PricewaterhouseCoopers (Australia)

Assistance and Access Bill 2018: Australia's new motion to enable decryption of encryption

Cabrera & Company (Philippines)

Tracking down dirty money: AMLC Guidelines on the Digitization of Customer Records

PwC International Business Reorganisations Network – Monthly Legal Update

Edition 11, November 2018

Contents

Welcome

Welcome to the eleventh edition of the PwC International Business Reorganisations (**IBR**) Network Monthly Legal Update for 2018.

The PwC IBR Network provides legal services to assist multinational organisations with their cross-border reorganisations. We focus on post-deal integration, pre-transaction separation and carve outs, single entity projects, and legal entity rationalisation and simplification as well as general business and corporate and commercial structuring.

Each month our global legal network brings you insights and updates on key legal issues multinational organisations.

We hope that you will find this publication helpful, and we look forward to hearing from you.

In this issue

In our November 2018 issue:

- PricewaterhouseCoopers (Australia) reports on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*; and
- Cabrera & Company (Philippines) examines the Anti-Money Laundering Council's Guidelines on Digitization of Customer Records.

Contact us

For your global contact and more information on PwC's IBR services, please contact:

Richard Edmundson

*Special Legal Consultant**

Managing Partner, ILC Legal, LLP

+1 (202) 312-0877

richard.edmundson@ilclegal.com

** Mr. Edmundson is admitted as a solicitor in England and Wales and is licensed to practice in the District of Columbia as a Special Legal Consultant.*

PricewaterhouseCoopers (Australia) – Assistance and Access Bill 2018: Australia's new motion to enable decryption of encryption

At a glance

On 14 August 2018, the Federal Government released its long-awaited *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (**Bill**). The Bill seeks to provide Australian law enforcement and national security agencies with broader powers to access encrypted data stored in communication devices. The Government's concern is that the growing use of encryption in these devices has significantly reduced the ability of law enforcement and security agencies to carry out investigations.

The Bill is intended to align Australia's laws with those of the UK and the US which have provided law enforcement agencies with similarly broader powers to require assistance from industry to access user data to tackle terrorism and national security related crime and issues.

Public consultation on the Bill is open until 10 September 2018.

In detail

Background to the Bill

The Explanatory Document to the Bill states that 95 per cent of the Australian Security Intelligence Organisation's (**ASIO**) most dangerous counter-terrorism targets use encrypted communications. The Minister for Law Enforcement and Cyber Security, Angus Taylor, has also commented that in the last 12 months, 200 investigations of serious crimes were impeded due to inability to access and decrypt encrypted data.

Through this Bill, the Government has clearly expressed desire to overcome technical barriers to enable its law enforcement and security agencies access to what it views as key sources of information crucial to public safety and security.

An overview of the key proposed changes

1. Industry assistance framework

A new Part 15 will be inserted into the *Telecommunications Act 1997* (Cth) to create an industry assistance framework enabling certain government agencies access to encrypted data and devices.

This framework includes:

a **Technical assistance request**: ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate and interception agencies **can require voluntary assistance** from designated communications providers to aid in the performance of their core functions related to enforcement of criminal law and protecting national security.

b **Technical assistance notice**: where a designated communications provider is unwilling to provide voluntary assistance, the Director-General of Security or a head of an interception **agency can require assistance that is reasonable, proportionate, practicable and technically feasible**, if the provider is already capable of providing that assistance. This includes situations where there is no end-to-end encryption and the provider holds the encryption key.

c **Technical capability notice**: where a designated communications provider is not capable of providing assistance, the Attorney-General can require the provider to build a new capability in order to provide that assistance. Any request must be **reasonable, proportionate, practicable and technically feasible**, and the provider must have been consulted before the issue of a technical capability notice.

2. New computer access warrants

Proposed amendments to the *Surveillance Devices Act 2004* (Cth) will create a new class of computer access warrants allowing law enforcement agencies to search and access content on electronic devices. The powers included in a computer access warrant are broad and may include:

a entering premises and removing a computer from premises to execute a warrant;

b intercepting data to execute a warrant (the use of intercept data requires an additional interception warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth) – this is waived for ASIO under new powers, unless it is using the information for its own purposes); and

c concealing access (while the warrant is in force, within 28 days of it ceasing, or the earliest time at which it is reasonably practicable).

While a computer access warrant is in force, a law enforcement officer may apply to a judge or Administrative Appeals Tribunal member for an order compelling reasonable and necessary assistance from a person with knowledge of the device.

3. Enhanced search warrants and ASIO assistance powers

Schedule 3 of the Bill will amend the *Crimes Act 1914* (Cth) to allow law enforcement agencies to remotely collect evidence from electronic devices under an overt warrant instead of having to physically go onto the premises, as required under the current law. It will also introduce a new definition of 'account-based data' which will allow agencies to access data from online accounts associated with those devices (e.g. Facebook or email).

Schedule 3 will also amend section 3LA of the *Crimes Act 1914* (Cth) to enable law enforcement agencies to apply for court orders to compel certain individuals to assist in giving access to devices found both within the warrant premise and during an in-person search. Schedule 4 of the Bill will amend the *Customs Act 1901* (Cth) by providing the Australian Border Force (**ABF**) with the power to apply for a search warrant to use computers or other data storage devices to access data in order to determine whether the relevant data is evidential material.

Finally, Schedule 5 of the Bill will amend the *Australian Security Intelligence Organisation Act 1979* (Cth) to provide greater assistance powers to ASIO in the performance of its functions. For example, section 21A(1) provides a protection from civil liability for a person that voluntarily assists ASIO following a request made by the Director-General, subject to certain limitations.

Consultation

There is much to consider in this Bill, and it will take time to fully comprehend the extent of the Bill's wide ranging effects.

Public consultation on the Bill is open until 10 September 2018 and the Bill can be viewed **here**.

PricewaterhouseCoopers (Australia)

Assistance and Access Bill 2018: Australia's new motion to enable decryption of encryption

Cabrera & Company (Philippines)

Tracking down dirty money: AMLC Guidelines on the Digitization of Customer Records

Who to contact

For more information, please contact:

Adrian Chotar

Partner, Sydney

+61 2 8266 1320

adrian.chotar@pwc.com

Hugo Chan

Associate, Sydney

+61 2 8266 5721

hugo.chan@pwc.com

Cabrera & Company (Philippines) – Tracking down dirty money: AMLC Guidelines on the Digitization of Customer Records

At a glance

The Anti-Money Laundering Council (**AMLC**) is vested with the authority to implement measures as may be necessary and justified to counteract money laundering.

In its bid to further improve efficiency in tracking down dirty money deals, it adopted AMLC Regulatory Issuance (ARI) A,B and C, No. 2, Series of 2018 or the Guidelines on Digitization of Customer Records (**DIGICUR Guidelines**). It took effect 13 October 2018.

DIGICUR Guidelines requires Covered Persons to digitize all customer records within six (6) months from its effectivity, and store the digitized records in a central database. It, likewise, mandates covered persons to update its Money Laundering and Financing Terrorism Prevention Program.

Non-compliance with the Guidelines shall subject the covered person to administrative sanctions and penalties and shall be considered grave violations.

In detail

The AMLC and its purpose

The AMLC was created pursuant to Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001" (**AMLA**), to protect the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity.

Money laundering

AMLA is a special law that penalizes Money Laundering. The Supreme Court has defined Money Laundering Offense as "any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources."

Under AMLA, money laundering may be committed through:

a knowingly transacting or attempting to transact any monetary instrument or property which represents, involves or relates to the proceeds of an unlawful activity;

b knowingly performing or failing to perform an act in relation to any monetary instrument or property involving the proceeds of any unlawful activity as a result of which he facilitated the offense of money laundering; and

c knowingly failing to disclose and file with the AMLC any monetary instrument/property required to be disclosed and filed, among others.

Money laundering allows criminals to enjoy the proceeds of their illegal activities through putting layers of financial activities enabling them to sanitize their money trail and legitimize their dirty money. To curb this criminal activity, Covered Persons under AMLA are required to report to AMLC any covered or suspicious transactions.

Covered Persons

Covered Persons may be divided into groups:

a persons supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC) and Insurance Commission (IC);

b Designated Non-Financial Businesses and Professions (DNFBPs); and

c casinos, including internet and ship-based casinos, operating within the territorial jurisdiction of the Philippines and authorized to engage in gaming operations.

AMLC issued, last May 2018, "Guidelines for DNFBPs". It provides that lawyers and accountants who provide services such as:

a managing of client money, securities or other assets;

b management of bank, savings, securities or accounts;

c organization of contributions for the creation, operation or management of companies; and

d creation, operation or management of juridical persons or arrangements, and buying and selling business entities, are considered covered persons, and must therefore report covered and suspicious transactions to the AMLC. Notwithstanding the requirement, the Guidelines for DNFBP excludes disclosure of information that would compromise client confidences or attorney-client privilege.

Covered transactions

Generally, covered transactions involve transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five hundred thousand pesos (P500,000.00) within one (1) banking day.

For Casinos, a single casino cash transaction involving an amount in excess of Five million pesos (P5,000,000.00) or its equivalent in any other currency shall be considered as a covered transaction.

Suspicious transactions

These are transactions with covered institutions, regardless of the amounts involved which has no underlying legal or trade obligation, purpose or economic justification; or the client is not properly identified; or the amount involved is not commensurate with the business or financial capacity of the client, among others.

DIGICUR Guidelines

Under AMLA, Covered Persons are required to prepare and maintain documentation, in accordance with the client identification requirements, on their customer accounts, relationships and transactions such that any account, relationship or transaction can be so reconstructed as to enable the AMLC, and/or the courts to establish an audit trail for money laundering.

For efficiency in conducting the investigations, the AMLC issued Regulatory Issuance (ARI) A,B and C, No. 2, Series of 2018 or the DIGICUR Guidelines, which took effect last 13 October 2018. Its adoption is envisioned as a step to address the issue of extracting above mentioned data in a timely manner.

With centralized digitized records in place, covered persons are expected to become effective partners in facilitating the prompt transmission of data in the manner and quality that would assist AMLC in its financial investigations and institution of legal actions.

Digitization of Customer Records

Customer Records are those obtained by the covered persons to establish the true and full identity of customers in accordance with their Customer Due Diligence policies and procedures (i.e. customer information files and account transaction histories or statement of accounts, whether in Philippine pesos or other currency).

With the implementation of DIGICUR Guidelines, the covered person's compliance officer or other duly authorized officers are expected to retrieve customer records quickly, and, upon request or order, upload these to the AMLC's portal, without having to request said records from branches/offices on a per need basis.

Development and Access to Central Data Base

Under DIGICUR Guidelines, covered persons are now required to develop a central database of customer records to be maintained in their respective head offices or main branches of foreign banks operating in the Philippines, and authorize the compliance officer, or any duly authorized officer, or representative, to have direct, immediate, and unimpeded access to database.

Updating of Money Laundering and Financing Terrorism Prevention Program

Covered persons are also required to update its Money Laundering and Financing of Terrorism Prevention Program (**MLPP**) to reflect the requirements under the DIGICUR Guidelines. The updated MLPP must provide and establish appropriate controls to ensure the confidentiality of the data base as well as prevent tipping-off.

MLPP shall be duly approved by its Board of Directors, partners or owners.

Period to comply

Covered Persons are required to update their MLPP and start digitization of all customer records within six (6) months from the time of DIGICUR effectivity (i.e. 13 April 2019).

While digitization of all existing customer records and establishing the central data base that is accessible to the officers of covered persons, should be completed within two (2) years from the expiration of the six (6) month period (i.e. 13 April 2021).

Digitization includes those pertaining to accounts existing prior to the implementation period of DIGICUR Guidelines but excluding customer records of closed accounts beyond the five (5) year record-keeping requirement of the AMLA.

Submission of digitized customer records to AMLC

Whenever requested, or directed to submit customer records, the compliance officer, or any duly authorized officer, or representative, shall submit the customer records extracted from the covered person's central database to the AMLC's File Transfer and Reporting Facility (FTRF), using their respective log-on credentials, or in such other mode as the AMLC may prescribe.

Sanctions and penalties

Non-compliance with the DIGICUR Guidelines shall subject the covered person to administrative sanctions and penalties provided under the AMLC's Rules on Imposition of Administrative Sanctions, and shall be considered grave violation.

Disclosure of any information in relation to a covered or suspicious transaction report, including the financial investigations initiated by the AMLCC as a result of its analysis shall constitute a criminal offense under the provisions of the AMLA.

Who to contact

For more information, please contact:

Harold S. Ocampo
Partner, Makati City
+63 2 845 2728
harold.s.ocampo@ph.pwc.com

PricewaterhouseCoopers (Australia)

Assistance and Access Bill 2018: Australia's new motion to enable decryption of encryption

Cabrera & Company (Philippines)

Tracking down dirty money: AMLC Guidelines on the Digitization of Customer Records

Kyra Kae B. Diola

Makati City

+63 2 845 3490

kyra.kae.diola@ph.pwc.com

www.pwc.com