International Centre™
FOR MISSING & EXPLOITED CHILDREN
AUSTRALIA

The Committee Secretary
Review of AML/CTF Regime
Senate Legal and Constitutional Affairs Committee
P.O. Box 6100
Parliament House
Canberra, A.C.T 2600, Australia

25 August 2021

Dear Committee Secretary,

ICMEC Australia is pleased to make this submission on behalf of vulnerable people whose lives, whether they be within Australia or offshore, are being harmed by the **online sexual exploitation of children.**

The problem is growing. In 2020, the Australian Centre to Counter Child Exploitation's (ACCCE) Child Protection Triage Unit received more **than 21,000 reports of online child sexual exploitation**. In the past year alone, the ACCCE has intercepted and examined more than 250,000 child abuse material files. The Australian Federal Police charged a total of 191 people with 1847 alleged child abuse-related offences in 2020.[1]

Behind the child sexual exploitation materials (CSEM) are offenders from Australia and overseas who inflict misery on children by creating and distributing images, videos and livestreams; often on a commercial basis. The offences are largely reliant on transfers of funds among individuals, and between individuals and businesses. Financial institutions in Australia; including banks, money remitters, and other industry partners, are motivated to prevent their systems from being used to enable such online sexual exploitation of children (OSEC). All are keen to cooperate and collaborate to detect and prevent such crimes now and in the future.

Pertinent Aspects of What We Do

ICMEC is an international organisation focused on the protection of children from exploitation and abduction. Over the past twelve years, our Asia-Pacific Managing Director has brought together financial institutions, technology companies, regulators, and law enforcement representatives to the APAC Financial Coalition Australia Working Group to address issues and opportunities to protect children from exploitation and abduction. Members of this coalition have recently been focused on how they can work together through data sharing to better identify when their payment systems are being used for OSEC and how to prevent this from happening in future. ICMEC Australia has now been established to support these initiatives.

Over time, our stakeholder engagements have provided us with insights into the impact of the current AML/CTF regime on our joint efforts to combat the exploitation of children. It is from this perspective, and with our mission to protect more children at the fore, that we respectfully make our recommendations.

Summary

We seek to bring together stakeholders to share data and insights that, once applied serve to better protect children within and outside Australia from exploitation. However, currently the Australian legislative framework for AML/CTF imposes a number of constraints to our work. As such our recommendations relate primarily to (a)(ii) of the Terms of Reference, which assesses how the Australian Transaction Reports and Analysis Centre (AUSTRAC) identifies emerging challenges based on the reporting it receives from regulated entities.

[1] Australian Centre to Counter Child Exploitation, 'ACCCE Statistics 2020'.

	Constraint	Recommendation
1	In its preamble, the AML/CTF Act does not specifically define "other serious crime". While sub-section 41(f)(iii) of the AML/CTF broadly requires reporting of suspicions relevant to the investigation of any offence against a law of the Commonwealth or of a State or Territory, we believe that the law should specifically include crimes against children.	**Define 'serious crimes' in the Act and ensure these crimes include crimes against children**. The Act should specify crimes that endanger the safety of persons, especially children, given they are the most vulnerable in our society. Once defined these 'serious crimes' should be prioritised in terms of both how they are reported to AUSTRAC, as well as how they are investigated and prosecuted. We believe such a change would serve to increase the reporting of suspicions of OSEC by regulated entities, and would enhance their training and procedures that are directed towards combatting OSEC.
2	AUSTRAC is creating valuable data assets such as its registry information. An example of the registry information is a list of digital currency exchanges. This registration information is not always made available to other reporting entities that are regulated by AUSTRAC (a registration of remitters *has* been available).	**AUSTRAC to provide access to registry information for reporting entities.** Enabling access to registration data for reporting entities would assist with the detection of non-compliance and gaps in reporting by un-registered businesses. As an example, sharing a registry of cryptocurrency vendors may assist reporting entities to identify suspicions by providing an additional data point on an individual's behaviour. Appropriate safeguards may be required to ensure registry information is not used for anti-competitive behaviour or promotes 'de-banking' by the reporting entities.
3	Reporting entities share ICMEC's motivation to improve the value of suspicious matter reports (SMRs) to the regulator and law enforcement authorities as they act against criminals. Currently reporting entities lack feedback from the regulator and law enforcement. This is in part because of the secrecy provisions in the Act. In addition, concerns around tipping off limit their ability to share data that would help improve their ability to identify suspicious measures in the future.	**Clarify secrecy provisions and enable data sharing**. Emphasise in the Act that the tipping off offence (at section 123) relates to actions that lead to informing the person or entity which is the subject of suspicion. Empower some sharing of relevant information on possible OSEC offences amongst reporting entities, similar to that which exists in the USA Patriot Act s.314(b). It would also be helpful to introduce the requirement for a feedback mechanism where AUSTRAC and law enforcement can provide information in response to SMRs to continuously improve the quality of reporting. This feedback is sought by reporting entities to enable statistically driven approaches to aid future detection.
4	Australia's Privacy Act is a major constraint on data analysis with respect to persons. Data owners are unwilling to share even de-identified records at scale for use in developing predictive capability across data from multiple financial institutions.	**Empower reporting entities to use and share de-identified data.** By sharing, in a secure and well-governed manner, data can be applied using modern data science to develop multi-variate predictive models (and create assets and statistical applications), to assist in identifying, investigating, and prosecuting offenders.
5	Presently high-risk customers, or those for which suspicions have been formed, have a likelihood of being 'de-banked' based on a suspicion alone, given there is no subsequent feedback from AUSTRAC or law enforcement as to whether an offence has actually occurred.	**Create a protocol on de-banking that can be applied across the industry to inform action**. This would assist the financial institutions in systemising and monitoring their actions, help to protect their customers from unnecessary exclusion from the banking system, and assist those seeking to prosecute offenders. The protocol would ideally be developed by industry, with input from a broader stakeholder group.

The Review as an Opportunity to Better Protect Children

The financial footprint of crimes against children are hidden in financial transactions and, while the efforts of AUSTRAC and its reporting entities are commendable in the context of our mission, we believe that there remain significant opportunities for improvement. This should build on the existing work of entities like ACCCE and the Australian Federal Police, who have made combatting child exploitation a priority. This has only become more critical due to the COVID-19 pandemic and its economic impact.

No element of our recommendations should be read as critical of the regulator or its reporting entities. We have observed nothing but cooperation and support for the protection of children through our collective work to disrupt its financial underpinnings.

In line with the Terms of Reference for the review, we believe that the AML/CTF Act (in conjunction with other Acts), has some unintended and constraining impacts on collaboration and thereby it introduces systemic weaknesses. These shortfalls also curtail the ability of reporting entities to collectively address weaknesses that can emerge over time.

Context: Investigating Cases or Innovating Using Modern Data Science

Financial institutions use a combination of technical and manual means to identify possible transactional and other evidence of OSEC. They use sophisticated filtering technologies to identify possible suspicious events and circumstances and then staff members examine the results prior to issuing any suspicious matter report. This manual element is highly resource intensive, but crucial to limiting the number of unhelpful SMRs provided to AUSTRAC.

Modern statistical techniques, such as machine learning, could improve the ability of financial institutions to reduce false positives, and to identify suspicious activities that would otherwise fall through the gaps. However, because of constraints in the amount of data they have, as well as resource limitations, only a few of our largest financial institutions can effectively apply these modern techniques. In addition, data from other industries, if it could be made available, would significantly enhance these efforts, as additional pertinent data points increase accuracy and reduce uncertainties.

ICMEC is working to increase collaboration between the financial industry and other relevant parties, to extend the use of these methods across the sector. Our partners seek to share information about their methodologies and to share data which, combined with data analytics, could identify patterns of behaviour that indicate involvement in OSEC, which could be applied across the whole industry. Their ability to do this is currently constrained by existing legislation.

Recommendations on the AML/CTF Act

Section 3 - Objects of the AML/CTF Act

Section 3(1) of the Act refers to both "other serious financial crime" and "other serious crimes". The emphasis in this preamble is placed on money laundering and terrorism financing, without defining the other serious crimes that leave a financial footprint, such as the abuse and exploitation of children. This could unintentionally diminish other crime types which are a threat to life for vulnerable individuals.

We recommend that section 3(1) be amended to provide context for "other serious crime", or a definition be added at section 5 of the AML/CTF Act, to include crimes against children or those which have a risk to people's life or safety. This will likely increase both reporting entities' inclusion of OSEC in their risk assessment, as well enhancing their training to combat OSEC. A similar effect, in enhancing compliance has been seen with obligations in preventing modern slavery and human trafficking.[2]

We note that sub-section 41(f)(iii) of the AML/CTF Act broadly requires reporting of suspicions relevant to the investigation of any offence against a law of the Commonwealth or of a State or Territory. Once defined these "serious crimes" should be prioritised by AUSTRAC and law enforcement in terms of their investigation and prosecution.

Those working to prevent OSEC crime (within law enforcement, government, financial institutions) all note that transactions and money transfers related to child exploitation are generally of a lower monetary value than other crime types (such as drug trafficking and money laundering). As a result, OSEC crime is accordingly more difficult to detect, increasing the importance of the best possible legislation to encourage detection, reporting and disruption of these offenders.

[2] Modern Slavery Act 2018 (Cth); Divisions 270 and 271 of the Commonwealth Criminal Code Act 1995 (Criminal Code) (Cth).

Section 76B of the AML/CTF Act - Register of Digital Currency Exchanges and Reporting Entities

Part 6A of the AML/CTF Act relates to digital currency exchanges. Specifically, section 76B refers to the register of digital currency exchanges which AUSTRAC maintains, alongside other registry information. The information contained in the digital currency exchange register is an example of the type of registry information that would be useful to the reporting entities, as it would enable greater tracing and reporting of suspicions with respect to cryptocurrency.

At present the traditional banking system has mechanisms to aid transparency using platforms such as SWIFT that show instruction and payment chains. However, cryptocurrency has yet to establish these industry norms, and it is these gaps which can be exploited by criminals.

We recommend that a register of all reporting entities (including digital currency exchanges) be made accessible to reporting entities. This would improve the ability of financial institutions to assess transaction dates, times, amounts and frequencies, in evaluating suspicious transactions where crypto currencies are involved. We appreciate the probable need for protections to be in place regarding the use of the registers of reporting entities, particularly to avoid anti-competitive behaviour or a negative impact (e.g., on an investigation) that could arise from a high-risk customer being 'de-banked'. Please also see our section below titled "Customers at Risk of Being De-banked".

Part 11 of the AML/CTF - Secrecy and Access

The need for secrecy and to avoid tipping off offenders who may come under investigation (addressed at section 123 of the AML/CTF Act) is understood and paramount. However, concerns about the secrecy provisions serve to curtail collaborative efforts to improve the efficacy of work on OSEC crimes. Institutions are limited in their ability to share intelligence data with each other, or with a trusted third party, and so progress is restricted.

For this reason, we recommend that the tipping off provisions at section 123 of the AML/CTF Act, be amended to emphasise that tipping off refers to actions that specifically lead to informing the person or entity which is the subject of suspicion.

We note the success of the section 314(b) of the USA Patriot Act, which permits financial institutions, upon providing notice to the US Department of the Treasury, to share information with one another to identify and report to the federal government activities that may involve money laundering or terrorist activity. These safe harbour provisions, which the US Financial Crimes Enforcement Network (FinCEN) strongly encourages financial institutions to participate in, has facilitated a more comprehensive and accurate picture of a customer's activities.[3] Adopting a similar approach in Australia would have significant advantages in both preventing and investigating OSEC.

In addition, if there were a requirement for a feedback mechanism whereby AUSTRAC and law enforcement could provide information back to reporting entities in response to SMRs, this should result in a significant improvement to these reports. Such feedback does not need to be immediate as we appreciate that investigation and prosecution of crimes may take several months, if not years.

Customers at Risk of Being 'De-banked'

Presently there is a reputational risk to financial institutions and an increased cost of monitoring associated with retaining high-risk customers or those for whom suspicions have been formed. This results in the likelihood of their being de-banked. The lack of subsequent feedback from AUSTRAC or law enforcement as to whether criminal conduct has actually occurred, increases the probability of de-banking. In addition, there is a risk that suspicion alone can lead to an individual customer having their relationship terminated. This creates a greater likelihood of tipping off from this termination (OSEC crime often has a network dimension), as well as a potential civil claim by the customer against the reporting entity, as no substantive reason can be provided for the closure of accounts.

Reporting entities are concerned, under their obligations under the AML/CTF Act in relation to risk management, that the action they take on de-banking high risk customers be appropriate. In its joint

[3] US Financial Crimes Enforcement Network (FinCEN), Section 314(b) Fact Sheet, (December 2020).

submission (with the Department of Home Affairs) to the Senate Select Committee on Australia as a Technology and Financial Centre June 2021, AUSTRAC noted that the decision to de-bank a customer belongs to individual financial institutions, and that the AML/CTF Act does not cover the need to continue to provide services to customers. This appears to place responsibility for de-banking firmly with financial institutions, but they are taking this responsibility in a context of a social obligation to provide access to the financial system, a desire to work effectively with law enforcement and the need to meet their own legislative and regulatory obligations.

To assist with minimising inappropriate de-banking, we recommend the creation of a protocol for financial institutions that can be used to guide decisions, manage risk, and consider consequences when a reporting entity considers de-banking. Ideally, development of such a protocol would be industry-led, with input from appropriate government and non-government stakeholders. This guidance should also align with Chapter 75 of the AML/CTF Rules which governs the situation where law enforcement is investigating an individual at risk of being de-banked.

Recommendations for AML/CTF in the context of other Acts

The Attorney General's Department is also currently reviewing Australia's *Privacy Act 1988* (Cth). Its embedded principles and its emphasis around protecting personal information have led to organisations acting very conservatively around sharing any data that pertains to an individual, even if de-identified and with a focus on stopping financial crime. This allows criminals who are sufficiently astute to evade current alert systems by spreading their activity across multiple institutions.

Data analytics and machine learning can help to improve the ability of industry to identify and prevent the financial system being used to support OSEC activities. For this to be effective, it is crucial that de-identified data be shared at scale. ICMEC Australia is committed to supporting the ability of Australia's financial institutions to be able to do this.

Importantly the Monetary Authority of Singapore (MAS) has acknowledged the need for information sharing and data analytics in efforts around AML.[4] However, importantly Loo Siew Yee, Assistant Managing Director of Policy, Payments and Financial Crime at MAS states:

> Sharing of information needs to take place within a robust legal and technical framework, to maximise its effectiveness and address legitimate concerns about the loss of privacy and misuse."[5]

We recommend that the AML/CTF Act be amended to allow reporting entities to collaborate using data at a person or customer level, provided that the data is de-identified (only re-identifiable by the reporting entity that owns it), and then supplied and used under secure conditions. This would clarify how data can be applied to improve identification of criminal activity, while taking steps to protect the data subjects.

Our Privacy Act requires clarification to enable the use of large-scale, de-identified data to help combat crime. As a nation, we are comfortable to set aside privacy for those under investigation but cannot use data at scale and apply modern data techniques to help identify suspects for the next investigation. Julie Inman Grant, the Australian eSafety Commissioner, has spoken passionately about this tension and has identified that we are yet to strike the correct balance with respect to the safety of children.[6] Although the OAIC has set out some guidance on de-identification, most organisations are unwilling to proceed, without further regulatory certainty.

Thank you for your review and consideration of these recommendations.

Bindu Sharma
Director - ICMEC Australia

Paul McCarney
Executive Chairman – ICMEC Australia

[4] Yixiang Zeng, Regulatory Intelligence News 'Singaporean central bank to launch tech-driven platform in AML/CFT push', published 11 August 2021.
[5] Ibid.
[6] Julie Inman Grant, eSafety Commissioner, 'Protection of children should always trump protection of privacy', published 6 November 2020.