****

**GEMALTO COMMENTS ON THE JOINT CONSULTATION PAPER JC 2015 061**

Gemalto welcomes the opportunity to comment on the Joint Consultation Paper JC 2015 061 on Simplified and Enhanced Customer Due Diligence. Our proposal is divided into two parts:

1. First, a series of comments in the different clauses of the consultation paper
2. Our opinion with regards the three precise questions raised by the EBA

|  |  |  |
| --- | --- | --- |
| TITLE | Section | Comment |
| **Scope** | 4. | It is asserted that these guidelines are addressed to the “firms”, namely credit and financial institutions. However, Title III addresses the risks for entities other than the “firms”. It is unclear whether Title III refers to specific factors that the “firms” have to assess prior to engaging in a business relationship with undertakings operating in the business identified in Title III. Or rather, there are guidelines also apply for internal use by entities operating in those sectors quoted in Title III, subject to AML/CFT themselves. |
| 6. | Do the “Competent authorities” in 6. refer to those monitoring AML practices for business activities identified in Title III ? If so, it should be clearly stated that this is the case. But definition in 8. The term “competent authority” refers to those competent for “firms” |
| **Assessing ML / TF Risk** | 31-37 | We understand that the guidelines let to each regulated firm the responsibility to decide on their own assessment in terms of “weighting risk factors”. This information if available would help criminals to profile the kind of firm featuring a risk policy minimizing the chances to identify their transactions as suspicious.  But on the other hand, the risk is that the under-specification of guidelines may lead to a real lack of harmonization of counter-measures facilitating financial crime. The traditional “regulatory shopping” between countries might well apply to the choice by criminals of firms with lower scoring practices in terms of monitoring transaction risks. |
| **Simplified Customer Due Diligence** | 41-45 | A critical process for services requiring security is the customer enrollment. For innovative payments a higher-than-expected level of fraud is often correlated with a flawed enrollment process. The robustness of the enrollment process should be the same for Simplified and for Enhanced Customer Due Diligence, because it will condition the efficiency of the overall Know Your Customer policy.  Thus the verification of the identity of the new customer on the basis of one document only, should be limited to official documents, available in all the EU member states such as a biometrics passport. But even in this case, Enhanced Customer Diligence (bullet 106.) needs more Ideally the firm should operate automatic processing devices able to authenticate the customer identity using biometric passport data. If the comparison is successful, the firm could then use the captured biometric for enrolling the new customer and issuing a secure firm device storing this biometrics.  Because at present authentication biometrics using the passport is exclusively allowed for cross-border checking in authorized countries, an agreement should be reached at political level, to authorize use of biometrics by the firms whilst enforcing practices that avoid the proliferation of the captured biometrics.  In particular the credentials issued to the customer during the enrollment should enable for instance the strong authentication of the customer at any time with a level similar to the ECD, even if strong authentication only applies for transactions exceeding a threshold according to the firm risk policy.  Additional advantages for this approach include:   * If the customer or beneficiary owner is aware that the information captured for the enrollment process enables a very precise monitoring of their future operations, the risk of ML/TF will be reduced * If a customer contracting low risk services at first, want to proceed to financial operations with potential for ML/TF , a closer CDD effort can be done by the firm without requiring further credentials to be issued   It is during the contractual lifetime, that application of guidelines in bullets 62.-67. Simplified Due Diligence, meaning an ongoing simplified yet proportionate level of monitoring might apply, avoiding cumbersome obligations. |
| **Enhanced Customer Due Diligence**  **(ECDD)** | 48. | This bullet is almost exactly a duplication of 47. Both could be merged in a single one.    As previously suggested, a common and robust enrollment process will enable the firm a flexible application of their Customer Due Diligence obligations based on the regular re-evaluation of precedent assessments:   * If this reevaluation provides evidence that the CDD effort should be enhanced, this extra effort will be done without necessary issuing new credentials * If the initial effort can be relaxed, only a partial use of the enrolled data may be needed. If it appears necessary to enhance CDD efforts that can be done by using the overall set of data available |
| 49. | The identification of the source of funds for ECDD is required from the basis of “reliable and independent” data. Are these sources those identified in bullets 14. to 16.? Is there any centralized database of information for firms foreseen for fight against ML/TF purposes? |
| **Sectorial Guidelines for money remitters** |  | This sector presents four specific characteristics, which makes it challenging from ML/TF risk assessment prevention prospective:   1. Cross-border remittances are a major driver for financial inclusion. 2. The identity of the ultimate beneficiary may be difficult to verify by the money remitter and may be outsourced to a local agent. This local agent should then be responsible to apply measures to prevent ML/CT. But documented evidence of the identity of the beneficiary may not be available. 3. Major actors in the remittance market are not firms 4. There are alternative remittance circuits usually unregulated that are suspected to be used for FT purposes   There is a strong social incentive to facilitate remittances.  May be specific guidelines on designing AML/CFT procedures that are not restrictive to beneficiary of remittances, usually unserved or underserved persons are needed.  This guidelines could be developed in coordination with international organizations such as the World Bank and the Basel Committee on Banking Supervision. |
| **Additional Comment** |  | An important question is whether or not the firm enables the opening of an account using exclusively an online process. The offer of this service raises the issue of the online identity verification of the customer in one hand, and also whether or not funds transfers to/from such an account should be under special scrutiny at least during a period of time long enough to provide evidence that the ML/TF risk associated with the customer or the beneficial owner is low.  The reliable verification of the identification online may not be easy when the customer is a citizen of a non-EEA state, but is to be enforced (bullet 55.) when the non-EEA state is a high risk third country. |

1. Do you consider that these guidelines Hare conducive to firms adopting risk-based, proportionate and effective AML/CFT policies and procedures in line with the requirements set out in Directive (EU) 2015/849?

The guidelines do not elaborate risk assessment for online or in branches operations. Transaction monitoring can allow holistic view of a customer transaction behavior (whether online or face-to-face), if an enterprise fraud management are set up. In this case all products and channels data can be set in one system, allowing to identify customer behavior with regards to his past behavior and to normal customer behavior of his kind. Yet online operations may need specific risk assessment. Customer registration and identity check may be more complex to set up as a process. Also, identity itself has to be protected. If transaction risk assessment can bring to customers some consequences linked to the output of the risk scoring, like the customers being signaled to authorities, then it is important that the online identity delivery process is secured, and that the use of the e-identity is secured as well. Also, transaction monitoring may request that in some cases (unusual transaction, risk of fraud or suspicion of infringement of AML directive), the transaction occurs only after another round of authentication, or transaction signature, to clearly link the customer to the transaction he is willing to perform. Identity is not only linked to the use of secured credentials, whether they are 2-factor authentication or 3-factor authentication, but also to the risk assessment of the context of the transaction. Device identity, device reputation, behavior analysis, session analysis, authentication method assessment, malware detection, all those technologies bundled together may refine the identity of a given customer at a given time, and will give a richer risk assessment than  just transaction monitoring. It will help to refine knowledge of malevolent behavior, and fraud or money laundering rings that have gone through various channels, products, and financial firms

1. Do you consider that these guidelines are conducive to competent authorities effectively monitoring firms’ compliance with applicable AML/CFT requirements in relation to individual risk assessments and the application of both simplified and enhanced customer due diligence measures?

Same as above. Besides device and customer reputation network, shared between many service providers acting in many different fields (banks, social networks, online game networks, merchants…) may be very effective into identity check and reputation risk score, thus refining the global risk assessment of a customer, at registration stage or at transaction stage

c) The guidelines in Title III of this consultation paper are organised by types of business. Respondents to this consultation paper are invited to express their views on whether such an approach gives sufficient clarity on the scope of application of the AMLD to the various entities subject to its requirements or whether it would be preferable to follow a legally-driven classification of the various sectors; for example, for the asset management sector, this would mean referring to entities covered by Directive 2009/65/EC and Directive 2011/61/EU and for the individual portfolio management or investment advice activities, or entities providing other investment services or activities, to entities covered by Directive 2014/65/EU.