European FinTech Association

# Position Paper
# on
# Anti-Money Laundering
# and
# Know Your Customer Procedures

(June 2020)

# Executive Summary

**The European FinTech Association (EFA) calls for:**

1) **EU-wide harmonization of digital identification methods**

   - Minimum set of qualified methods and criteria for the digital identification of customers need to be accepted EU-wide

   - Facilitating third party reliance via mutual recognition of AML-compliant identification procedures across EU member states is key for safe and convenient KYC procedures. The design of applicable “suitable safeguards” as described by recital 35 AMLD should be conclusive on the European level

2) **Transsectoral approach for mutual recognition of ID-levels between different regulated sectors**

   - “eIDAS” Regulation (EU) No. 910/2014 and use of Qualified electronic signatures (QES) could provide for identification standard that facilitates interoperability of digital identities across industry sectors, including banking, health, mobility, public and telecommunication

3) **More regulatory guidance regarding application of AML rules to new regulated services, e.g. via circulars or guidelines**

4) **Re-consideration of AML Rules for Account Information Service and Payment Initiation Service Providers**

5) **Harmonization of Suspicious Transaction Reporting and improving the cooperation between the FIUs according to Art. 52, 53 AMLD**

# 1. Introduction

The European FinTech Association (EFA), in its effort to give content input to the European legislators, has identified certain key topics that are an impediment to a single European market for financial services and more specifically for digital business models. Anti-money laundering (AML) rules play an important role as they constitute a key regulatory framework for the activities of FinTechs across Europe. These rules and their implementation are central to the members of EFA, and we would like to give our support to the involved legislators and regulators to promote a safer marketplace. From our perspective, AML rules need to evolve to make sure that they address cross-border and digital services in a proportionate and effective manner.

The European market on financial services is still to a large extent fragmented along national borders, and one of the central reasons for this is the existence of diverging AML rules. We have identified certain topics that create difficulties for cross-border financial services across various business models. These include in particular:

- Different methods for the identification of customers;
- Diverging rules for third party reliance for the identification of customers;
- Incoherent extension of the AML rules to new business models and regulated services; and
- The lack of harmonization of suspicious transaction reporting.

In these areas, there remains a fractured framework, which is an obstacle for a modern, digital and European market for financial services. It means that FinTechs need to implement different types of identification depending on the jurisdiction in which they are active. This has a severe impact on the development of EU-wide solutions for the product offering. For example, having different identification methods for one mobile app or website depending on the country from which the customer is accessing the website is a big challenge from a legal, operational and technical perspective. It leads to substantial costs as well as substantial delays in the roll-out of business models across Europe. It actually even leads to products not being offered in certain jurisdictions because the identification method is from a practical perspective not possible to implement.

# 2. Harmonized Methods for the Digital Identification of Customers across EU Member States

***Position:***

*The methods for the digital identification of customers need to be harmonized to the extent that at least a minimum set of qualified methods for identification and the combination thereof need to be accepted EU-wide. These identification methods should include the following:*

- *Identification via a trust service according to Regulation (EU) No. 910/2014, including the use of QES as an identification tool;*
- *Video-Identification of the customer based on certain safeguards;*
- *Identification based on copies of two documents (e.g. always including a copy of an official ID) and a reference transaction to or from an account of the customer;*
- *Identification based on copies of two documents (e.g. always including a copy of an official ID) and a declaration by an obliged entity to have identified the customer. This in particular includes systems of pooled identification by obliged entities (e.g. BankID in Sweden);*
- *Identification of an automated process based on certain safeguards, e.g. Liveness detection, biometric identification or fingerprint; and*
- *Identification via review of reliable database sources or data pools (see e.g. BankID in Sweden).*

## A. Background

The rules for identification are not harmonized on the European level. Art. 11 of Directive (EU) 2015/849 (together with Directive 843/2018, "AMLD") requires the Member States to ensure that obliged entities apply customer due diligence measures when establishing a business relationship. This includes that the obliged entity identifies the customer (Art. 13 (1) lit. a AMLD) and the beneficial owner (Art. 13 (1) lit. b AMLD), and assesses the nature of the business relationship (Art. 13 (1) lit. c AMLD). In addition, the obliged entity must conduct ongoing monitoring of the business relationship (Art. 13 (1) lit. d AMLD). In practice, the rules for identification vary to a large extent and make it impossible to use one identification method for business models across Europe. European law only indirectly stipulates in Annex III of the AMLD which conditions should be applied to the digital identification. It considers non face-to-face identification, which includes digital identification, as a risk factor under the following conditions:

> *"non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities"*

The AMLD allows the use of trust services for identification as defined in Regulation (EU) No. 910/2014. With regard to further identification methods, it refers to processes that are "regulated, recognized, approved or accepted by relevant national authorities". Thus, the matter is passed on to the national legislators and regulators to single out identification methods that they qualify as sufficient in order to identify a customer during the onboarding.

The national legislators and regulators have taken different approaches with regard to this. Many countries have not provided public guidelines with regard to identification methods that they consider sufficient for the identification of customers.

Some jurisdictions have explicitly regulated the types of identification methods. We have included additional information as deep-dives in Exhibit 1. Most notably the following identification methods have been regulated:

- The identification via trust service providers regulated under Regulation (EU) No. 910/2014 is permitted in most countries. However, there are differences as regards the level of assurance that has to be used. In some countries, an advanced electronic signature is sufficient (e.g. BankID in Sweden) – in other countries, a qualified electronic signature plus a reference transaction are necessary.

- The video-identification system has been notably developed and regulated in Germany. The customer is interviewed via video-call and needs to show his/her passport in various ways following a strict, regulated procedure. In Italy, the Bank of Italy has recently updated its measures on customer due diligence providing that video-identification shall be considered an adequate method to identify customers if certain requirements are met. Video-identification is not permissible in all jurisdictions, e.g. in France, the regulator does not consider video-identification sufficient. In Spain, the regulator provided different requirements for video-identification than the German regulator.

- Most jurisdictions allow identification in a combination of a copy of an identification document – in some cases plus a copy of another document, e.g. utility bill (France) – in combination with a reference transaction. The reference transaction may be executed from an account held at a licensed entity in the name of the customer to an account held by the obliged entity or by the obliged entity to an account of the customer held at a licensed entity.

- Some jurisdictions allow identification in a combination of a copy of an identification document – in some cases plus a copy of another document, e.g. utility bill (France) – in combination with a declaration by another obliged entity that it knows the person.

- Many jurisdictions apply a risk-based approach and leave the method of identification to the relevant obliged entities. In these cases, identification methods are designed by the relevant obliged entities. Identification needs to be effective. However, no specific rules apply to such identification.

- FinTechs have developed customized identification methods for such countries. This includes in particular the so-called automated identification. This process can include, e.g., the following components: (i) gathering of information on the person; (ii) one or more photographs or video of an identification document (e.g. to capture different safety elements), (iii) automated reading of the content of the ID and check for consistency with the information given by the customer, (iv) video of the person being identified, (v) assessment of further information gathered in the background (e.g. IP address, geo-location).

- In some jurisdictions, verification based on reviews of databases is accepted as part of the identification process. This is in particular the case for the UK. However, this requires reliable database sources, which are not the case for most European jurisdictions.

**B. Challenges for FinTechs based on the Different Rules for Digital Identification Methods**

Different rules on acceptable identification methods make it difficult to scale business models cross-border. In particular, there are no solutions for identifying customers digitally across Europe in all jurisdictions. The possibility, which comes closest to an identification across Europe, is the identification via a trust service provider, i.e. using an EIDAS certified provider. We fully support the measures taken

by the European Union to strengthen the use of this mechanism. Nevertheless, this identification method cannot be used across Europe for practical reasons. The underlying technology is - generally speaking - not available for customers in all countries. For example, many of the trust service providers require that customers have an electronic identification card. Such eIDs, however, are not available in all jurisdictions across Europe. For other identification methods there are major jurisdictions that do not accept these methods, e.g. in France, where video-identification is not accepted and identification via reference transaction is not considered sufficient for the identification. Furthermore, some identification methods that may be accepted by customers in some countries are not acceptable to customers in other countries.

In the context of platform models, this divergence can also create a situation in which clients have to be identified differently depending on the specific situation at hand. For example, under the prevalent crowdfunding models, the identification method for a borrower/project owner depends on the home jurisdiction of the investor. In many cases, this almost rules out cross-border investment given that a German investor may be obliged to carry out checks on a Dutch borrower via video-identification, which is not offered in that country.

Further, the disparity of identification methods also leads to regulatory arbitrage and a race to the bottom. As financial institutions – based on the passporting mechanism – according to Art. 39 *et seq.* Directive EU No. 36/2013 may offer their products cross-border and under the AML law of the home jurisdiction, companies have an incentive to search for the jurisdiction with a low standard with regard to the identification method. This cannot be in the interest of the fight against money laundering across Europe.

# 3. Harmonized Rules on Third Party Reliance

***Position*:**

*The Rules on Third Party Reliance should be further harmonized. The rules on third party reliance and especially on the design of applicable "suitable safeguards" as described by recital 35 AMLD should be conclusive on the European level. The current AMLD contains sufficient measures to safeguard not only the quality, but also the non-discrimination of service providers. These include in particular:*

- *reliance is possible either on an obliged entity, which is licensed within the European Economic Area, or - based on a contract – on a reliable third party;*
- *the institution is supervised by a regulator from the EEA and hence subject to European regulatory requirements; and*
- *the institution is subject to the national implementation of the AMLD and subject to regulatory oversight with regard to the AMLD.*

*There should be a concrete set of requirements on the EU level that include further safeguards which are not subject to interpretation by individual member states and which do not allow further gold plating from national legislators/regulators. If necessary, there should be an amendment to AMLD with regard to this set of requirements.*

## A. Background

Art. 25 AMLD stipulates that Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements, amongst those the identification of the customer and the beneficial owner as well as the assessment and the obtaining of information on the purpose and intended nature of the business relationship. Recital 35 of the AMLD acknowledges the necessity to avoid undue delays and facilitate the process for customers and the obliged entity:

> *"In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for customer due diligence should remain with the obliged entity to which the customer is introduced. [...]"*

The AMLD does not elaborate further on the design of these so-called suitable safeguards. National legislators and regulators have taken different approaches with regard to these safeguards. Many countries have chosen to gold-plate these provisions, which makes the process of scaling-up business models increasingly difficult.

The additional requirements for third party reliance depend on each jurisdiction. We have encountered in particular the following:

- Requirement that the third party must have collected the customer's data in order to establish an "own business relationship" with the customer, if the identification was made on an earlier date (Germany).

- Requirement that the third party collected the information "directly" from the customer (Italy and Germany). The specific meaning of this restriction, however, is not further defined.

- Obligation to conclude a contract between the obliged entity and the third part (Ireland, United Kingdom, Netherlands, Spain, Luxembourg).

- Time limitations between the original identification and the use of the identification for reliance, e.g. 24 months and obligation to re-identify the customer if the identification document has expired in the meantime (Germany).

We have included the legal/regulatory basis for these requirements in Exhibit 2 to this paper.

**B. Challenges for FinTechs due to Inconsistent Rules on Third Party Reliance**

There are various business models of European FinTechs that build on a cooperation between multiple parties that are obliged entities. Examples for these business models are asset management/robo-advisors and deposit brokerage platforms. In these business models FinTechs cooperate with a custodian/sponsor banks and further product offering banks. These business models provide customers, who have already been identified whilst opening an account with an existing market participant, with access to a variety of services. Under the current set of rules in some jurisdictions, customers do have to be identified multiple times by new service providers.

This requires more effort for the client and leads to lower acceptance rates of new, digital business models and therefore does not comply with the stated goals of digital and open-banking initiatives.

In particular, a criterion regarding the time at which the data was collected will lead to significant disruptions in the FinTech industry by way of obstructing the customer friendly provision of services. Without having to – as the AMLD does not require such an “age limit” for the data collected. Moreover, the constant and continuous AML compliant supervision of the customer within the existing business relationship with the “original” AML obliged entity which serves as a third party provides for an even higher security level as an additional one-time identification procedure.

A very strict set of safeguards favours institutions with an existing customer base and a wide range of products and adversely affects new, innovative business models. This particularly disadvantages business models that include various obliged entities, such as the above mentioned providers of asset management and deposit intermediation. The effort of completing multiple identifications leads to a “lock-in effect” that favours incumbent companies benefit and harms overall competition.

# 4. Re-consideration of AML Rules for Account Information Service and Payment Initiation Service Providers

AML rules should apply to cases where business models have a clear connection with money laundering risks. For example, where businesses are responsible for executing transactions and come into possession of customer funds.

When the new Payment Services of Account Information Service (AIS) and Payment Initiation Service (PIS) were introduced by PSD2, providers of both services were automatically classed as obliged entities under AMLD, despite the fact that neither type of provider executes transactions or comes into possession of funds. As the EBA itself acknowledges in its recent Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and ML/TF risk factors (EBA's Risk Sector AML Guidelines), "the inherent ML/TF risk associated with [these services] is limited" for these very reasons.

The inclusion of these services needs to be re-examined as part of the Commission's AML action plan, to remove duplication and friction which will ultimately prevent consumer take-up of these innovative new services and hamper innovation and competition.

We ask that the EBA's Risk Sector AML Guidelines are not finalised until the conclusion of the Commission's consultation - particularly given the contention around whether AIS and PIS were intended to be included as obliged entities, or whether this was the unintentional result of cross referencing between PSD2, CRD and AMLD.

If, despite their low risk, PISPs were to remain in scope of AMLD, a number of changes need to be made to ensure PIS business models remain viable:

- Since PISPs' primary relationship is with the online merchant (with whom they contract to provide the regulated service) it should be clarified that AML due diligence is required to be carried out on the PISPs merchant client, and not on every PSU who makes purchases from the merchant via PIS. To do otherwise will hugely disadvantage PISPs compared to other payment methods, who are not under this obligation.

- If PISPs are to be required to undertake transaction monitoring, banks must be required to return certain information about the PSU to the PISP including via API (BIC, IBAN, and name of the account holder). This is necessary to allow PISPs to uniquely identify transactions, without adding extra dissuasive steps into the PSU's payment experience.

# 5. Harmonization of Suspicious Transaction Reporting

Credit institutions, financial or payment providers are obligated to perform Suspicious Transaction Reporting (STR) in case of facts that indicate that the account behavior is suspicious. The required reporting needs to be submitted to the respective local Financial Intelligence Unit (FIU) where the respective credit institution, financial or payment provider has its head office (home country).

With respect to the offering of bank businesses, financial or payment services within the aforementioned cross border service passport regime, the current STR leads to the problem that suspicious behavior of customers within the passported countries needs to be reported to the FIU of the home country of the credit institution, financial or payment provider. However, the home country FIU generally is not the authority to investigate such cases. To give an example: A German credit institution acts via cross border service passport into France. A French customer who engages in suspicious activity needs to be reported to the German FIU.

From our experience, the home country FIU does not transmit the STRs to the respective local FIU, i.e. the authority that should actually investigate the case or forward the case to the local enforcement agencies is not aware of the cases. Therefore, an effective law enforcement is not in place and criminals are aware of this loophole and know that they are not being prosecuted.

We recommend to improve the cooperation between the FIUs according to Art. 52, 53 AMLD.

# Exhibit 1:
# Deep-Dive Diverging Rules on Identification Systems

Germany

In Germany, the regulator has provided detailed guidelines for identification via video-identification. According to the circular 3/2017 of the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*, "**BaFin**"), identification via video-identification is defined in detail (English version available under this link). The process includes several requirements regarding the training of the employees, the premises, the consent by the customer, technical and organizational measures and the actual performance of the video discussion. The video identification per se consists of several steps that aim at excluding fraud by customers, verifying the authenticity of the identification documents by several means. There are specialized providers available in Germany that perform these services.

The video-identification procedure from Germany works as well in further European countries, e.g. in Austria, but cannot be used for business models across Europe mainly for three reasons:

- The process has specific technical requirements that exclude certain countries from its use. For example, in Italy, the majority of customers still own and use old identification cards that do not fulfil the requirements under Circular 3/2017.

- In some jurisdictions the regulator does not allow video-identification for the identification of its customers, e.g. in France.

- The process is rather sophisticated. Thus its implementation is labor and cost-intensive and time consuming. Customers from many countries do not accept this process and refuse to use it.

In addition, Germany allows for the identification of the person via a trust service provider regulated under Regulation (EU) No. 910/2014 ("**EIDAS-Regulation**"). This may be done via a qualified electronic signature according to Art. 3 No. 12 EIDAS-Regulation or a notified electronic identification system according to Art. 8 (2) lit. c in connection with Art. 9 EIDAS-Regulation. However, in case of the use of a qualified electronic signature, the customer needs to make a reference transaction from an account held in the name of the customer.

France

In France, the regulator has adopted a system under which the obliged entities may choose from a set of measures. The obliged entities need to use at least two of the following measures (cf. Article R561-20 Code Monétaire et Financier and No. 47 *et seq.* Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, Dec. 2018):

- Obtain a copy of an official identification document plus an additional document identifying the customer (e.g. utility bill);
- Obtain an independent third party verification of an official identification document;
- Require that the first payment is made from or to an account held in the name of the customer with an obliged entity located and regulated within the EEA;
- Obtain a direct confirmation of the identity of the person by a third party, which is an obliged entity;
- Use a trust service provider as stated in Regulation (EU) No. 910/2014; or
- Use an advanced or qualified electronic signature relying on a valid certificate by a service provider according to Regulation (EU) No. 910/2014.

In essence, this allows for the identification in particular using the following methods:

- Trust service providers regulated under Regulation (EU) No. 910/2014;
- Providing a copy of two identification documents (e.g. ID and utility bill) and receipt or execution of a reference transaction from/to an account of the customer at another obliged entity regulated in the EU/EEA;
- Providing a copy of two identification documents (e.g. ID and utility bill) and receipt of a confirmation from another obliged entity regulated in the EU/EEA.

In contrast, France does not allow for the use of a video-identification process.

Italy

In Italy, the regulation has recently been reviewed in order to transpose the provisions of the AMLD into the national legal framework. The new rules have been incorporated into the Legislative Decree No. 231/2007 (the "**Italian AML Decree**") and into the new "Provisions concerning customer due diligence for anti money laundering and counter terrorism financing purposes" issued by the Bank of Italy on 30th July 2019 and effective as of 1st January 2020 (the "**Italian CDD Measures**").

According to both the Italian AML Decree (Article 19) and the Italian CDD Measures (Part I - Section VIII), obliged entities shall be deemed to have fulfilled their obligations with regard to non-face-to-face identification in the following cases:

- customers whose identity has been verified in the context of public authentic instruments (*atti pubblici*), private deeds authenticated by a Public Notary (scritture private autenticate) or qualified certificates used to generate a digital signature in accordance with article 24 of Legislative Decree No. 82 of 7th March 2005 (the "Digital Administration Code");

- customers with a high-level security digital identity in accordance with article 64 of the Digital Administration Code or with Article 9 of Regulation (EU) 910/2014;

- customers whose identifying data result from a statement issued by the Italian Consular Authority;

- customers whose identity had already been verified by the obliged entity in the context of another business relationship or in the context of the provision of another service, as long as the existing information on the customer is up to date and suitable to the risk profile of the client;

- customers whose identity have been verified through adequate measures, according to the instructions coming from the National Competent Authorities.

The Italian CDD Measures provide further detail on the adequate measures mentioned above under bullet point 5, clarifying that, in the case of non-face-to-face identification, obliged entities shall:

- obtain the identifying data of the client and check them against a copy of an up to date ID document (received either via fax, post, email or equivalent means);

- carry out further checks on the received information, in proportion to the specific level of risk, for instance, they can make welcome calls, send communications via registered mail with return receipt to a physical domicile, ask the customer to make a bank transfer using a financial intermediary with offices in Italy or another Member State, request the customer to send back countersigned documents, request the competent offices for proof of residence. These checks may also be carried out through innovative and reliable technologies (such as biometric recognition) if they are accompanied by adequate security safeguards.

- incorporate a description of the measures that they wish to adopt to perform the aforementioned checks in their AML policy.

As an alternative to the requirements set out above, obliged entities may identify their customers following the audio/video identification procedure set out in Annex III to the Italian CDD Measures.

Insurance undertakings and intermediaries operating in the life insurance sector are subject to the analogous requirements introduced by the National Competent Authority ("**Istituto di Vigilanza sulle Assicurazioni**" or "**IVASS**") with the IVASS Regulation No. 44 of 12th Feburary 2019 ("**IVASS AML Regulation**") (article 39).

The Netherlands

In the Netherlands, the act implementing AMLD, the amended Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en het financieren van terrorisme* – "**Wwft**"), entered into force on 25 July 2018. The regulation implementing the Wwft ('*Uitvoeringsregeling Wwft*') contains a list of documents that qualify as information from reliable and independent sources as meant in the Wwft. This list currently contains ID-documents such as a valid passport or a valid Dutch driver's license. The list does not include any specific document or information from a 'digital solution' for the identification and the verification of the identity of the business relationship.

The list included in the regulation implementing the Wwft is a non-exhaustive list. Both the Authority for the Financial Markets ("**AFM**") and the Dutch Central Bank (*De Nederlandsche Bank* – "**DNB**") state that other documents/information from a reliable and independent source may be used. However, they do not provide examples of sources that qualify as such. It is up to the obliged entity to assess whether a source qualifies as a reliable and independent source as meant in the Wwft, taking into account the applicable risk factors.

Latvia:

On July 3rd, 2018, the Latvian Cabinet of Ministers adopted Cabinet of Ministers Regulation No.392 on the requirements for remote customer identification. According to this regulation, companies are obligated to use one or several of the following measures depending on their ML risk:

- a secure electronic signature which provides qualified electronic identification with enhanced security that corresponds to the level determined in accordance with laws and regulations or Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- video identification;
- acquisition of data accrediting the identity of a natural person from a credit institution or payment institution by using an identification payment or another method which enables the receipt of the data necessary for the customer identification from a credit institution or payment institution;
- comparison of the photograph in a personal identity document and electronic self-portrait photograph.

The regulation stipulates strict requirements for performing video identification.

The principal issues regarding remote customer identification encountered by Latvian companies are:

- documents that do not contain optical security features (e.g., holographic cinematographic signs or printed elements with latent image effects) cannot be accepted, which applies for example to old Italian ID cards;

- it is prohibited to accept identification documents with overdue expiry dates on the face of the document even if, under the law of the country of issue, the document is valid beyond the expiry date indicated. For example, such is the case with French ID cards;

- in some other countries (e.g., Poland, Denmark), citizens either refuse to submit copies of their documents, claiming they are prohibited to do so by law, or submit partially covered copies to service providers. In contrast, Latvian legislation requires customers to provide uncovered, clearly visible copies of identification documents during the identification process.

# Exhibit 2:
# Additional Requirements for Third Party Reliance

Germany

In Germany, the most recent amendment of the German Money Laundering Act (*Geldwäschegesetz*, "**GwG**") and the Interpretation and Application Guidance in relation to the German Money Laundering Act of BaFin of December 2018 (*Auslegungs- und Anwendungshinweise zum Geldwäschegesetz* - "**AuA GwG**") provide for additional requirements for the reliance on third parties. Section 17 para. 3a GwG and Section 8.4 AuA-GwG limit the forwarding of an identification data record (English version available under this link). Section 17 para. 3a GwG and Sec. 8.4 AuA-GwG stipulate that identification by a third party by way of forwarding of data collected during previous identification is, inter alia, subject to the following preconditions:

- The third party must have collected the data of the contracting party in order to establish a separate business relationship. Forwarding of data collected on the basis of simplified due diligence obligations is not permitted.
- These data have been collected within the past 24 months.
- At the time of use of the identification data, the validity date of the identification document may not yet have expired. In addition, the obliged entity must be notified of the date of "initial identification".

The amendment of the German Money Laundering Act (*Geldwäschegesetz*, "**GwG**") came into effect in January 2020 and incorporates the aforementioned preconditions but allows for the data to have been either collected *or updated* within the past 24 months prior to forwarding. However, the amendment does not provide details on what "update" shall mean in this regard.

Ireland

In Ireland, Art. 40 (4) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 requires a relying entity to conclude an arrangement on the reliance. In September 2019, the Central Bank of Ireland ("**CBI**") issued its "Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector" ("**CBI AML Guidelines**", link to the guidelines) which state in Sec. 5.2.6 and 9.2.5 that this arrangement needs to be signed and in writing. The reliance is de facto void in the absence of such a written agreement.

Furthermore, the relying entity needs to set out policies and procedures with regard to the identification, assessment, selection and monitoring of third party relationships, including the frequency of testing performed on such third parties, Sec. 5.2.6 of the CBI AML Guidelines.

UK

In the UK, Art. 39 (2) (b) of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (link to the regulations) requires the relying entity to enter into arrangements with the third party enabling the relying entity to obtain from the third party, immediately on request, copies of any identification and verification data and any other relevant documentation on the identity of the customer, customer's beneficial owner, or any person acting on behalf of the customer. It also requires the third party to retain copies of those data and documents for the same period as the relying entity would be obligated to.

Netherlands

In the Netherlands, § 2.4 Art. 10 of the Dutch Law on the prevention of money laundering and terrorist financing (*Wet ter voorkoming van witwassen en financieren van terrorisme* – "**Wwft**") stipulates, for the externalisation of the customer due diligence, that an obligated entity shall agree with the third party in writing if such externalisation is of "structural nature", without differentiating between reliance in third parties and outsourcing to third parties.

Spain

In Spain, Art. 8 (3) of the Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo ("**Spanish AML Act**") requires the prior conclusion of a written agreement prior to any reliance on third parties. This is clarified by Sec. 13 (3) of the Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo ("**Spanish AML Decree**").

Luxembourg

In Luxembourg, the Luxembourg Financial Supervisory Authority (*Commission de Surveillance du Secteur Financier* - "**CSSF**") has issued Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing ("**CSSF Regulation**") clarifying the requirements regarding the reliance on third parties set out in Art. 3-3 of the Law of 12 November 2004 on the fight against money laundering and terrorist financing ("**Luxembourg AML Act**") and the Grand-ducal Regulation of 1 February 2010 providing details on certain provisions of the amended law of 12 November 2004 on the fight against money laundering and terrorist financing ("**Grand-ducal Regulation**").

The CSSF Regulation stipulates, among others, that the third party needs to commit in writing to fulfil the obligations laid out on third party reliance in the Grand-ducal Regulation (Art. 36 second en dash).

Austria

In Austria, obligated entities may rely on third parties unless they have indications which cast doubt on an equivalent fulfilment of the customer due diligence, Sec. 13 (1) of the Austrian Anti Money Laundering Act (*Finanzmarkt-Geldwäschegesetz* – "**FM-GwG**"). This is clarified by the Circular on the Duties of Care on the Prevention of Money Laundering and Terrorist Financing (Document Number: 09/2018, published on 18 December 2018) issued by the Austrian Financial Supervisory Authority (*Österreichische Finanzmarktaufsichtsbehörde* - "**FMA**"): the obligated entity shall not have any indications which cast doubt on the equivalent fulfilment of the duty of care, margin no. 13. Furthermore, if the AMLD has been implemented in the EU member state in which the third party has its registered office, the obligated entity may rely on the third party if, after carrying out the necessary plausibility check, the obligated entity has no indications which cast doubt on the third party's fulfilment of the corresponding due diligence and storage obligations in an equivalent manner, margin no. 17.

Italy

The legal requirements in relation to reliance on third parties are set out by the Italian AML Decree (articles from 26 to 30) and by the Italian CDD Measures (Part V).

According to both the Italian AML Decree and the Italian CDD Measures, without prejudice to their responsibility under the applicable law, obliged entities are allowed to rely on third parties to carry out some of the activities relating to their customer due diligence obligation. Eligible third parties include financial institutions based in Italy or in another Member State, as well as financial institutions based in a third country, provided that certain conditions are met. In the case of reliance on third parties, obliged entities shall be deemed to have fulfilled their obligations if the third party is able to issue a statement

confirming that it has carried out the relevant activities in the context of an ongoing business relationship or of a single transaction. Notwithstanding the above, obliged entities are requested to assess whether the information obtained and the checks performed by third parties are suitable to comply with the applicable legislation. Should obliged entities have any doubt, they shall identify the customer on their own.

Insurance undertakings and intermediaries operating in the life insurance sector are subject to the analogous requirements introduced with the IVASS AML Regulation (Chapter III - Section V).

**About us**

The European FinTech Association (EFA) is the first not-for-profit organization representing leading FinTech companies of all sizes, from across Europe.

We are designed by and for Europe's FinTech community. We aim to serve as a resource and forum for education, information sharing and networking between companies, policymakers and the general public.

For more information, visit www.eufintechs.com or follow @EFAssociation on Twitter.