"Your Identity Secured, your payments made Safe"

22/01/2016

European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA| UK

Joint Consultation Paper JC 2015 061 (21 Oct 2015)

Dear Sir / Madam,

We thank you for the opportunity to allow iSignthis BV to participate in the public consultation process.

This submission responds to the Joint Consultation Paper JC 2015 061 of 21 October 2015 by the European Supervisory Authorities (the **ESA**). The draft Guidelines set out therein are to be made pursuant to the Directive (EU) 2015/849 of 26 June 2015 (the **Directive**).

1. Submission by iSignthis BV

This submission is provided by iSignthis BV, a Netherlands registered legal entity (KvK-nummer 60762187), a wholly owned subsidiary of iSignthis Ltd, which is a company listed on the Australian Stock Exchange (code ISX).

iSignthis is a global leader in online, dynamic verification of identity and financial transactions via regulated e-payment instrument authentication. The automated, online identification of persons remote to the transaction is made possible via a patented electronic verification method, and is available to more than 3 billion customer accounts across more than 200 countries.

We provide the legal basis for compliance to meet customer identification requirements for AML/CTF obligated entities, as well as operational benefits for any online business looking to reducing customer on-boarding friction, mitigating CNP fraud, monitoring transactions and streamlining operations.

The iSignthis services are consistent with the requirements of key international regulatory supervisors including the European Banking Authority's Recommendations for the Security of Internet Payments.

iSignthis BV conforms with the EU Data Protection Directive[1], and is registered with both the Dutch Data Protection Agency and the United Kingdom's Information Commissioner.

iSignthis is also a Level 1 PCI DSS certified payment processor, and provides a Strong Customer Authentication platform that provides the basis for Payment Service Providers to conform with the requirements of the EBA's 'Recommendation for the Security of Internet Payments'[2].

2. Approaches to the Guidelines (Section 5.1)

It is our submission that the draft Guidelines are appropriate in terms of the option taken by the ESA in respect of:

a) Consistency with international AML/CFT standards (*paragraph 10 of Section 5.1*)
b) Structure of the Guidelines (*paragraph 21 of Section 5.1*)
c) Addressees (*paragraph 29 of Section 5.1*)
d) Level of prescription (*paragraph 40 of Section 5.1*).

The approaches adopted are conducive to risk based processes and procedures being used by firms in complying with the Guidelines and the Directive. We posit that in our opinion this is the correct approach.

3. Overview Questions (Section 5.2)

a) Do you consider that these guidelines are 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?

Subject to specific comments below in Section 5 of this Submission, it is our position that the draft Guidelines are conducive to firms adopting risk-based, proportionate and effective AML/CFT policies and procedures in line with the Directive.

[1] Directive 95/46/EC
[2] EBA-GL-2014-12 (Guidelines on the *security* of *internet payments*)

b) 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?

Subject to specific comments below in Section 5 of this Submission, it is our position that the draft Guidelines are conducive to competent authorities effectively monitoring firm's compliance with applicable AML/CFT requirements.

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.

Subject to comments below in Section 4 regarding missing sectoral guidelines, in organising the draft Guidelines by types of business, it is our position that the ESA has given sufficient clarity to the various entities subject to the requirements of the Guidelines.

4. Missing Sectoral Guidelines

We contend that there are several sectors that are subject to significant ML/TF risks, which do not have sectoral guidelines in Title III of the draft Guidelines but which ought to be covered in the final Guidelines.

These three sectors are namely Foreign Exchange, Gaming and Securities Trading.

We further contend that the Guidelines should not be made without including sectoral guidelines for these sectors given the ML/TF risks of these sectors, and the intense competition and significant number of new enterprises starting in these sectors across the EU.

In relation to the Foreign Exchange and Gaming sectors guidelines our recommendation is that they could be similar to or the same as those for electronic money issuers.

In relation to the Securities Trading sector guidelines our recommendation is that they could be similar to or the same as those for wealth management.

Whilst Gaming, including wagering, betting and games of chance, may not be specifically regulated by the ESA, the means with which these are funded online are certainly regulated by the ESA and they are predominantly by the use of payment instruments including cards, credit transfers or wallets.

These payment instruments are regulated under the Payment Services Directive 2[3], with authentication requirements per the European Banking Authority's 'Recommendations for the Security of Internet Payments'[4].

It is our position that the Customer Due Diligence requirements for remote identification of a customer, that intends to use either cards, wallet or credit transfer for online payment of gaming and other regulated services, should link i) the payment instrument to the ii) Strong Customer Authentication methodology (that is, two factor technology) *and* iii) link the customer's identity via customer due diligence.

In the case of cards, this would allow the European Central Bank's stated policy objective of 'One Leg Out' Authentication[5] to be achieved, and would allow the issuer of a payment instrument to be located outside of the European Union, provided that the acquirer is located and regulated within the Union.

There are a number of technologies that can verify a customer's ownership of a payment instrument from the acquiring side, independent of the dated 3D Secure platform. These new non-legacy technologies also resolve some of the security issues associated with the enrolment of cards to 3D Secure, one of which is the enrolment process. The enrolment process in many jurisdictions

[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)
[4] EBA/GL/2014/12_Rev1
[5] European Central Bank, 31 January 2013, Recommendations for the Security of Internet Payments : Outcome of the Public Consultation, Page 2

is the simple requirement to provide the card details together with the full name and date of birth of the user via an online enrolment process, which unfortunately provides a false sense of security under 'lost or stolen' wallet scenario, whereby the un-enrolled card is often lost together with other credentials.

These card verification technologies, that are independent of 3D Secure, have already been deployed by PayPal Inc (NASDAQ : PYPL) : and iSignthis Ltd (ASX : ISX) successfully over the course of many years, and they require the holder of the payment instrument to utilise their issuing institution's personalised security credentials to enrol the card (or subsequent use).

5. Details within the draft Guidelines

1. Paragraphs 1 to 3:

In our submission, it would assist firms and competent authorities to understand the effect of the Guidelines, if they were explicit as to whether compliance with these standards is a minimum requirement, or alternatively, that compliance would be effectively a 'safe harbour'.

2. Paragraph 10, dot point *CDD*, sub-paragraph (i):

We contend that it would assist with consistency if the sub-paragraph were to contain the words '*in a way that the firm is satisfied it knows who the customer is*', matching the phrase in sub-paragraph (ii) relating to a customer's beneficial owner.

3. Paragraph 12:

In our submission, the paragraph would be more in keeping with a risk-based approach if it read " … ML/TF risks they are, or *might* be, exposed to …" or " … ML/TF risks they are, or *could* be, exposed to …", rather than as currently " … ML/TF risks they are, or <u>would</u> be, exposed to …".

4. Paragraph 17:

In our submission, this paragraph contains an important reinforcement of the risk-based approach. This wording should remain a clear part of the final Guidelines.

5. Paragraph 18 and 20 (inter alia):

These paragraphs contain a number of references to "reputation", "media reports" and "allegations". In our submission, it would be helpful if the

wording used in paragraph 23 ("credible sources" and "credible and trustworthy source") were incorporated into the earlier paragraphs. While this may require firms to determine the credibility of sources, it is probably implied that they will do so anyway.

If incorporated, it will be clearer that not all information or allegations should be treated equally. Further, over the last decade or more, media has undergone a transformation, including the advent of social media, blogging, and independent editorial websites. Guidance may be necessary such that 'allegations' must be able to be directly attributed to a Judicial or Enforcement entity.

6. Paragraph 30:

The opening dot point of the paragraph contains a sensible and clear expression of the way in which a firm should respond to the difference between face-to-face CDD and CDD when a customer is not physically present. The final Guidelines should not, in our submission, seek to impose overly prescriptive processes on non face-to-face CDD, such as by requiring processes that attempt to mimic face-to-face CDD. To do so could undermine the benefits of going online, the collaborative economy and emerging innovative business models.[6]

The Directive has adopted a technology neutral basis in allowing reliance on "documents, data or information", and the Guidelines should not limit this without good reason or proper consideration. See also paragraph 104, where, we contend, appropriately technology neutral wording is also used in the draft Guidelines, and paragraph 118 where it is implied that with adequate safeguards, non face to face need not be higher risk.

7. Paragraph 41:

This paragraph contains important reinforcement that simplified due diligence is not an exemption from proper CDD. We support this wording remaining a clear part of the final Guidelines.

[6] Such an approach would also be consistent with the objectives of European Commission currently being explored its Consultation on Online Platforms, Cloud and Data, Liability of Intermediaries, and the Collaborative Economy. The Consultation is part of the Commission's assessment of the role of online platforms, promised in its Communications on a Digital Single Market Strategy for Europe on 6 May 2015. See http://europa.eu/rapid/press-release_IP-15-5704_en.htm

8. Paragraph 42:

This paragraph notes (*inter alia*) that customer identity cannot be verified based on information obtained from the customer, rather than an independent source.

It would be helpful if the Guidelines made clear that this exclusion applied when such information was the sole source of information provided as a means of verification of the customer.

We also note that, in the absence of other information, uploaded documents are effectively information obtained from the customer, and may lead to significant impersonation risk if relied upon as the primary source of customer verification. Typically, such uploaded documents may include passports, national ID, bank statements and birth certificates.

A number of service providers currently purport to provide Customer Due Diligence services whereby unverified documents are uploaded by a customer, and such documents are compared with a photograph taken by the customer. Such services in our view do not currently conform nor will they ever with the independent verification requirements, and they provide a means for significant impersonation risk.

We do distinguish this by noting that unverified customer uploaded documents may support other information, documents or data where such is verified by independent means, or where the uploaded documents may be validated and verified by independent means linked to their issuing source. (eg an online passport validity check per the Australian DVS[7]).

As a minimum, uploaded identity documents should be subject to Machine Readable Zone (MZR) checks together with a check against a lost or stolen database. These may be on a risk based approach in lieu of, or in addition to, an issuer validity check.

9. Paragraph 121

The ESA has helpfully provided examples of the types of monitoring systems firms should put in place, which include:

[7] http://www.dvs.gov.au/Pages/default.aspx

• transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of the product in a way it was not designed for;

• systems that identify discrepancies between submitted and detected information – for example, between submitted country of origin information and the electronically detected IP address;

• systems that compare data submitted to data held on other business relationships, and that can identify patterns such as the same funding instrument or same contact details;

• systems that identify whether the product is used with merchants dealing in goods and services that are associated with increased financial crime risk.

iSignthis offers a unified payment processing, customer due diligence and transaction monitoring service that includes the above requirements.

iSignthis offers a means to identify persons remotely by processing multiple data sources in order to dynamically compare the information between the various sources and seek either consistency between the data, or, identify anomalies that are presented to the Money Laundering Responsible Officer.

The advantage to the iSignthis process is that it instigates a Strong Customer Authentication process on electronic payment instruments such as credit cards, debit cards, credit transfers, and direct debits, and uses the data associated with the verified payment instrument as the core reference data against which other data is compared.

Data and metadata elements of the verified payment instrument and an associated payment transaction executed via the secure payments network, are then linked to data and metadata elements of the telecommunications network, the internet, device data, public source databases and end user provided information, and unique attributes identified for each end user, above and beyond the usual name, address and civil registration number requirements.

In effect, the iSignthis process adapts and improves the accepted manual practices, and machine executes them in real time in a repeatable and traceable manner, using the most up to date sources of data.

The iSignthis process also captures and analyses the metadata associated with transmission of the core data, whereby the underlying metadata is also analysed for consistency against the data and other metadata elements. Such metadata may include IP address, internet service provider, proxy network, TOR detection, browser settings, GPS data, mobile network metadata, device characteristics and payment network metadata.

These metadata sources are collected independent of the customer. Where the customer attempts to disguise any metadata, the iSignthis process detects this and factors accordingly, with notifications to the MLRO.

The iSignthis service is able to link separate payment instruments to a person's real world identity in real time, by associating historic data and metadata attributes automatically.

The iSignthis capability implements real-time risk and transaction analysis taking into account (a) the full transaction history of that customer per AML operator (and across multiple operators utilising iSignthis) to evaluate the latter's typical spending and behaviour patterns, (b) information about the customer device used (e.g. IP address, model, operating system, language preferences) and where applicable (c) a detailed risk profile of the payee (e.g. types of service provided, transaction history) and the payees device (where applicable).

10. Paragraph 106 and paragraph 122:

The wording for measures required of retail banks and electronic money issuers in conducting EDD is different, but the substance appears to be the same for many of the measures.

It would be helpful to firms and competent authorities if steps that are the same were worded identically. Applying, different wordings typically leads the reader (and the hence firms and competent authorites) to the conclusion that different actions are required.

For example, the identity and verification requirements are worded differently, but it is not apparent that any substantial difference in required

action is intended. Similarly the CDD requirements on source of funds and nature of business are set out differently, but without a clear difference in required activity.

We content that this will lead to differences in responses not supported by differences in risk or underlying business activity.

11. Paragraph 124:

The paragraph provides that SDD in low risk circumstances may be concluded by verification "… on the basis of a payment drawn on an account in the … name of the customer with a EEA-regulated credit institution." In our submission, it would be helpful to firms and competent authorities if the paragraph were amended to make it expressly clear this is only permitted where such an account has been subject to proper CDD for that customer.

N J Karantzis, LLM
CEO & Attorney

C Muir, LLB
COO & General Counsel