FINANCIAL REGULATOR REFORM (NO. 1) BILL 2019: ACCESS TO TELECOMMUNICATIONS INTERCEPTION INFORMATION

EXPOSURE DRAFT EXPLANATORY MATERIALS

Table of contents

Glossary..... 1

Chapter 1 Access to Telecommunications Interception Information..... 3

Glossary

The following abbreviations and acronyms are used throughout this explanatory memorandum.

Abbreviation	*Definition*
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
Bill	Financial Regulator Reform (No. 1) Bill 2019: Access to telecommunications interception information
Corporations Act	*Corporations Act 2001*
SMS	Short message service
TIA Act	*Telecommunications (Interception and Access) Act 1979*

Chapter 1
Access to Telecommunications Interception Information

Outline of chapter

1.1 This exposure draft Bill amends the TIA Act to allow ASIC to receive and use intercepted information for its own investigations and prosecutions of serious offences.

1.2 All legislative references in this chapter are to the TIA Act unless indicated otherwise.

Context of amendments

The establishment of the ASIC Enforcement Review Taskforce

1.3 On 19 October 2016, the Government established the ASIC Enforcement Review Taskforce in response to Recommendation 29 of the Financial System Inquiry.

1.4 The ASIC Enforcement Review Taskforce was established to review the enforcement regime available to ASIC and assess the suitability of the existing regulatory tools ASIC uses to perform its functions.

1.5 In reviewing the matters outlined in its terms of reference, the ASIC Enforcement Review Taskforce made a number of recommendations to:

- address gaps or deficiencies to allow more effective enforcement of the regulatory regime;
- foster consumer confidence in the financial system and enhance ASIC's ability to prevent harm effectively;
- promote engagement and cooperation between ASIC and its regulated population without imposing undue regulatory burden on business; and
- promote a competitive and stable financial system that contributes to Australia's productivity and growth.

The Taskforce's findings

1.6 On 18 December 2017, the ASIC Enforcement Review Taskforce provided its final report to Government. The final report contained 50 recommendations in total.

1.7 The ASIC Enforcement Review Taskforce grouped its recommendations into eight broad themes. These include:

- enhancing the requirement for financial services and credit licensees to report significant breaches to ASIC;
- harmonising and enhancing search warrant powers;
- providing ASIC with access to telephone intercepts for the investigation and prosecution of corporate law offences;
- shifting to a co-regulatory model in appropriate cases where industry participants are required to subscribe to an ASIC approved code;
- strengthening ASIC's licencing powers;
- extending ASIC's banning powers to ban individuals from managing financial services businesses;
- strengthening penalties for corporate and financial sector misconduct; and
- providing ASIC with a directions power to complement ASIC's current powers to regulate an Australian financial services licensee's or credit licensee's systems and conduct.

ASIC's access to telecommunications intercept material

1.8 The TIA Act sets out a regime that enables agencies to access various forms of telecommunication information in prescribed circumstances. This regime has staggered levels of access, with agencies that are designated 'interception' agencies able to seek warrants to intercept telecommunications for the purpose of investigating serious offences.

1.9 Interception agencies are subject to a range of strict controls in how they access and use telecommunications intercept information. Interception agencies must also apply to an eligible judge or nominated member of the Administrative Appeals Tribunal for a telecommunications intercept warrant.

1.10 Interception agencies may also share information they have obtained with other 'recipient agencies' if the material appears to relate to a matter that could be investigated by the recipient agency.

1.11 ASIC is not, however, an interception agency or recipient agency under the TIA Act. This is despite the fact that the definition of 'serious offence' in the TIA Act includes offences against provisions of the Corporations Act relating to insider trading, market manipulation and financial services fraud, as well as other fraud offences that are commonly investigated and prosecuted by ASIC.

1.12 Chapter 3 of the ASIC Enforcement Review Taskforce Report recommended that ASIC should be able to receive telecommunications intercept material to investigate and prosecute serious offences.

1.13 On 16 April 2018, the Government agreed to this recommendation.

Summary of new law

1.14 The amendments allow interception agencies to provide information about interception warrants or lawfully intercepted information to ASIC for any serious offences that ASIC can investigate or prosecute.

1.15 The amendments also allow an ASIC staff member to provide the received information to another person where the information relates to a serious offence that ASIC can investigate or prosecute.

Comparison of key features of new law and current law

New law	***Current law***
The chief officer of an interception agency can provide an ASIC staff member with information about an interception warrant or the lawfully intercepted information, where the information relates, or appears to relate, to a matter that ASIC can investigate involving the likely commission of a serious offence. The chief officer can also provide the information through a person of the interception agency.	The chief officer of an interception agency cannot provide an ASIC staff member with information about an interception warrant or the lawfully intercepted information.
An ASIC staff member can also provide another person with, use or record information about an interception warrant or the lawfully	An officer of a Commonwealth Royal Commission can provide another person with, use or record information about an interception

New law	*Current law*
intercepted information for a permitted purpose.	warrant or the lawfully intercepted information for a permitted purpose. An officer or staff member of an interception agency can provide another person with, use or record information about an interception warrant or the lawfully intercepted information, if: • the information was intercepted by the interception agency and its dissemination is for that agency's permitted purpose; or • the information was intercepted by another interception agency and its dissemination is connected with an investigation that the warrant was issued for or under certain control order warrants. An ASIC staff member can receive the information if the ASIC staff member is assisting the interception agency's investigation or for the purpose of a Royal Commission inquiry but cannot provide the information to another person for the purpose of an ASIC investigation.
A permitted purpose includes an investigation of a serious offence by ASIC and the subsequent reporting or prosecution.	A permitted purpose does not include an investigation of a serious offence by ASIC, or any subsequent reporting or prosecution.

Detailed explanation of new law

1.16 ASIC investigates and prosecutes offences under the Corporations Act and other corporate crime. Some of these offences are defined as serious offences under the TIA Act, such as insider trading, market manipulation and financial services fraud.

1.17 The TIA Act prohibits the interception of communications and access to stored communications. The *Telecommunications Act 1997* prohibits telecommunications service providers from disclosing

information about their customers' use of telecommunications services (telecommunications data).

1.18 The TIA Act sets out certain exceptions to the prohibitions to permit eligible Australian law enforcement agencies and the Australian Security Intelligence Organisation to obtain warrants to intercept communications, access stored communications or authorise disclosure of telecommunications data. This includes the provision of information to other agencies for subsequent reporting and prosecutions.

1.19 Telecommunications interception information is obtained by listening to or recording content passing over a telecommunications service (for example, real-time listening of telephone calls).

1.20 This is different to stored communications and telecommunications data. Stored communications are the content of historical communications (such as SMS or email) held by the carrier. Telecommunications data are the underlying details or 'metadata' of communications, such as subscriber details, call time or call location.

1.21 ASIC is currently able to access and use stored communications and telecommunications data. However, it cannot presently access information about interception warrants or lawfully intercepted information when available from an interception agency.

1.22 As indicated above, the TIA Act contains an exception to allow for the interception of communications in certain circumstances (for example, for the purposes of investigating serious crime).

1.23 Only specific listed agencies may obtain an interception warrant under the TIA Act; these are 'interception agencies'. Interception agencies are broadly the police, the Australian Security Intelligence Organisation and anti-corruption bodies.

1.24 ASIC is not listed as an interception agency and its staff members do not have access to telecommunications intercept information, unless they are assisting with an interception agency's investigation or prosecution or a Royal Commission inquiry.

Enabling ASIC to access and use intercepted information

1.25 Information obtained by interception activities is defined as 'lawfully intercepted information' under sections 5 and 6E of the TIA Act respectively. Information about a warrant is defined as 'interception warrant information' under sections 5 and 6EA respectively. Under specific legislated circumstances, interception agencies can share this information with other bodies, such as Commonwealth Royal Commissions.

1.26 The Bill extends those circumstances so that the chief officer of an interception agency (or officer delegated of that interception agency)

can provide interception warrant information or lawfully intercepted information to an ASIC staff member where the information relates, or appears to relate, to a serious offence that ASIC can investigate. ***[Schedule #, item 11, paragraph 68(p)]***

1.27 This ensures ASIC has access to intercepted information as well as telecommunications data and stored communications for its own investigations and prosecutions. Importantly, the Bill does not allow ASIC to itself intercept information but rather allows ASIC to receive and use information already intercepted by other agencies.

1.28 To facilitate ASIC's investigations and prosecutions of serious offences, the Bill allows an ASIC staff member to use and record the received information, as well as share the information with another person for a permitted purpose in relation to ASIC. ***[Schedule #, item 10, subsection 67(3)]***

1.29 'Permitted purpose' is defined in the TIA Act in relation to a specific agency or body under section 5. The definition does not currently capture ASIC or its functions.

1.30 Accordingly, the Bill expands the scope of 'permitted purpose' to include an ASIC investigation of a serious offence, a report on such an investigation, the making of a decision whether or not to begin a prosecution as a result of the investigation, and the prosecution itself. ***[Schedule #, items 2 to 4, definition of 'permitted purpose' in subsection 5(1)]***

1.31 An example of a report on such an ASIC investigation is an interim report on the investigation.

1.32 The Bill does not change the existing scope of serious offences defined in the TIA Act or permit ASIC to obtain an interception warrant.

Consequential amendments

1.33 The terms ***ASIC*** and ***staff member of ASIC*** are inserted into the definition section of the TIA Act. ***[Schedule #, items 1 and 5, subsection 5(1)]***

1.34 The Bill amends the headings within section 67 of the TIA Act to better reflect that communicating, using and recording intercepted information is not limited to an officer or staff member of an interception agency. The section currently also makes provision for an officer of a Commonwealth Royal Commission. ***[Schedule #, items 7 to 9, section 67]***

Application and transitional provisions

1.35 The amendments apply to information about interception warrants or lawfully intercepted information obtained by an interception agency before, at or after the day after Royal Assent. ***[Schedule #, item 12]***

1.36 This ensures that ASIC has access to interception information that interception agencies currently hold, which will enhance ASIC's ability to investigate and prosecute serious offences successfully going forward.