlighting the strong controls that must govern its use. In doing so, we believe the FSRA's regulatory framework will align the FATF Guidance's specifications for ensuring "reliable and independent" eKYC is in operation. Finally, we believe the proposals strike an appropriate balance between drafting Rules and Guidance to facilitate eKYC and measures to mitigate its risks, and between high-level and granular requirements.

Proposed amendments

- **Appendix 1 Anti-Money Laundering and Sanctions Rules and Guidance (AML)**
- **Appendix 2 General Rulebook (GEN)**
- **Appendix 3 Glossary (GLO)**
- **Appendix 4 Anti-Money Laundering and Sanctions Rules and Guidance (AML)
- miscellaneous changes not subject to consultation**