Consultation on Revised Guidelines on Money Laundering and Terrorist Financing (ML/TF) Risk Factors (EBA/CP/2023/11)

29 August 2023

Our disclaimer

This document contains our comments on European Banking Authority's (EBA) Guidelines on money laundering and terrorist financing (ML/TF) risk factors in relation to your consultation on revised Guidelines on money laundering and terrorist financing (ML/TF) risk factors (EBA/CP/2023/11) and is based on our views as per the date of this document. Consequently, our views might be subject to change.

None of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this document, rendering professional advice or services. You can place no reliance on this document or its contents whatsoever. We accept no duty, responsibility or liability to you in respect of the subject matter or contents of this document.

Solely EBA is responsible for any decision making or taking any action in relation to the revised Guidelines on money laundering and terrorist financing (ML/TF) risk factors (EBA/CP/2023/11). No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this document.

All information in this document should be treated strictly confidential. This document may not be disclosed, quoted or referenced or otherwise.

Reader's guide to our response to the EBA consultation's questions

Our response to question 1 to 8 is formulated in the following table form:

Guideline	EBA's original guidelines	EBA's proposed amendments	Our suggestion	Our argument

This column concerns the relevant guideline

This column concerns the original text of EBA's Guidelines on ML/TF risks. In the case that our suggestion concerns multiple guidelines at the same time, the following text is used as reference: "See EBA Guidelines for the full guideline."

The text in **black** concerns the original text from the EBA Guidelines, whereas the text in **orange** concerns the amendments proposed by EBA for the current consultation.

The text in *black italic* concerns the description of our suggestion. The text in **black** concerns the original text from the EBA Guidelines. The text in **orange** concerns EBA's proposed amendments, whereas the text in **blue** concerns our suggestions as a respond to EBA's proposed amendments.

This column concerns our arguments on our suggestions. Our arguments are mainly based on guidance from the Financial Action Task Force, legislation and guidance from different jurisdictions and expertise within Deloitte.

Our response to question 9 is formulated without the second column above, as question 9 concerns Guideline 21 – a newly proposed guideline that is not present in the original guideline.

Question 1: Do you have any comments on the proposed changes to definitions.

Paragraph	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
12	'Occasional transaction' means a transaction that is not carried out as part of a business relationship as defined in Article 3(13) of Directive (EU) 2015/849.	Paragraph 12 point (f) is deleted.	*Bringing back point 12(f) with the addition of Article XXX of Regulation (EU) YYYY/XX as reference:* 'Occasional transaction' means a transaction that is carried out as part of a business relationship as defined in Article 11 of Directive (EU) 2015/849 and Article XXX of Regulation (EU) YYYY/XX.	The guideline concerns ML/TF risks associated with business relationships and occasional transactions. The definition of occasional transaction must be included for the firms to understand what 'occasional transaction' entails and which transaction(s) fall(s) under this definition. In this way, firms have better clarity when identifying, assessing and mitigating the ML/TF risks in their day-to-day business. For the clarification, Article XXX of Regulation (EU) YYYY/XX refers to the Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which is currently still under proposal.

Question 2: Do you have any comments on the proposed changes to Guideline 1.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
1.7	The systems and controls that firms should put in place to ensure their individual and business-wide risk assessments remain up to date should include: a) […] b) […] c) […]	Addition of letter d): The systems and controls that firms should put in place to ensure their individual and business-wide risk assessments remain up to date should include: a) […] b) […] c) […] d) Where the firm is launching a new product or service, or a new business practice, including a new delivery mechanism, or is adopting an innovative technology as part of its AML/CFT systems and controls framework, it should assess the ML/TF risk exposure prior to the launch and reflect this assessment in the firm's business-wide risk assessment and its policies and procedures.	d) Where the firm is launching a new product or service, or a new business practice, including a new delivery mechanism, or is adopting an innovative technology as part of its new and pre-existing products, services and AML/CFT systems and controls framework, it should assess the ML/TF risk exposure prior to the launch and reflect this assessment in the firm's business-wide risk assessment and its policies and procedures.	When innovative technology is deployed on a new or pre-existing product or service, it changes the nature of the product or service. Consequently, this can increase or decrease the ML/TF risk exposed to business and/or customers.

Question 3: Do you have any comments on the proposed changes to Guideline 2.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
2.4 b)	Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?	Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, unregulated businesses that provide services related to crypto assets as described in Guideline 9.21, casinos or dealers in precious metals?	N/A.	N/A

Question 4: Do you have any comments on the proposed changes to Guideline 4.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
4.60	[…]. Transactions maybe unusual because: a) they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs; b) […] c) […]	This letter is amended and replaced with*:* a) they differ from what the firm would normally expect, including when transactions are larger or more frequent than usual or transactions involving small amounts that are unusually frequent, or there are successive transactions without obvious economic rationale;	*Addition of letter d):* d) they demonstrate a pattern suggesting the customer is persistently avoiding CDD requirements by transferring amounts that are just below the threshold defined in Article 14(5) and Article 16(2) of Regulation (EU) 2015/847 (re-cast).	Avoiding CDD requirements by persistently transferring amounts that are just below the threshold determined by the firms can be interpreted as unusual and/or suspicious, as this is not a usual customer behavior, and it poses high ML/TF risks.

Question 4: Do you have any comments on the proposed changes to Guideline 4.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
4.74	What is appropriate will depend on the nature, size and complexity of the firm's business, as well as the risk to which the firm is exposed. Firms should adjust the intensity and frequency of monitoring in line with the risk-based approach. Firms should in any case determine: a) […] b) Whether they will monitor transactions manually or using an automated transaction monitoring system. Firms that process a high volume of transaction should consider putting in place an automated transaction monitoring system; and c) […]	Change of b) and addition of d): b) whether they will monitor transactions manually or by using an automated transaction monitoring system. Firms that process a high volume of transactions or transactions at high frequencies should consider putting in place an automated transaction monitoring system; c) […] d) whether the use of advanced analytics tools, like the distributed ledger analytics tools, is necessary in light of the ML/TF risk associated with the firm's business, and with the firm's customers' individual transactions.	*Changing the original article 4.74-4.78 into 4.75-4.79, and replacing 4.74 with:* 4.74 As part of the transaction monitoring process, firms should at least screen the following: • Name of originator/beneficiaries • Entity name • Nationality • Place of residence • XXXX	Additional clarification on which elements should be monitored and screened can serve as guidance for the industry.

Question 5: Do you have any comments on the proposed changes to Guideline 6.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
6.1	Firms must make their staff aware of the provisions they have put in place to comply with their AML/CFT obligations.	None	*Specify which type of staff must be aware of their AML/CFT obligations*: Firms must make their staff aware of the provisions they have put in place to comply with their AML/CFT obligations. The staff who should follow the firm's AML/CFT training are those who are: a) relevant to the firm's compliance with any requirements in the Directive (EU) 2015/849; b) capable of contributing to the: i. identification or mitigation of the ML/TF risks to which the firm's business is subject; ii. prevention or detection of ML/TF in relations to the firm's business; and c) senior management including C-level.	The guideline only mentions that the AML/CFT training should be tailored to staff and their specific roles. However, it does not explicitly specify who should follow it. This addition gives a guideline that this group of staff is particularly important to receive AML/CFT training for compliance purposes.

Question 5: Do you have any comments on the proposed changes to Guideline 6.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
6.2	As part of this, and in line with guidance contained in Title I, firms should take steps to ensure that staff understand: a) […] b) […] c) […]	Addition of letter d): d) How to use automated systems, including advanced analytics tools, to monitor transactions and business relationships, and how to interpret the outcomes from these systems and tools.	d) How to use automated systems, including advanced analytics tools, such as distributed ledger analytics tools, to monitor transactions and business relationships, and how to interpret the outcomes from these systems and tools.	This addition will help giving more weight and importance on monitoring CASPs. On top of that, other parts of the EBA guidelines are proposed to amend this way. This addition will therefore give better consistency throughout the guidelines.
6.3	Firms should ensure that AML/CFT training is: a) […] b) […] c) […] d) […]	None	*Addition of new letter e):* e) followed periodically.	The AML/CFT training must not be one-off, and must be given regularly, in order to refresh the knowledge of the staff with the newest development and trends of ML/TF.

Question 6: Do you have any comments on the proposed changes to Guideline 8.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
8.8 a)	The respondent is based in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to those jurisdictions: i. […] ii. […] iii. […] iv. […] v. […]	None.	*Addition of vi. under letter a):* iv. With no or no robust regulation on crypto assets.	Many jurisdictions are engaging with CASPs yet have no or relatively poor regulatory framework on crypto assets. The current EU third-country high risk list does not necessary cover jurisdictions with weak regulatory framework on crypto assets. Therefore, this element should be considered as a country or geographical risk factor that contribute to increasing ML/TF risk.

Question 7: Do you have any comments on the proposed changes to Guideline 9.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
9.20	Firms should take into account the fact that apart from providers engaged in exchange services between virtual currency and fiat currencies and Custodian Wallet Providers which are obliged entities under Directive (EU) 2015/849, the issuing or holding of virtual currencies as defined in point (18) of Article 3 of Directive (EU) 2015/849 remains largely unregulated in the EU and this increases the ML/TF risks. Firms may wish to refer to the EBA's report on crypto assets of January 2019.	This guideline is replaced with: When entering into a business relationship with a customer who is a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under Regulation (EU) [xxxx/xxx] or under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto assets.	When entering into a business relationship with a customer who is a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under Regulation (EU) [xxxx/xxx] or under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto assets set out in the MiCA Regulation (2019/1937).	The MiCA Regulation states three types of crypto assets; utility tokens, asset-referenced tokens and electronic money tokens. The distinction between the types of crypto assets is essential for developing an effective and comprehensive framework to mitigate ML/TF risks.
9.21 c)	When entering into a business relationship with customers that provide services related to virtual currencies, firms should, as part of their ML/TF risk assessment of the customer, consider the ML/TF risk associated with virtual currencies.	This guideline is replaced with: […], banks, as part of their CDD measures, should at least: a) […] b) […] c) understand the extent to which these customers apply their own customer due diligence measures to their clients either under a legal obligation or on a voluntary basis d) […]	c) understand the extent to which these customers apply their own customer due diligence measures to their clients either under a legal obligation or on a voluntary basis and assess the adequacy of these customer due diligence measures.	It is not clear from the proposed amendments if a firm should only understand or should also assess the customer due diligence measures of their clients. EBA should elaborate what is exactly expected from the industry.

Question 8: Do you have any comments on the proposed changes to Guideline 10, 15 and 17.

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
10, 15 and 17	See EBA Guidelines for the full guideline.	Proposed amendments replace references to 'virtual currencies' with references to 'crypto assets'.	N/A	N/A

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.11	CASPs should ensure that systems used by them to identify ML/TF risk associated with individual business relationships, transfers or occasional transactions and to identify sus-picious transactions comply with the criteria set out in Title I. In particular, CASPs should ensure that they have adequate transaction monitoring and advanced analytics tools in place that are commensurate to the nature and volume of the CASP's activities, includ-ing the type of crypto assets made available for trading or exchanged.	*Addition of new article on screening under "Measures", namely after guideline 21.11:* As part of customer due diligence measures, CASPs should match a customer's address against a list of blacklisted addresses on popular blockchains, e.g., addresses that have been misused or have been found to have been used by malicious individuals.	Guideline 2.5 letter a) mentions only adverse media reports or other relevant sources of information that can lead to customer risk associated with a customer's or beneficials owner's reputation. Guideline 2.7 letter a) advises that firms should screen customers and beneficial owners against sanctions list. However, these are general guidelines that apply to all firms. For CASPs, it is important to highlight that CASPs should also screen their customers' addresses against a list of blacklisted addresses on popular blockchains as an additional safeguard. Blacklisted addresses can continue to receive and receive crypto assets for ML/TF purposes, if they are not effectively monitored and blocked.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.1	CASPs should be mindful that they are exposed to ML/TF risks due to specific features of their business model and technology used as part of their business which allows them to transfer crypto assets instantly across the world and onboard customers in different jurisdictions. The risk is further increased when they process or facilitate transactions or offer products or services which contain privacy-enhancing features or which offer a higher degree of anonymity.	CASPs should be mindful that they are exposed to ML/TF risks due to specific features of their business model and technology used as part of their business which allows them to transfer crypto assets instantly across the world and onboard customers in different jurisdictions. This risk is further increased when they process or facilitate transactions or offer products or services which contain privacy-enhancing features, or which offer a higher degree of anonymity. Relevant employees of CASPs should be trained to get a better understanding about general principles of crypto assets in relation with ML/TF risks.	Guideline 6 already highlights the requirements of training. However, it is only a general guideline that applies to all firms. For CASPs, it is important to highlight the training on the understanding of the technical aspects of crypto assets.
21.3 a)	The following factors may contribute to increasing risk: a) the products or services offered by CASPs entail privacy-enhancing features or offer a higher degree of anonymity such as, but not limited to, mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins;	a) the products or services offered by CASPs entail privacy-enhancing features or offer a higher degree of anonymity such as, but not limited to, mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs, so-called privacy coins and when a significant proportion of the crypto assets involved in a transaction are associated with second-party escrow services;	This is also an important example of ways to have a higher degree of anonymity, because escrow services provider can act as an intermediary to offer services involving smart contract technology that buyers can use to send or transfer money in exchange for crypto-assets when the provider has custody over the crypto-assets. Having this example can help firms to recognize such transactions better.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.3	The following factors may contribute to **increasing risk**: a) […] b) […] c) […] d) […] e) […] f) […]	*Addition of letter g):* g) the results of an analysis ran by advanced analytics tools indicate a higher ML/TF risk.	Any result indicating a higher ML/TF should also be considered as a factor increasing ML/TF risk.
21.4	The following factors may contribute to **reducing risk**: a) […] b) […] c) […] d) […]	*Addition of letter e):* e) the results of an analysis ran by advanced analytics tools indicate a lower ML/TF risk.	Any result indicating a higher ML/TF should also be considered as a factor reducing ML/TF risk.
21.5 a) vi.	The following factors may contribute to **increasing risk**: a) Regarding the **nature of the customer** in particular: […] vi. an undertaking or a person who is using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.	iv. an undertaking or a person who is using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails, anonymous or temporary email services and VPNs.	The use of anonymous or randomly generated email increases the anonymity of a customer. This makes it difficult to know who is the originator or the beneficiary behind the transaction. The same applies to customers using temporary email services. Such feature increases ML/TF risks.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.5 b) i.	b) Regarding the **customer's behavior**, situations where the customer: i. tries to open multiple crypto asset accounts with the CASP;	i. tries to open multiple crypto asset accounts with the CASP and/or creates separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by CASPs;	This is an indication of ML/TF risk.
21.5 b) ii. b)	b) Regarding the **customer's behavior**, situations where the customer: i. […] ii. Or the customer's beneficial owner is unable or unwilling to provide the necessary CDD information, without any legitimate reason for it, by: a) […] b) trying to obscure the beneficial owner of the funds through the engagement of agents or associates, such as providers or trust services or corporate services, in the business relationship or transactions;	b) trying to obscure the beneficial owner of the funds through the engagement of agents or associates, such as providers or trust services or corporate services or money transmitters, in the business relationship or transactions;	The use of money transmitters can be seen as an increasing ML/TF risk, especially if the money transmitters cannot produce the required CDD information and documentations.
21.5 b) xv. c)	Repeatedly receives crypto assets from or sends crypto assets to: […] c) a newly created crypto asset account or a distributed ledger address held by a third party;	c) A newly created or previously inactive crypto asset account or a distributed ledger address held by a third party;	Previously inactive accounts can be used for fraud or for ML/TF purposes.
21.5 b) xv.	Repeatedly receives crypto assets from or sends crypto assets to: […]	*Addition of letter h):* h) the customer's different crypto asset accounts or distributed ledger addresses held by the same or different CASP(s);	This behavior can increase ML/TF risk, because it can be a behavior aiming to layer the transaction for ML/TF purposes.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.5 b)	The following factors may contribute to **increasing risk**: a) […] b) regarding the **customer's behaviour,** situations where the customer: i. […] ii. […] iii. […]	*Addition of the following factor that may contribute to increasing risk:* appears to obtain the crypto asset which comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes, sanctioned bitcoin addresses or gambling sites.	The source of funds and the source of wealth are two important pieces of customer information in the AML/CFT domain, especially if the transactions or business activities are deemed to be of increasing risk. Therefore, if the source of the crypto asset is associated with the darknet or illegal/high risk sources, the customer's behavior could indicate higher ML/TF risk.
		Addition of the following factor that may contribute to increasing risk: deposits crypto assets at an exchange and then immediately withdraws the crypto assets from a CASP to a private wallet.	This effectively turns the CASPs into a money laundering mixer, which increases ML/TF risk.
		Addition of the following factor that may contribute to increasing risk: claims that the crypto asset the customer wishes to exchange for another crypto asset or fiat currency, has been obtained through mining or staking rewards, when the transaction fees are not proportionate to the value of the transferred crypto asset.	Crypto assets transactions involve transaction fees that are generally proportional to the amount of computation or storage that is required to perform the transaction. Claiming that a crypto asset was obtained through mining or staking rewards, while transaction fees being significantly disproportionate to the transferred asset's value. In essence, this could be utilized as a method to engage in money laundering, wherein the miner or staker fabricates an excessively high transaction fee to launder money discreetly.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.5 b) xv.	Repeatedly receives crypto assets from or sends crypto assets to: […]	*Addition of letter h):* h) the customer's different crypto asset accounts or distributed ledger addresses held by the same or different CASP(s);	This behavior can increase ML/TF risk, because it can be a behavior aiming to layer the transaction for ML/TF purposes.
21.7 b)	The originating or the beneficiary crypto asset account or a distributed ledger address is linked to a jurisdiction: i. […] ii. […]	*Addition of new number iii.:* iii. with no or no robust regulation on crypto assets.	Many jurisdictions are engaging with CASPs yet have no or relatively poor regulatory framework on crypto assets. The current EU third-country high risk list does not necessary cover jurisdictions with weak regulatory framework on crypto assets. Therefore, this element should be considered as a country or geographical risk factor that contribute to increasing ML/TF risk.
21.12 a)	[…] In addition, CASPs should apply the following EDD measures: a) verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source. b) […] c) […]	a) verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source. In order to assist in verifying the customer's identity, CASPs should corroborate the identity information received from the customer with additional information such as an IP address with an associated time stamp; geo-location data; device identifiers; wallet addresses; and transaction hashes.	The identification and verification of CASPs' customers should contain additional measures compared to other industries, as CASPs usually conduct non-face to face business relationship with their customers and online business relationship offers a certain level of anonymity. Elements such as IP address with an associated time stamp, geo-location data, device identifiers, wallet addresses and transaction hashes, all represent the digital identity of a person. Therefore, it is important to use these elements for the identification and verification of CASPs' customers.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.16	Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849 and Guidelines 5.1 and 5.2 above.	Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849 and Guidelines 5.1 and 5.2 above. For example, the information available on the distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. Additional information and procedures will therefore be necessary to associate the address to a private key controlled by a natural or legal person.	A clear example of why reliance on distributed ledger for recordkeeping is not sufficient to emphasize the importance of additional steps to be taken.

Question 9: Do you have any comments on the proposed changes to Guideline 21.

Guideline	EBA's proposed amendments	Our suggestion	Our argument
21.16	Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849 and Guidelines 5.1 and 5.2 above.	Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849, Directive 2015/847 and Guidelines 5.1 and 5.2 above.	Directive 2015/847 includes also record keeping requirements that must be complied with by firms.
21.16	See Record Keeping chapter under Guideline 21. Currently, only 21.16 exists: Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849 and Guidelines 5.1 and 5.2 above.	*Addition of new article 21.17:* Records should at least include information relating to the identification and verification of relevant parties. Examples of information for record keeping may include: - The originator's name and the name of the beneficiary; - The address and date and place of birth of the originator/beneficiary; - The public keys (or equivalent identifiers) of relevant parties; - The addresses or accounts (or equivalent identifiers); - The nature (e.g., deposit, transfer, exchange) and date of transactions; - Amounts transferred; and - Where an account is not used to process the transfer of crypto assets, the unique transaction reference number or transaction hash that permits traceability of the transaction.	Since guideline 21 is new, concrete examples of records that should be kept regarding CASPs would give a good industry guidance on what the record-keeping requirements are for CASPs.

Extra suggestion

Guideline	EBA's original guideline	EBA's proposed amendments	Our suggestion	Our argument
All except 9 and 16	See EBA Guidelines for the full guideline.	None.	*Guideline 9 and 16 explains to whom firms CDD measures should apply. We suggest to add such section to all other sectoral guidelines.*	Such addition can clarify who is obliged to comply with CDD requirements, in order to comply to the Directive (EU) 2015/849.

Deloitte.