"Your Identity Secured, your payments made Safe"

16 September 2016

AML/CFT consultation team
Ministry of Justice
SX10088
Wellington
New Zealand

aml@justice.govt.nz

Dear Sir/Madam,

This submission responds to the *Ministry of Justice consultation paper on Phase Two of the AML/CFT Act* of August 2016.

iSignthis thanks the Ministry for the opportunity to comment on the consultation paper.

This submission responds to select aspects and questions raised in the consultation paper upon which iSignthis believes it has a contribution to make.

iSignthis

This submission is provided by iSignthis Ltd, a company listed on the Australian Stock Exchange (code ISX), and currently valued at around AUD$200M. iSignthis operates in a number of jurisdictions, principally in Europe currently, but also North America, Australia and the developed markets in Asia. iSignthis anticipates shortly commencing operations in New Zealand.

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 an evidentiary basis for compliance to meet customer identification requirements for AML/CFT 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.

Our processes are able to provide AML/CFT obligated entities with compliance KYC services in jurisdictions implementing the Financial Action Task Force recommendations

on customer identification, such as those indicated above, and we believe under the New Zealand *Anti-Money Laundering and Countering the Financing of Terrorism Act 2009* (**AML/CFT Act)**.

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 conforms with the EU Data Protection Directive, 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 European Banking Authority's 'Recommendation for the Security of Internet Payments'[1].

Approach of our submission

iSignthis has significant experience in retail facing AML/CFT obligated sectors, such as online gaming and gambling. Our response is more focused on the proposed general enhancements to the AML/CFT regime and the specific changes to the gambling provisions. However, we believe our submissions on technological neutrality are applicable to the proposed changes to other sectors.

Given close economic and other ties, and the current similarity of AML/CFT regulations, comparisons are drawn between the approach proposed in the consultation paper and the approach in Australia. Reference is also made to the European approach, including the Fourth AML Directive as an example of global standards. Given New Zealand's membership of the FATF, reference is made to the 40+9 Recommendations of FATF.

Technological Neutrality

iSignthis advocates for maintaining a technologically neutral approach to achieving the aims of AML/CFT goals. We note New Zealand has embraced this approach in the existing AML/CFT Act which, for example through section 13, provides for verification of identity on the basis of 'documents, data, or information'.

The growth in online services, emerging technologies, and a growing individual 'digital footprint' raises new challenges in performing satisfactory customer due diligence. Numerous jurisdictions have taken the broad technologically neutral approach to the sources of identity verification adopted by New Zealand and extended it to embrace reliable, alternative means of identity verification.

We support an approach to Phase Two implementation which embraces technological neutrality in its drafting, allowing reporting entities to adapt to changing business environments and rapidly evolving technologies.

[1] EBA-GL-2014-12 (Guidelines on the *security* of *internet payments*)

Lawyers, Accountants, Real Estate and High-Value Goods

iSignthis has no industry specific submissions to make on these sectors.

At a general level, we submit that the timing of identification, and in particular the verification of identity, should not be specified with such rigidity that a risk based approach is effectively eliminated.

For example, specifying that verification must be completed prior to a lawyer beginning to take instructions from their client could unnecessarily inhibit both the reasonable formation of a business relationship and commencing urgent representation, without significantly preventing money-laundering or the financing of terrorism. Similar points can be made about share trading as a comparator, which we address below.

Provided that identity verification is completed as soon as practicable, and before the final execution of a transaction to the irrevocable benefit of a customer, we submit that money-laundering and financing of terrorism risk can be adequately managed. Naturally, where there is actual suspicion of money laundering for the financing of terrorism, delayed identification should not apply.

Multiple jurisdictions provide a specific dispensation allowing a specified time between opening an account, including receiving money from a customer, and completion of identity verification in share trading or gambling.

For example, Cyprus and Hong Kong permit this on opening of share trading accounts. This is permitted to allow for the need for urgent trading, combined with an acceptance of a generally low level of money-laundering or financing of terrorism risk. Both regimes have provisions to prevent the customer gaining the benefit of the trading if identity verification cannot be completed within the allowed time.

This can be found in *Section 4.7 Timing of identification and verification of identity* of the Hong Kong Securities and Futures Commission *Guideline on the Anti-Money Laundering and Counter-Terrorism Financing*[2], and in particular in paragraphs 4.7.4 and 4.7.5.

We can also refer the Ministry to Circular C143[3] of the Cyprus Securities and Exchange Commission, altering its Guidance to allow a delay in similar circumstances.

Gambling Sector

Based on significantly greater specific industry experience in implementing AML/CFT identity verification systems, we have made more detailed submissions on proposed changes to gambling sector coverage.

Questions

[2] http://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guideline-on-anti-money-laundering-and-counter-terrorist-financing/Guideline%20on%20Anti-Money%20Laundering%20and%20Counter-Terrorist%20Financing.pdf

[3] http://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=f3c214a9-63d3-49fd-8b77-6da6dc5e753c

1. **How should AML/CFT requirements apply to the gambling sector to help ensure the Act addresses the risks specific to it? For example, which business activities should the requirements apply to? At what stage in a business relationship should checks, assessments and suspicious transaction reports be done? Who should be responsible for doing them?**

The proposed definition of 'gambling activities' provided in the Consultation Paper is largely in conformity with the Australian approach in Section 6 Table 3 of the AML/CFT Act 2006.

The EU's 4th AML Directive[4] definition of 'providers of gambling services' in Article 3 (14) provides that a gambling service is:

> *A service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.*

The latter part of this definition provides greater clarity as to the scope of 'gambling services' than that proposed and is more accommodating of emerging technologies and non-traditional mediums of gambling.

The definition of 'gambling activities' proposed in the consultation paper could be enhanced by incorporating similar descriptive language.

Alternatively, we suggest inserting a non-exhaustive list of examples of 'gambling activities' and mediums through which they can be conducted. This would provide greater clarity as to the scope of the definition, whilst keeping it adaptable to future technologies and processes.

The timing of checks and assessments can be critical in stemming the flow of money laundering and the financing of terrorism. The standard existing approach requires a reporting entity to carry out verification of identity prior to establishing a business relationship or conducting an occasional transaction.[5]

Provision is made to allow for verification after establishment of the relationship where necessary not to interrupt the normal business practice or risks of money laundering and the financing of terrorism are low[6]. The inclusion of 'gambling activities' could easily conform to the existing framework for casinos, and non-face-to-face transactions.

An alternative method is the Australian approach which incorporates a time-delay method. Under this approach, the general rule requires identify verification prior to

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L0849&from=EN
[5] Act s 16(3)
[6] see Act s 24

business establishment. However, in special circumstances *Anti-Money Laundering and Counter-Terrorism Financing Rules*[7] allows verification of identity may be delayed by up to 90 days. Withdrawal of funds from the account is not permitted until the identity verification procedure is completed.

Responsibility for conducting the required checks, assessment and transaction reports should be the same for the entities currently under the AML/CFT framework. Reporting entities which may be captured under the proposed changes may already have business interests caught under the current framework. As such, conformity with the existing framework is desirable. We note this approach is in conformity with the EU, Australian, and FATF approaches.

2. **Should there be a threshold that would trigger AML/CFT customer due diligence and reporting requirements for cash transactions related to gambling and betting activities with customers who don't have an account with you? If so, what would be an appropriate threshold? Please tell us why.**

iSignthis has no submission to make on the limits set for cash transactions.

Supervision

Questions

1. **Do you think any of our existing sector supervisors (the Reserve Bank, the Financial Markets Authority and the Department of Internal Affairs) are appropriate agencies for the supervision of Phase Two businesses? If not, what other agencies do you think should be considered? Please tell us why.**

The multi-agency approach taken in New Zealand is common in most jurisdictions. In contrast, the Australian single supervisory approach is rare.

The Gambling Commission New Zealand would seem an obvious industry supervisor. iSignthis understand that the Gambling Commission already hears casino licensing application and appeals made by the Secretary of Internal Affairs.

Implementing Period and Costs

Questions

1. **What is the necessary lead-in period for businesses in your sector to implement measures they will need to put in place to meet their AML/CFT obligations?**

[7] Rule 10.4

2. **Where possible, please tell us how you calculated how long it will take to develop and put in place AML/CFT requirements.**

iSignthis agrees a four-year timeframe for implementation is unnecessarily lengthy.

We submit that a lead-in period of 12 months should be sufficient in the absence of specific evidence from industry participants. This period from final passage of the Phase Two coverage should give reporting entities time to include appropriate changes to their processes in their annual planning and budgeting.

We note there are existing tools available on the market, such as the patented iSignthis process, which can be readily be incorporated into a reporting entity's procedures to meet their AML/CFT obligations.

Reliance on Third-Parties

Question

1. **Are the existing provisions that allow reporting entities to rely on third parties to meet their AML/CFT obligations sufficient and appropriate? If not, what changes should be made?**

The provisions of the current AML/CFT Act dealing with a reporting entity's reliance on third parties to achieve their AML/CFT obligations are in essence the same as those in the Australian AML/CTF Act 2006. FATF Recommendation 17 provides much the same.

Article 25 of the 4th EU Anti-Money Laundering Directive is simpler and only contains one significant obligation, being that in such a circumstance the originally obligated entity remains liable for the identification.

We submit that it is appropriate to leave ultimate responsibility for identity verification with the reporting entity.

However, some level of assurance should be required of third parties upon whom reliance is placed. For example, if third parties are not regulated by the provisions of AML/CFT in any FATF member country, then they could be subject to the customer due diligence process prescribed under the Act. The data protection policy, processes and storage should be subject to external audit and compliance testing. This could come in the form of privacy compliance audit and testing leading to certification to a standard such as ISO27001.

Conclusion

iSignthis thanks the Ministry for the opportunity to provide a submission.

We consent to publication of our submission in conformity with the Ministry's ordinary procedures.

Yours faithfully,

N J Karantzis,
B.E. LL.M M.Ent FIEAust
Managing Director

C Muir, LL.B
General Counsel