

# THE ENFORCEMENT OF TELECOMMUNICATIONS CONSUMER PROTECTIONS

FEBRUARY 2024



**UTS**

Centre for  
Media Transition

# The Enforcement of Telecommunications Consumer Protections

## About the Centre for Media Transition

The Centre for Media Transition (CMT) is an applied research unit based at the University of Technology Sydney (UTS). Launched in 2017, the CMT is an interdisciplinary initiative of the Faculty of Arts and Social Sciences and the Faculty of Law.

CMT works across disciplines to explore and develop responses to the dramatic and ongoing movements wrought by digital disruption to the media industry, the role of journalism in Australian democracy and the world more widely, and the business models that support a diverse and prosperous industry.

### CONTACT

Centre for Media Transition  
Faculty of Law, University of Technology Sydney  
Building 2, Level 15  
UTS City Campus, Broadway  
PO Box 123, Broadway NSW 2007

[cmt@uts.edu.au](mailto:cmt@uts.edu.au) | [cmt.uts.edu.au](http://cmt.uts.edu.au)

This report was written by Karen Lee (ORCID 0000-0002-9640-221X), Derek Wilding (ORCID 0000-0002-7806-8895), Kieran Lindsay (ORCID 0000-0002-1624-7679) and Vidya Kathirgalingam. Report design and production by Rosa Alice.

The research was commissioned by the Australian Communications Consumer Action Network (ACCAN). The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Staff from the Australian Communications and Media Authority provided comments on an earlier draft of this report for which we are grateful. Any errors in this final report are our own.

**Suggested citation:** Karen Lee, Derek Wilding, Kieran Lindsay & Vidya Kathirgalingam, *The Enforcement of Telecommunications Consumer Protections* (UTS Centre for Media Transition, 2024).

DOI: 10.6084/m9.figshare.25241806



This work is licensed under the Creative Commons Attribution-Non-Commercial-ShareAlike 4.0 International License. To view a copy of this license, visit: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

# Contents

EXECUTIVE SUMMARY	5
INTRODUCTION	8
<b>1 RESPONSIVE AND RISK-BASED REGULATION</b>	<b>11</b>
<b>A Responsive Regulation</b>	<b>11</b>
1 Some Criticisms of Responsive Regulation	13
2 What Makes Regulators 'Responsive'?	14
3 The Strengths-based Pyramid	16
<b>B Risk-based Regulation</b>	<b>17</b>
<b>2 ENFORCEMENT MECHANISMS</b>	<b>20</b>
<b>A Categorising Penalties</b>	<b>20</b>
<b>B The ACMA's Enforcement Mechanisms</b>	<b>21</b>
1 Administrative Mechanisms	21
2 Civil Mechanisms	24
3 Criminal Mechanisms	25
4 Enforceable Undertakings	26
<b>C Which Mechanisms May be Used When?</b>	<b>27</b>
1 Industry Codes	27
2 Industry Standards	29
3 Select Service Provider Rules	31
4 Select Carrier Licence Conditions	34
<b>3 APPROACH TO ENFORCEMENT</b>	<b>37</b>
<b>A General Compliance and Enforcement Approach and Factors Influencing the ACMA's Approach</b>	<b>37</b>
1 Infringement Notice Factors	40
2 Enforceable Undertaking Factors	41
3 Remedial Directions Factors	41
<b>B Comparing the ACMA's Responsive Approach with Responsive Regulation Theory</b>	<b>41</b>
<b>C Enforcement Priorities</b>	<b>42</b>
<b>4 HOW HAVE THE ENFORCEMENT MECHANISMS BEEN USED?</b>	<b>44</b>
<b>A Research Limitations and Context</b>	<b>44</b>
1. Research Limitations	44
2. Contextual Information	47
<b>B Total Publicised Enforcement Actions and Amounts of Publicised Infringement and Civil Penalties</b>	<b>49</b>

<b>C</b>	<b>Examples of How the ACMA has Exercised its Enforcement Powers</b>	<b>50</b>
1	Administrative Enforcement Actions	51
2	Civil Penalty Enforcement Actions	56
<b>D</b>	<b>Telcos with the Most Investigations and Enforcement Actions</b>	<b>59</b>
1	Enforcement Actions Against Telstra	61
2	Enforcement Actions Against Lycamobile	62
3	Enforcement Actions Against Optus	63
4	Enforcement Actions Against SpinTel	63
5	Enforcement Actions Against TPG	64
6	Enforcement Actions Against Vodafone	65
7	Enforcement Actions Against Dodo	65
8	Enforcement Actions Against Exetel	66
9	Enforcement Actions Against iTalkBB	66
10	Enforcement Actions Against MyRepublic	66
11	Enforcement Actions Against Southern Phone Company	67
	Additional Note on the TPG Group	67
<b>E</b>	<b>Provisions with the Most Enforcement Actions in Published Investigations</b>	<b>70</b>
<b>F</b>	<b>Most Common Enforcement Actions in Published Investigations</b>	<b>71</b>
<b>G</b>	<b>Years When the ACMA Engaged in the Least and Most Enforcement Activity</b>	<b>78</b>
	<b>CONCLUSION</b>	<b>80</b>
	<b>ANNEX A</b>	<b>84</b>
	<b>Industry Codes Registered by the ACMA under Part 6</b>	<b>84</b>
	<b>ANNEX B</b>	<b>85</b>
	<b>Data Collection Methodology</b>	<b>85</b>
	<b>ANNEX C</b>	<b>87</b>
	<b>Examples of the ACMA Compliance Audits</b>	<b>87</b>

# Executive Summary

In this report we present a preliminary account of enforcement action taken by the Australian Communications and Media Authority (the ACMA) between 1 January 2010 and 30 June 2023 in relation to four sources of consumer protection rules arising out of the *Telecommunications Act 1997* (Cth) (Tel Act): industry codes registered under Part 6 of that Act, industry standards determined under ss 123, 124, 125 and 125AA, select service provider rules, and select carrier licence conditions.

An explanation of the types of enforcement mechanisms available to the ACMA and the circumstances in which they can be used (for example, in the first instance, the ACMA may be limited by legislation to issuing a formal warning or direction to comply) is provided in Chapter 2 below.

A comprehensive assessment of compliance enforcement action would require a richer understanding of context and access to additional data. In the Introduction below we outline limitations encountered in this research, qualifications to the findings, and comments on the presentation of the data. For example, we do not offer a comparative assessment based on the degree of consumer harm. In addition, information on compliance investigations conducted by the ACMA – as distinct from specific enforcement actions – is limited to those matters where the ACMA publicly reported a breach of one of the consumer protections rules, as the ACMA does not generally publish data on investigations where there is no breach finding. And, as explained below, the ACMA may consider it is not in the public interest to publicly release information about a breach even where enforcement action is taken. Nevertheless, the report offers some insight, not otherwise available, into the ACMA's enforcement practices over time.

## Findings

Overall, we found 487 investigations into breaches of our select consumer protection rules that the ACMA had made public. There were 309 providers that had enforcement action taken against them, and in total 502 enforcement actions pursued by the ACMA. Not all breach findings resulted in enforcement action: we found 26 instances of no recorded enforcement action arising from a publicised investigation.

The range of enforcement actions was as follows:

- 296 formal warnings
- 119 directions to comply
- 41 remedial directions
- 24 infringement notices with a total value of \$6,143,160
- 17 enforceable undertakings
- 3 civil penalty orders obtained from the Federal Court totalling \$1,077,625
- 1 injunction obtained from the Federal Court
- 1 deed of agreement.

Further information on these enforcement actions and how we have identified the providers that were subject to them can be found in Chapter 4.

Within the set of publicised enforcement action, the highest number of actions were taken in 2013-14, followed by 2018-19 and 2014-15. The actions in 2013-14 and 2014-15 coincided with

the ACMA conducting audits of compliance with the Telecommunications Consumer Protections Code (TCP Code). The least amount of enforcement action occurred in 2011-12. If the total of 502 enforcement actions is averaged over the 13.5 year period examined here, the ACMA took just over 37 actions per year.

Of the 309 providers with enforcement action taken against them, 79 were the subject of more than one action. The providers with the most enforcement actions taken against them were: Telstra (24), Lycamobile (12), Optus (11) and Spintel, TPG and Vodafone (8 each), although it should be noted that these providers together accounted for less than 15% of the overall number of actions.

The provisions that attracted the highest number of enforcement actions were those relating to:

- the obligations to provide Communications Compliance (CommCom) with compliance attestation documentation (240 actions)
- the provision of Integrated Public Number Database-related information (IPND) (73 actions)
- obligations relating to complaint handling (49 actions)
- requirements concerning advertising or provision of information to customers (35 actions)
- the requirements to join and comply with the Telecommunications Industry Ombudsman (TIO) scheme (28 actions).

As noted above, the most common enforcement actions were formal warnings and directions to comply. Some other observations are as follows.

- Remedial directions to comply with Tel Act obligations relating to the IPND Tel Act rules were often accompanied by directions to comply with the IPND Code (where both the IPND Code and related Tel Act obligations were breached).
- Infringement notices were issued less frequently than remedial directions. Telstra was issued with the most remedial directions: 3. Netfast, Optus and TransAct Communications were each issued with 2. Thirty-two other providers were each issued with 1. Telstra and Lycamobile were issued with the most infringement notices: 4. Exetel, Aussie Broadband and Circles Australia were each issued 2. Ten other providers each received 1.
- The three civil penalty orders (and one injunction) were all obtained in circumstances where there were repeated failures to comply with determinations made by the TIO or where issues of public safety were concerned.
- Enforceable undertakings were obtained for breaches of the Tel Act obligations relating to the IPND, the ACMA's Determination concerning migration to the NBN, the Telecommunications (Consumer Complaints Handling) Industry Standard 2018, the priority assistance obligation imposed on Telstra by way of the Telecommunications (Carrier Licence Conditions Telstra Corporation Limited) Declaration 2019, the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017, and the Telecommunications (Emergency Call Service) Determination 2009.

It should be noted that this reporting of year-on-year results is only one way of presenting enforcement data and does not take account of the complexity of compliance investigations or

the differing nature of consumer harm, and nor does it provide insight into the deterrence value of some enforcement actions over others. It should also be noted that the ACMA undertook numerous compliance audits of communications providers from 2010 to 2023, examples of which are provided in Annex C.

## Observations

A comprehensive assessment of the ACMA's practices against the principles of responsive and risk-based regulation would require a richer understanding of context and access to additional data. However, the publicly available data presented in this report suggests that when the ACMA takes enforcement action it acts in accordance with and subject to the limitations of the Tel Act. It also suggests that the ACMA broadly acts in a way that is consistent with its Compliance and Enforcement Policy and related guidelines.

In the five-year period 2018-19 to 2022-23, the ACMA took 211 enforcement actions; while this is lower than the 259 actions it took in the previous five years, the results for the earlier period are affected by a single compliance audit in 2013 (following the establishment of Communications Compliance and a new Compliance Framework under the TCP Code) which led to 95 formal warnings. Furthermore, it appears that the ACMA has diversified the types of enforcement actions it has taken since 2018-19, issuing more remedial directions and infringement notices and accepting enforceable undertakings rather than opting to issue formal warnings and directions to comply. This could suggest a stronger approach to enforcement than in previous years. It may also reflect the specific types of regulatory rules breached.

The data provokes questions (outside the scope of this report) about the adequacy of the ACMA's Tel Act enforcement powers – in particular, whether the ACMA needs additional tools (used in isolation or combination) to secure or motivate industry compliance. These questions would include whether the ACMA should have access to tools other than a formal warning and a direction to comply for breaches of codes of practice; whether the value of an infringement fine should be increased to cover situations where a relatively serious single breach attracts a heavier fine; and whether the ACMA should be able to seek the imposition of criminal penalties on providers who seriously and repeatedly fail to comply with consumer protection rules and exclude temporarily or permanently from the market service providers who serially breach their consumer protection obligations with the result of serious consumer harm.

The data also points to aspects of compliance and enforcement that deserve additional consideration. Charting the correlation of the ACMA's self-initiated audits with enforcement outcomes, for example, may highlight the value of this work, while additional consideration of the following aspects would help to inform industry, government and the community on the impact of regulatory interventions: the extent to which the degree of consumer harm is an element in decisions on enforcement action; the relative merits of using available alternative enforcement mechanisms (eg, formal warnings or directions to comply for code breaches); the targeting of available enforcement resources to service providers with demonstrated compliance problems; and the additional deterrence value of civil penalties and injunctions.

Finally, the material considered in this report highlights the importance of publicly available data on enforcement of consumer protection rules and suggests the need for a statutory register of completed investigations and enforcement action, subject to the ACMA being satisfied that publication is in the public interest.

# Introduction

In this report, we identify the tools the ACMA may use to enforce certain ‘core’ consumer-protection related provisions of the Tel Act and *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) (TCPSS Act). The report centres on a set of key telecommunications consumer protection measures, not on the full range of measures. The report does not cover all consumer-related provisions in these Acts and associated regulatory instruments; the scope of the research was restricted to take account of the available budget and timeline for the work. Accordingly, the research was designed to cover key consumer protection measures identified in conjunction with ACCAN — the leading Australian communications consumer body that funded this research. This means that some measures such as those in the TCPSS Act relating to the provision of untimed local calls or the operation of the Customer Service Guarantee, as well as separate schemes such as those relating to telemarketing calls or spam, are not covered. Other notes on methodology are set out in Annex B.

The Australian Competition and Consumer Commission (ACCC) also has a prominent role in promoting consumer protection outcomes in the telecommunications industry via its administration of the Australian Consumer Law, the industry-specific anti-competitive conduct, record keeping and access regime rules, that form part of the *Competition and Consumer Act 2010* (Cth) and other competition-related obligations set out in the Tel Act; this report does not address the ACCC’s enforcement of these measures.

The consumer-protection related provisions that are the focus of this report comprise:

- select industry codes applicable to sections of the telecommunications industry and registered by the ACMA under Part 6 of the Tel Act (industry codes)
- select industry standards applicable to sections of the telecommunications industry and determined by the ACMA under ss 123, 124, 125 and 125AA of the Tel Act (industry standards)
- select service provider rules; and
- select carrier licence conditions.

The select industry codes applicable to sections of the telecommunications industry and registered by the ACMA under Part 6 of the Tel Act comprise:

- the Mobile Premium Services (MPS) Code
- the Telecommunications Consumer Protections Code
- the Information on Accessibility Features for Telephone Equipment Code
- the Integrated Public Number Database Code
- the Reducing Scam Calls and Scam SMS Code
- the Local Number Portability Code.<sup>1</sup>

The select industry standards applicable to sections of the telecommunications industry and determined by the ACMA under ss 125 and 125AA of the Tel Act comprise:

---

<sup>1</sup> See Annex A for all editions of industry codes registered by the ACMA under Part 6 of the Tel Act at the time of writing.



- the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
- the Telecommunications (NBN Continuity of Service) Industry Standard 2018
- the Telecommunications (NBN Consumer Information) Industry Standard 2018
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018.<sup>2</sup>

The select service provider rules comprise:

- the calling line identification, number portability, standard terms and conditions, record-keeping, and pre-selection rules<sup>3</sup> that the ACMA can enforce as a result of Part 1 of Schedule 2 of the Tel Act (a standard service provider rule that requires compliance with the Tel Act and TCPSS Act);
- the TIO and emergency call services rules set out in the TCPSS Act that the ACMA can enforce because of Part 1 of Schedule 2 of the Tel Act;<sup>4</sup>
- the rules set out in Parts 2, 3, 4 and 5 of Schedule 2 of the Tel Act relating to operator services, directory assistance services, integrated public number database, itemised billing, and priority assistance (standard service provider rules); and
- four service provider determinations made by the ACMA under s 99(1) of the Tel Act: the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, the Telecommunications Service Provider (International Mobile Roaming) Determination 2019, the Telecommunications Service Provider (NBN Service Migration) Determination 2018, and the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

The select carrier licence conditions include:

- the calling line identification, number portability, pre-selection,<sup>5</sup> and record-keeping rules that the ACMA can enforce as a result of Part 1 of Schedule 1 of the Tel Act (a standard carrier condition that requires compliance with the Tel Act and TCPSS Act);
- the emergency call services rules set out in the TCPSS Act that the ACMA can enforce as a result of Part 1 of Schedule 1 of the Tel Act;<sup>6</sup> and
- certain additional licence conditions that now apply to Telstra Limited because of s 63A of the Tel Act and/or to Telstra Infraco Limited because of *Telecommunications (Carrier Licence Conditions – Telstra Infraco Limited) Declaration 2019* (Cth). They include obligations involving: operator services; directory assistance services; alphabetical public number directory; IPND; disclosure of specified Premises Location Information to NBN; priority assistance arrangements; and low-income measures.<sup>7</sup>

<sup>2</sup> The Telecommunications (Financial Hardship) Industry Standard 2024 was not in force during the time period that is the focus of this report.

<sup>3</sup> See, respectively, *Telecommunications Act 1997* (Cth) (Tel Act) pts 18, 22–23, s 529, pt 17.

<sup>4</sup> See, respectively, *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) (TCPSS Act) pts 6, 8.

<sup>5</sup> See, respectively, Tel Act pts 18, 22, 17, s 529.

<sup>6</sup> See, respectively, TCPSS Act pts 6, 8. Carriers are also required to join the TIO dispute resolution scheme, but this obligation falls outside the scope of this report as the TIO resolves disputes arising between carriers and landowners.

<sup>7</sup> See the ACMA, *Additional Conditions of a Carrier Licence – Telstra Limited* (ACN 086 174 781) <<https://data.gov.au/data/dataset/52db5013-1a63-4d14-90f8-c19fb6289695/resource/fbe82ecc-4975-409f-bbf0-c817d80c9195/download/additional-conditions-on-a-carrier-licence-telstra-limited.pdf>>.

Using publicly available information found on the ACMA's website and within annual reports, we also examine the way in which the ACMA has exercised its discretion to enforce these rules.

In Chapter 1 of the report, we provide an overview of responsive and risk-based strategies of regulation – two highly influential strategies of regulation that have informed and continue to inform the ACMA's approach to enforcement and compliance.

In Chapter 2 we explain and categorise the various mechanisms the ACMA may use to enforce the select industry codes registered by the ACMA under Part 6 of the Tel Act, the select industry standards determined by the ACMA under ss 125 and 125AA of the Tel Act, the select service provider rules, and the select carrier licence conditions. In addition, we explain when the ACMA is permitted to use these mechanisms.

In Chapter 3 we set out the ACMA's general approach to compliance and enforcement and the factors that influence its decisions to enforce the statutory provisions for which it is responsible. We also set out additional factors that the ACMA says it takes into account before using three of the mechanisms in its 'toolbox' – infringement notices, enforceable undertakings, and remedial directions. In addition, we compare the ACMA's responsive approach with responsive regulation theory. We conclude this chapter with a discussion of the ACMA's enforcement priorities over the last four years.

In Chapter 4 we describe how the ACMA has exercised its discretion to enforce the various consumer protection-related provisions after it has found providers have breached those rules. The enforcement actions we discuss are only a subset of the total number of consumer protection matters investigated by the ACMA. Each year the ACMA commences formal investigations into compliance with the consumer protection rules, although only some of these relate to the rules we examine in this report, only some proceed to breach findings and related enforcement action, and not all investigations are publicised. As the ACMA does not generally publicise investigations where it concludes no breach has occurred and has not adopted a standard format in its annual reports for reporting the number of investigations opened or closed in a reporting year, we are unable to describe how the ACMA has exercised its discretion to open and close investigations without making a finding of breach.

Annex A lists the industry codes currently registered by the ACMA under Part 6 of the Tel Act.

Annex B explains the methodology we used to collect the data that informs this report.

Annex C provides examples of compliance audits the ACMA undertook between 1 July 2009 and 30 June 2023.

# 1 Responsive and Risk-based Regulation

Before explaining the mechanisms the ACMA may use to enforce the select industry codes, the select industry standards, the select service provider rules and the select carrier licence conditions, we provide a short summary of responsive and risk-based strategies of regulation. We start by briefly explaining these strategies for two reasons. First, both theories have influenced the ACMA's approach to compliance and enforcement, which is considered in Chapter 3. Second, along with the continuum of administrative, civil and criminal sanctions explained in Chapter 2, the 'enforcement pyramid' associated with responsive regulation provides a way to illustrate the severity of the sanctions (outlined in section B of Chapter 2) that the ACMA may use to enforce the various consumer-protection rules.<sup>8</sup>

## A Responsive Regulation

Responsive regulation is a highly influential<sup>9</sup> regulatory strategy (both in Australia and worldwide) first developed by academics Ian Ayres and John Braithwaite in the early 1990s.<sup>10</sup> At its simplest, it is the idea that 'regulators should be responsive to the conduct of those they seek to regulate in deciding whether a more or less interventionist response is needed'.<sup>11</sup> Responsive regulation, in fact, encompasses a wide range of ideas and regulatory techniques including, for example, tripartism,<sup>12</sup> enforced self-regulation,<sup>13</sup> partial-industry intervention,<sup>14</sup> and delegation of regulatory responsibilities to third parties. However, it is most closely associated with the 'enforcement pyramid'.<sup>15</sup>

The enforcement pyramid is based on the idea that regulators need access to a range of punishments with varying degrees of severity to ensure corporations comply with their legal obligations. It is also based on the idea that regulators should use the least coercive means necessary to achieve the objective of securing compliance. It presumes that if a corporation breaches a law, regardless of the severity of the breach or the nature of the legal requirement, the initial response of a regulator should be to engage in dialogue with the company involved. The regulator should listen to the company's concerns, explain the purpose of the law, offer and obtain advice to/from the company, and persuade the company that compliance is the right thing

---

<sup>8</sup> See Arie Freiberg, *Regulation in Australia* (The Federation Press, 2017) 401.

<sup>9</sup> See, eg, Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* (Report No 95, March 2002) [2.60] noting its influence on the Australian government's decision to incorporate the use of civil penalties into the Corporations Law (now the Corporations Act) in 1993; Mary Ivec et al, 'Applications of Responsive Regulatory Theory in Australia and Overseas: Update' (Occasional Paper No 23, Regulatory Institutions Network, College of Asia and the Pacific, Australian National University, March 2015).

<sup>10</sup> Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

<sup>11</sup> John Braithwaite, *Regulatory Capitalism: How It Works, Ideas for Making It Work Better* (Edward Elgar, 2008) 88.

<sup>12</sup> Tripartism involves government fostering public interest group participation in the regulatory process.

<sup>13</sup> Enforced self-regulation involves regulators requiring companies to write their own rules – rules that reflect their specific needs. The rules are subject to the approval of regulators with public interest groups having the opportunity to comment on them in draft. Regulators are responsible for monitoring industry compliance with approved rules and taking enforcement action where required. However, large businesses are required to set up independent inspector groups that would have principal responsibility for enforcing the rules.

<sup>14</sup> Partial industry intervention is the idea that only select section(s) of an industry, rather than entire industries, should be regulated.

<sup>15</sup> Peter Mascini, 'Why Was the Enforcement Pyramid So Influential? And What Price Was Paid?' (2013) 7(1) *Regulation & Governance* 48.

to do.<sup>16</sup> If dialogue fails (ie, the company still does not comply with the law), the regulator should then begin to apply 'somewhat punitive approaches'<sup>17</sup> (eg, issuing a warning letter). If these approaches also fail, the regulator should apply 'even more punitive approaches'<sup>18</sup> (eg, imposing a financial penalty, suspending a licence). If these even more punitive approaches fail to secure compliance, the regulator should then seek to 'incapacitate' the company, for example, by excluding them from the market. The enforcement pyramid is, however, intended to be 'dynamic'; regulators have the flexibility to depart from the presumption of dialogue and apply punitive approaches when circumstances warrant them (eg, where levels of harm are severe).<sup>19</sup> Moreover, the philosophy behind the enforcement pyramid suggests that if less interventionist measures succeed (ie, compliance is achieved), then the regulator should 'de-escalate' and return to its practice of engaging in dialogue with the company concerned.<sup>20</sup>

An example of an enforcement pyramid is provided below.

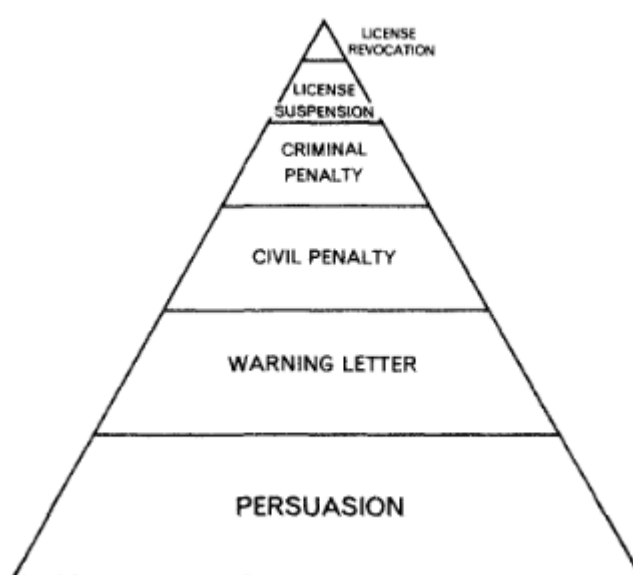


Figure 1. Enforcement Pyramid.<sup>21</sup>

It is important to recognise that the enforcement pyramid assumes corporations are not monolithic entities. They have 'multiple selves' (ie, different motivations for complying with the law - motivations that 'operate both serially and simultaneously').<sup>22</sup> Multiple enforcement tools are needed so that regulators can deploy them sensitively in light of the different motivations of corporate actors and their own experiences of interacting with them. Ayres and Braithwaite do not attempt to delineate or categorise the full range of compliance motivations corporate actors have or to design an exhaustive toolkit that successfully harnesses all of them. Rather, their key

<sup>16</sup> Ivec et al (n 9) 6.

<sup>17</sup> John Braithwaite (n 11) 89.

<sup>18</sup> Ibid.

<sup>19</sup> Ibid 90.

<sup>20</sup> Ibid.

<sup>21</sup> Ayres and Braithwaite (n 10) 35.

<sup>22</sup> Vibeke Lehmann Nielsen and Christine Parker, 'Mixed Motives: Economic, Social, and Normative Motivations in Business Compliance' (2012) 34(4) *Law and Policy* 428, 429.

insight, drawn from Braithwaite's studies of nursing homes and coal mines,<sup>23</sup> is that economic rationalism – the premise that underpins traditional deterrence theories of compliance – is not the only factor that motivates compliance. Corporate actors will often be motivated by economic rationalism and some corporate actors will only be motivated by profit-seeking motives, but some will also be motivated by '[doing] what is right, [being] faithful to their identity as a law abiding citizen, and [sustaining] a self-concept of social responsibility.'<sup>24</sup> And by denying the existence of those other motivating factors, regulators run the risk of undermining the incentives law-abiding corporate actors might have to comply. It is for that reason they suggest that regulators need to engage in dialogue with regulatees – dialogue that a 'tit for tat' enforcement strategy (as it is referred to in the literature) encourages and facilitates.

Over the last three decades, responsive regulation has been the subject of much study, discussion, and critique in the academic literature. We have not been asked to summarise and/or review that voluminous literature for this report. However, below we provide a small sample of the criticisms regulatory scholars have made about the enforcement pyramid to highlight that even though it has been influential, responsive regulation is not uncontested. We also highlight the various factors 'responsive' regulators are said to need to consider when seeking to enforce rules – a point we will return to in Chapter 4 where we highlight the difficulties of empirically assessing whether the ACMA has been a responsive regulator. In addition, we explain the concept of a support or strengths-based pyramid – another pyramid that in 2007 John Braithwaite, Toni Makkai and Valerie Braithwaite<sup>25</sup> suggested regulators should use in conjunction with the enforcement pyramid to secure compliance.

## 1 Some Criticisms of Responsive Regulation

Criticisms made by regulatory scholars about responsive regulation and the enforcement pyramid include the following.

- It assumes regulators have an ongoing and direct face-to-face relationship with regulatees – a relationship that many regulators may not have with the companies they oversee, especially in complex sectors with multiple players such as financial services.<sup>26</sup>
- It assumes regulators have knowledge about, or the capacity to learn about, the contexts in which regulatees operate, their motivations, backgrounds and objectives,<sup>27</sup> despite the existence of well-known information asymmetries between regulators and regulatees.
- Escalation up the pyramid assumes that all regulatees perceive and/or respond to the prescribed hierarchy of penalties in the same way even though regulatees may react to the same penalties differently.<sup>28</sup>
- It assumes regulators can clearly communicate to regulatees about how they will react to non-compliant behaviour and regulatees can easily understand the messages being

---

<sup>23</sup> See Ayres and Braithwaite (n 10) 21-27. John Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (State University of New York Press, 1985).

<sup>24</sup> Ayres and Braithwaite (n 10) 22.

<sup>25</sup> John Braithwaite, Toni Makkai and Valerie Braithwaite, *Regulating Aged Care: Ritualism and the New Pyramid* (Edward Elgar, 2007).

<sup>26</sup> Cristie Ford, 'Prospects for Scalability: Relationships and Uncertainty in Responsive Regulation' (2013) 7(1) *Regulation & Governance* 14; Freiberg (n 8) 447–8.

<sup>27</sup> Freiberg (n 8) 447.

<sup>28</sup> Julien Etienne, 'Ambiguity and Relational Signals in Regulator-Regulatee Relationships' (2013) 7(1) *Regulation & Governance* 30.

communicated, even though ensuring effective and unambiguous communication between parties can be difficult to achieve in practice.<sup>29</sup>

- Regulators often lack the legislative tools needed to escalate enforcement in their enabling legislation<sup>30</sup> as well as the resources and training required to implement a truly responsive regulatory approach.
- De-escalation down the pyramid or a return to dialogue may not be possible if strong enforcement action undermines any trust built between regulators and regulatees over time.

## 2 What Makes Regulators 'Responsive'?

The precise factors that regulators must consider to be classified as 'responsive' vary. They depend on the specific understanding or interpretation of responsive regulation adopted. Moreover, as more empirical research on regulatory enforcement is conducted and the theory of responsive regulation continues to evolve, the number of factors that regulators must consider (or be responsive to) continues to expand.

All forms of responsive regulation require regulators at a minimum to be sensitive to the specific 'conduct' of regulatees. Yet, as Nielsen has highlighted, conduct is an ambiguous term. She identifies five (non-mutually exclusive) types of conduct that 'responsive' regulators could possibly take into account when regulatees commit a breach. The different types of conduct include:

- the type, number and gravity of breaches committed by regulatees;
- the historical performance of regulatees over time, which enables regulators to focus on the seriousness and number of previous breaches committed by regulatees and categorise regulatees as 'good apples' or 'bad apples'. Taking into account the historical performance of regulatees gives regulators the flexibility to 'forgive' good apples if they make the odd mistake, and to punish 'bad apples' where regulatees have demonstrated multiple incidents of non-compliance over a period of time;
- the desire of regulatees to improve their behaviour;
- the extent to which regulatees involve regulators in their planning processes and/or meet with them to discuss other necessary changes to their behaviour; and
- the regulators' overall opinion of regulatees' compliance.

Nielsen describes regulators who take into account the type, number and gravity of breaches committed by regulatees as 'legalistic' or 'short memory' responsive. Regulators who focus on the historical performance of regulatees over time are 'long-memory' responsive. Regulators who consider the desire of regulatees to improve their behaviour are 'attitudinally' responsive. Regulators who respond to the number of times regulatees involve regulators in their planning processes and/or meet with them to discuss other necessary changes to their behaviour are 'dialogically' responsive. Regulators who factor in their overall assessment of regulatees' compliance before taking or when deciding enforcement action are 'subjective performance' responsive.<sup>31</sup>

However, as Nielsen points out, Ayres and Braithwaite's understanding of responsive regulation places great weight on the desire of regulatees to improve their behaviour; the extent to which

---

<sup>29</sup> Mascini (n 15) 50–1.

<sup>30</sup> Freiberg (n 8) 446. See also *ibid* 52.

<sup>31</sup> Vibeke Lehmann Nielsen, 'Are Regulators Responsive?' (2006) 28(3) *Law & Policy* 395, 397–8, 406–7.

regulatees engage in dialogue with regulators (eg, by involving regulators in their planning processes and/or meeting with them to discuss other necessary changes to their behaviour); and their overall opinion of regulatees' compliance. This is because, for Ayres and Braithwaite, regulators must be able to 'forgive the bad guy's history of wrongdoing'<sup>32</sup> and cooperate with regulatees from the beginning if they are to drive improvements within regulatees. In other words, Ayres and Braithwaite's approach means that 'responsive' regulators should give relatively little consideration to:

- the types, seriousness and number of breaches involved;
- the historical performance of regulatees over time (ie, regulators should not categorise regulatees as 'good apples' or 'bad apples' and should not respond in light of these categorisations when confronted by new breaches committed by regulatees).<sup>33</sup>

Indeed, according to Nielsen, for Ayres and Braithwaite, consideration of these factors means regulators are adopting a less than ideal form of responsiveness (ie, a form of responsiveness that is less cost efficient).<sup>34</sup>

In addition to affecting the precise conduct that regulators take into account, different understandings of responsive regulation also dictate whether and the extent to which regulators must consider their own enforcement behaviours or 'enforcement styles' (ie, how they 'relate to those they are regulating'<sup>35</sup>). If regulators adopt a 'tit for tat' understanding of responsive regulation (the approach most commonly associated with the enforcement pyramid), they must be sensitive to the ways in which they interpret and apply the rules in question (eg, formally or liberally) and the extent to which they seek to help or punish regulatees in breach of the rules.<sup>36</sup> In other words, the job of regulators is to 'match' their enforcement behaviour to the demonstrated attitudes and behaviour of regulatees.<sup>37</sup>

If regulators adopt a 'restorative justice' approach to responsive regulation (as Braithwaite did in his later work<sup>38</sup>), however, regulators are not required to match their enforcement behaviour to the demonstrated attitudes of regulatees. Rather, regulators must never explicitly threaten regulatees when they interact with them. Regardless of the attitudes regulatees display throughout the enforcement process, regulators should continue to engage in open dialogue with them. Regulators can continue to escalate up the enforcement pyramid if regulatees fail to comply, but the 'threat' of escalation comes from the legislation empowering regulators, not direct threats regulators make.<sup>39</sup>

A non-exhaustive list of other matters that scholars have argued and/or identified that responsive and 'really responsive' regulators should take into account includes:

---

<sup>32</sup> Ibid 397.

<sup>33</sup> Ibid.

<sup>34</sup> Ibid 399.

<sup>35</sup> Peter J May and Robert S Wood, 'At the Regulatory Front Lines: Inspectors' Enforcement Styles and Regulatory Compliance' (2003) 13(2) *Journal of Public Administration Research and Theory* 117, 119.

<sup>36</sup> Vibeke Lehmann Nielsen and Christine Parker, 'Testing Responsive Regulation in Regulatory Enforcement' 3(4) *Regulation & Governance* 376, 381.

<sup>37</sup> Ibid 382.

<sup>38</sup> See, eg, John Braithwaite, *Restorative Justice and Responsive Regulation* (Oxford University Press, 2002).

<sup>39</sup> Nielsen and Parker (n 36) 382.

- ‘motivational postures’ – the ‘signals that people send to authorities ... to indicate their liking for that authority and their willingness to defer to the authority’s rules and processes’;<sup>40</sup>
- the factors that influence the organisational cultures of regulatees (eg, the internal and external pressures on companies, the extent to which internal objectives depart from regulatory goals, and how regulatory rules and norms are embedded in those organisations);<sup>41</sup>
- the factors that shape the institutional environment in which regulators act (eg, the norms that regulate their conduct, their resourcing, and the extent to which regulators with overlapping jurisdiction ‘coordinate’ their enforcement strategies);<sup>42</sup>
- ‘those upon whom the [regulatory] institution depends; and ... the community whose well-being it affects’<sup>43</sup> and/or the ‘public interest’.<sup>44</sup>

### 3 The Strengths-based Pyramid

Unlike the enforcement pyramid, which is concerned with ensuring regulatees comply with minimum standards (ie, they conform to set rules), the goal of a strengths-based pyramid is to encourage regulatees to engage in continuous improvement. Like the enforcement pyramid, it is grounded in dialogue and persuasion. However, instead of using threats and punishments to secure compliance, the strengths-based pyramid is built around the use of rewards.<sup>45</sup> Under this approach, regulators are meant to identify the strengths of regulated organisations and encourage regulated organisations to ‘build’ on those strengths by rewarding positive behaviour and other activities that improve outcomes. The strengths-based pyramid assumes regulators have access to a range of rewards (eg, positive feedback, prizes, grants, public praise) with varying degrees of appeal to regulatees, which they can bestow as and when the circumstances warrant and in proportion to the degree to which regulatees make improvements and build their compliance capacity. Braithwaite, Makkai and Braithwaite emphasise that a strength-based pyramid offers alternative, not complementary, compliance strategies to an enforcement pyramid.<sup>46</sup>

This means that after assessing the different compliance motivations of regulatees and other compliance-related factors, including context and culture,<sup>47</sup> regulators choose between deploying supports or sanctions as is appropriate in the particular circumstances. As with the enforcement pyramid, there is a preference in the strengths-based pyramid for dialogue in the first instance; however, when dialogue and encouragement fail and standards are (or continue

<sup>40</sup> Valerie Braithwaite, ‘Defiance and Motivational Postures’ in David Weisburd and Gerben Bruinsma (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer, 2014) 915. See also Valerie Braithwaite, Kristina Murphy and Monika Reinhart ‘Taxation Threat, Motivational Postures, and Responsive Regulation’ (2007) 29(1) *Law & Policy* 137; Valerie Braithwaite et al, ‘Regulatory Styles, Motivational Postures, and Nursing Home Compliance’ (1994) 16(4) *Law & Policy* 363.

<sup>41</sup> Robert Baldwin and Julia Black, ‘Really Responsive Regulation’ (2008) 71(1) *The Modern Law Review* 59, 69–70.

<sup>42</sup> See *ibid* 70, 78, 85–6; Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press, 2<sup>nd</sup> ed, 2012) 270.

<sup>43</sup> Seung-Hun Hong and Jong-sung You, ‘Limits of Regulatory Responsiveness: Democratic Credentials of Responsive Regulation’ (2018) 12(3) *Regulation & Governance* 413, 419.

<sup>44</sup> This might be done, for example, by enabling public interest groups to participate in discussions concerning potential enforcement action with regulators and regulatees. See, eg, Ayres and Braithwaite (n 10) ch 3.

<sup>45</sup> Braithwaite, Makkai and Braithwaite (n 25) 330.

<sup>46</sup> *Ibid* 319–23.

<sup>47</sup> See, eg, Christine Parker and Vibeke Lehmann Nielsen, ‘Compliance: 14 Questions’ in Peter Drahos (ed), *Regulatory Theory: Foundations and Applications* (Australian National University Press, 2017) 217.



to be) below the minimum expected of a regulated entity, then enforcement action needs to be taken.<sup>48</sup>

An example of a strengths-based pyramid and an accompanying enforcement pyramid is provided in Figure 2 below.

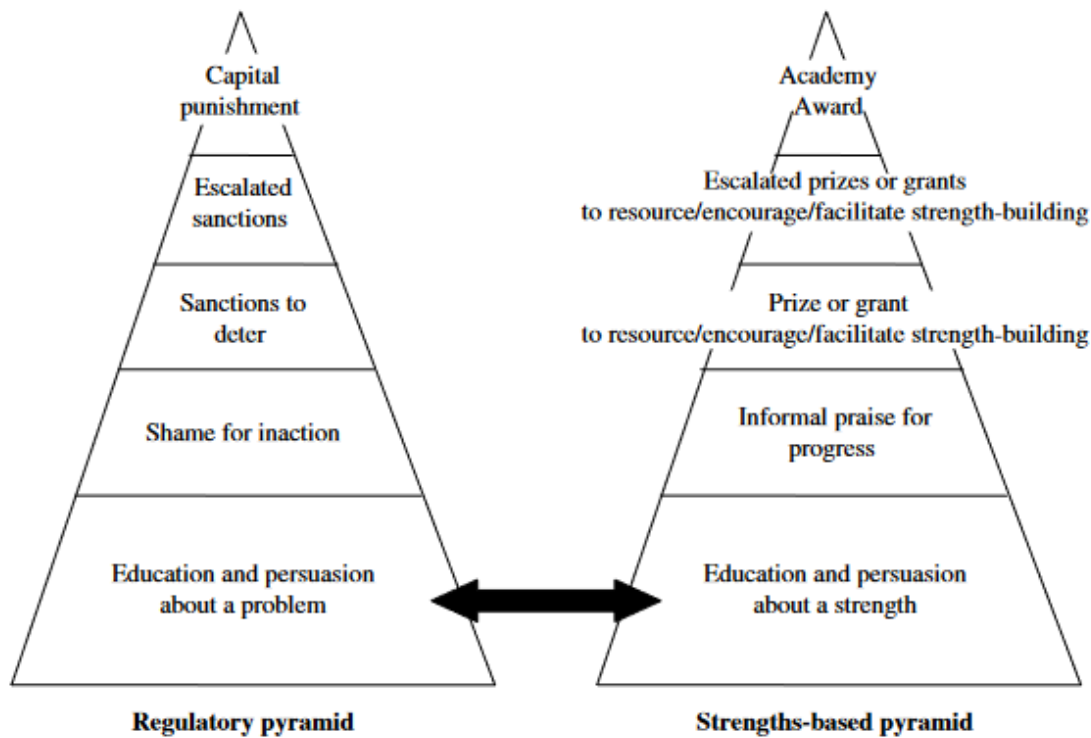


Figure 2 Strengths-based Pyramid <sup>49</sup>

## B Risk-based Regulation

Risk-based regulation emerged in the early 2000s in the UK under the label of 'better regulation'<sup>50</sup> but has since been embraced elsewhere including in Australia. For example, the *Public Governance, Performance and Accountability Act 2013* (Cth) requires all 'accountable authorities' of 'Commonwealth entities' 'to establish and maintain ... an appropriate system of risk oversight and management for the entity'.<sup>51</sup>

Risk-based regulation recognises that a regulator's enforcement resources are finite. It is premised on the assumption that risks to the achievement of regulatory objectives 'can be

<sup>48</sup> Ivec et al (n 9) 9.

<sup>49</sup> Braithwaite, Makkai and Braithwaite (n 25) 319. Braithwaite, Makkai and Braithwaite link the two pyramids together with an arrow only because they say education and persuasion about problems and strengths 'might well have the same delivery vehicle'. They do not believe that shame, for example, can be used effectively in conjunction with praise.

<sup>50</sup> See Julia Black, 'Risk-based Regulation: Choices, Practices and Lessons Being Learnt' in OECD (ed), *Risk and Regulatory Policy: Improving the Governance of Risk* (OECD, 2010) 185, 188–9.

<sup>51</sup> *Public Governance, Performance and Accountability Act 2013* (Cth) s 16(a).

reduced or managed but not eliminated'.<sup>52</sup> Elimination of all risk is seen as too expensive for government to achieve in practice, a hindrance to innovation because it imposes additional (and unnecessary) costs on business, and likely to lead only to higher costs for consumers in the long-term.<sup>53</sup> Different regulators have different regulatory objectives and confront different risks. However, risk-based regulation is intended to provide a 'transparent, systematic, and defensible'<sup>54</sup> way for regulators, utilising available evidence and economic and scientific decision-making tools, such as risk matrices and decision-trees,<sup>55</sup> to identify risks and prioritise them, and to allocate their limited resources accordingly.

Risk-based regulation is meant to be an ongoing and continuous process and one specific to the regulatory context and industry concerned, but it has been described as having up to six 'common' stages or 'core' elements.<sup>56</sup> These elements include:

- (1) Identification of the regulator's regulatory objectives and the risks it must control.<sup>57</sup>
- (2) Determination of the regulator's 'risk appetite' (eg, identification of the types of risk and amount of risk, including political risk, it will tolerate,<sup>58</sup> given its statutory obligations, guidance provided by government, resources, and stakeholder feedback<sup>59</sup>).
- (3) Risk assessment. This involves identification and evaluation of the potential harms or adverse impacts that regulated businesses might cause, and the costs and benefits of regulatory intervention. It also involves an assessment of the types of businesses that generate the greatest risks and the ability of market participants to manage those risks without regulatory intervention.<sup>60</sup>
- (4) Prioritisation of risks. This involves regulators scoring and ranking regulated businesses to determine which ones pose the most risk in light of the information gathered in stage 3. Different systems for scoring and ranking may be used depending on the regulated industry involved. They may include, for example, the use of 'traffic light models' (eg, green, yellow or red), or more detailed lists of assessment criteria.<sup>61</sup> Factors taken into account in assessments include business size and compliance history.
- (5) Resource allocation. The regulator determines how it will allocate its finite compliance and enforcement resources given the assessments it has undertaken.
- (6) Evaluation. The regulator determines whether it has been successful or otherwise in reducing risk and adjusts its resource allocation accordingly after again completing the analyses required in stages 1-4.

Risk-based regulation has been defined in multiple ways;<sup>62</sup> however, in this report, we define

---

<sup>52</sup> Freiberg (n 8) 455.

<sup>53</sup> Ibid, citing Productivity Commission, *Regulator Engagement with Small Business* (Research Report, September 2013) 271. See also Henry Rothstein, Olivier Borraz and Michael Huber, 'Risk and the Limits of Governance: Exploring Varied Patterns of Risk-based Governance Across Europe' (2013) 7(2) *Regulation & Governance* 215, 216–7.

<sup>54</sup> Julia Black and Robert Baldwin, 'Really Responsive Risk-Based Regulation' (2010) 32(2) *Law & Policy* 181, 181.

<sup>55</sup> Examples include cost-benefit analysis, risk matrices, and decision-trees.

<sup>56</sup> Black and Baldwin (n 54) 183–5; Freiberg (n 8) 455, 458–62; Productivity Commission (n 53) 275–7.

<sup>57</sup> Productivity Commission (n 53) 275.

<sup>58</sup> Black and Baldwin (n 54) 184.

<sup>59</sup> Productivity Commission (n 53) 275.

<sup>60</sup> Black and Baldwin (n 54) 184; *ibid*.

<sup>61</sup> Black and Baldwin (n 54) 185.

<sup>62</sup> See Black (n 50) 187–8.

risk-based regulation as ‘the targeting of enforcement resources on the basis of assessments of the risks that a regulated person or firm poses to the regulator’s objectives.’<sup>63</sup> In Chapter 3, we explain how risk-based regulation has been embedded in the ACMA’s compliance and enforcement policies.

---

<sup>63</sup> Black and Baldwin (n 54) 181.

## 2 Enforcement Mechanisms

Below we explain the differences between administrative, civil and criminal sanctions. Next, we briefly explain and categorise the seven discretionary mechanisms the ACMA may use to enforce the relevant Tel Act and TCPSS Act provisions. We also set out the mechanisms in their order of severity (ie, we begin with the least severe mechanism, gradually moving to the more severe). In addition, we explain an enforceable undertaking – a mechanism which does not fall neatly into the administrative, civil, or criminal sanction categories but is nevertheless an important tool used by the ACMA for securing compliance. We then summarise when the seven mechanisms are available to the ACMA for breaches of industry codes, industry standards, the select service provider rules, and the select carrier licence conditions.

### A Categorising Penalties

Sanctions for non-compliance have traditionally been classified into three different categories: administrative sanctions, civil sanctions, and criminal sanctions.<sup>64</sup> These are represented in Figure 3.



*Administrative sanctions* are sanctions ‘imposed by a regulatory authority or directly by the legislature without the intervention of a court or tribunal.’<sup>65</sup> *Civil sanctions* are sanctions imposed by a court of law at the conclusion of civil (ie, non-criminal) proceedings.<sup>66</sup> The civil proceedings are initiated by a person against another person usually with the intention of obtaining damages (ie, compensation) as a result of harm. *Criminal sanctions* are sanctions imposed by a court of law at the conclusion of criminal proceedings. Their aims are to punish and rehabilitate the wrongdoer and to deter and ‘denounce undesirable conduct and generally to protect society’.<sup>67</sup>

<sup>64</sup> Freiberg (n 8) 400. See also Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* (Report No 95, December 2002).

<sup>65</sup> Australian Law Reform Commission (n 64); Freiberg (n 8) 400, citing Australian Law Reform Commission (n 64) [2.63]–[2.64].

<sup>66</sup> Australian Law Reform Commission (n 64) [2.45].

<sup>67</sup> Freiberg (n 8) 400, 424.

In this classification scheme, administrative sanctions are seen as less severe than civil and criminal sanctions. Civil sanctions are seen as more severe than administrative sanctions. Criminal sanctions are seen as the most severe sanctions.

As Freiberg and others have highlighted, it can often be difficult to reliably classify the severity of penalties using the administrative, civil and criminal sanction ‘continuum’. This is, in part, because different sanctions can be used to achieve the same or similar purposes – purposes such as punishment, condemnation, deterrence, and retribution. Nevertheless, in this report, we adopt and apply the continuum for two reasons. First, the continuum provides a way to categorise and illustrate the severity of the sanctions the ACMA may use to enforce the Tel Act and TCPSS Act. Second the ACMA adopts a similar continuum in its compliance and enforcement policy documentation,<sup>68</sup> even though it disagrees with Freiberg’s conclusion that an enforceable undertaking is not an administrative sanction as we explain in section B(3) of Chapter 2 below.

## B The ACMA’s Enforcement Mechanisms

### 1 Administrative Mechanisms

The Tel Act and TCPSS Act provide the ACMA with up to four administrative mechanisms to enforce the different provisions of interest: formal warnings, directions to comply, infringement notices, and remedial directions. These are represented in Figure 4.



<sup>68</sup> See, eg, ‘Compliance and Enforcement Policy’, *Australian Communications and Media Authority* (Web page, 28 July 2023) <<https://www.acma.gov.au/compliance-and-enforcement-policy>> (the ACMA Compliance and Enforcement Policy).

A **formal warning** is a written warning that puts the recipient on notice that they are in breach of a rule (eg, a registered industry code of practice,<sup>69</sup> an industry standard,<sup>70</sup> a service provider rule,<sup>71</sup> a licence condition<sup>72</sup>) and the ACMA may take further enforcement action if non-compliance is not rectified.<sup>73</sup>

A **direction to comply** is an order in writing that a person must comply with a rule (eg, to comply with a registered industry code of practice<sup>74</sup> or the requirement to join the TIO<sup>75</sup>).

An **infringement notice** is a notice issued to a recipient where the ACMA 'has reasonable grounds to believe' they have 'contravened a particular civil penalty provision' of the Tel Act or the TCPSS Act,<sup>76</sup> and gives them the choice of 'resolving the matter immediately'<sup>77</sup> by paying a specified penalty or having the Federal Court decide the matter. If the recipient pays the penalty specified in the infringement notice, the liability for the alleged contravention is discharged and no civil penalty proceedings can be brought against them.<sup>78</sup> If the recipient does not pay the penalty, then the ACMA may bring civil penalty proceedings in the Federal Court.

If the ACMA brings proceedings because the notice recipient has refused to pay the specified penalty, the Federal Court will determine if the recipient has breached the Tel Act or TCPSS Act. Where a breach has occurred, the court may impose a financial penalty. The maximum penalty the Federal Court can award is much higher than the maximum penalty the ACMA can impose in an infringement notice.<sup>79</sup> Unless the Minister for Communications determines otherwise, the maximum penalty the ACMA can impose for a breach of 'a particular civil penalty provision' of the Tel Act or TCPSS Act is 60 penalty units.<sup>80</sup> The amount of a penalty unit is prescribed by the *Crimes Act 1914* (Cth) and at the time of writing is \$313 for offences committed on or after 1 July 2023. 60 penalty units equates to \$18,780.

Infringement notices may be issued when a carrier or service provider's conduct involves contravention of a civil penalty provision of the Tel Act or TCPSS Act.<sup>81</sup>

However, if a person's conduct involves breach of a carrier licence condition or a service provider rule (both civil penalty provisions) and one or more other civil penalty provisions (eg, breach of a direction to comply,<sup>82</sup> breach of the emergency call services determination<sup>83</sup>), the ACMA may issue an infringement notice only in relation to the other civil penalty provision. It

---

<sup>69</sup> Tel Act s 122.

<sup>70</sup> Ibid s 129.

<sup>71</sup> Ibid s 103.

<sup>72</sup> Ibid s 70.

<sup>73</sup> See the ACMA Compliance and Enforcement Policy (n 68).

<sup>74</sup> Tel Act s 121.

<sup>75</sup> TCPSS Act ss 128, 130. A direction to comply is only one mechanism the ACMA may use to enforce the TCPSS Act requirement to join the TIO. See the mechanisms to enforce the select service provider rules discussed in section B(3) of this chapter.

<sup>76</sup> Tel Act s 572E(1).

<sup>77</sup> Australian Communications and Media Authority, *Regulatory Guide No. 5: Infringement Notices* (Guidance No 5, February 2023) [2.2].

<sup>78</sup> Tel Act s 572J.

<sup>79</sup> The maximum penalties the ACMA and the Federal Court may impose vary depending on the statutory provision breached and the party in breach.

<sup>80</sup> Tel Act s 572G.

<sup>81</sup> Ibid s 572E(3). See also Explanatory Statement, *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022* (Cth) 1; Australian Communications and Media Authority, *Telecommunications (Infringement Notices) Guidelines 2022* (3 March 2022) [9.1].

<sup>82</sup> Tel Act s 121(1).

<sup>83</sup> TCPSS Act s 148(4).

cannot issue an infringement notice in relation to the breach of a carrier licence condition or service provider rule.

For breaches of the Tel Act or TCPSS Acts involving a breach of a carrier licence condition or a service provider rule (other than breaches of Part 1 of Schedules 1 and 2 of the Tel Act) infringement notices can be issued when the same conduct also breaches a provision that the ACMA has declared to be a 'listed infringement notice provision' and that provision has been listed for at least three months.<sup>84</sup> The ACMA may declare that certain provisions of the Tel Act and TCPSS Act, carrier licence conditions declared by the Minister under s 63 of the Tel Act,<sup>85</sup> and the ACMA-adopted service provider determinations<sup>86</sup> are 'listed infringement notice provisions'.<sup>87</sup>

Guidance about the declaration process and the types of provisions suitable for declaration can be gleaned from the Explanatory Statement the ACMA prepared for the Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth).<sup>88</sup> In that document, the ACMA said it consulted with the Department of Communications and the Attorney-General's Department and took into account guidance contained in *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011).<sup>89</sup> Drafted by the Attorney-General's Department, the Guide suggests that only certain statutory provisions are suitable for inclusion in infringement notice regimes. Suitable provisions include:

- strict or absolute liability offences
- 'relatively minor offences, where a high volume of contraventions is expected, and where a penalty must be imposed immediately to be effective' and
- those where 'an enforcement officer can easily make an assessment of guilt or innocence'.<sup>90</sup>

Infringement notices have been a feature of the telecommunications regulatory framework since the enactment of the *Telecommunications Legislation Amendment (Competition and Consumer Safeguards) Act 2010* (Cth).

A **remedial direction** is an order in writing made by the ACMA that a service provider or a carrier must 'take specified action directed towards ensuring that the provider does not contravene a rule, or is unlikely to contravene a rule, in the future'.<sup>91</sup> Examples of action required by the ACMA in a remedial direction include appointment of independent auditors, development of project plans to implement their recommendations, staff training, reporting, and implementation of compliance systems, practices and processes.<sup>92</sup>

---

<sup>84</sup> See Tel Act s 572E(5)–(7).

<sup>85</sup> The *Telecommunications (Carrier Licence Conditions – Telstra Corporation Limited) Declaration 2019* (Cth) and *Telecommunications (Carrier Licence Conditions – Telstra Infracore Limited) Declaration 2019* (Cth) were adopted pursuant to Tel Act s 63.

<sup>86</sup> See Chapter 2, section C(3) below, for more information about service provider determinations.

<sup>87</sup> Tel Act s 572E(7).

<sup>88</sup> See the Authorised Version Explanatory Statement Registered 25 March 2022 to F2022L00387 at p. 3.

<sup>89</sup> Explanatory Statement, *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth)* 3.

<sup>90</sup> Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guide, September 2011) 58. See also *ibid*.

<sup>91</sup> See, eg, Tel Act ss 69(2), 102(2).

<sup>92</sup> See, eg, Australian Communications and Media Authority, *Direction to Optus Internet Pty Ltd in relation to subsections 14(2), 14(3) and 15(1) of the Telecommunications Service Provider (NBN Service Migration) Determination 2018* (11 March 2022); Australian Communications and Media Authority, *Direction to Lycamobile*

## 2 Civil Mechanisms

As represented in Figure 5, the ACMA has up to two civil mechanisms to enforce the various provisions of interest: it is entitled to commence legal action in the Federal Court seeking the award of an injunction<sup>93</sup> and/or the imposition of a civil penalty.<sup>94</sup>



An **injunction** is an order made by the Federal Court at the ACMA's request that a person must stop engaging in conduct in breach of the Tel Act or TCPSS Act or must do something to become compliant with those Acts.<sup>95</sup>

A **civil penalty** is a monetary penalty for breaching a 'civil penalty provision' of the Tel Act or TCPSS Act. A civil penalty provision is a provision declared as a civil penalty provision in these Acts. An example of a civil penalty provision is the requirement to comply with emergency call services determinations under s 148.<sup>96</sup> In addition, the obligations to comply with a direction to comply with an industry code,<sup>97</sup> an industry standard,<sup>98</sup> a service provider rule<sup>99</sup> and a carrier licence condition<sup>100</sup> are all civil penalty provisions. However, compliance with a remedial direction to comply with the Tel Act and TCPSS Act provisions that are the focus of this report is not a civil penalty provision.<sup>101</sup>

The maximum penalty the Federal Court can impose for breach of a civil penalty provision depends on the party in breach and the provision contravened. The maximum penalty the Federal Court can impose on a corporation is much higher than the maximum penalty it can impose on individuals and other legal entities. For example, the requirements to comply with

---

*Pty Ltd in relation to the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 (May 2021).*

<sup>93</sup> Tel Act s 564(1).

<sup>94</sup> *Ibid* s 571(1).

<sup>95</sup> *Ibid* s 564.

<sup>96</sup> TCPSS Act s 148(4).

<sup>97</sup> Tel Act ss 121(2) and 121(4).

<sup>98</sup> *Ibid* ss 128(1) and 123(3).

<sup>99</sup> *Ibid* ss 101(1) and 101(3).

<sup>100</sup> *Ibid* ss 68(1) and 68(3).

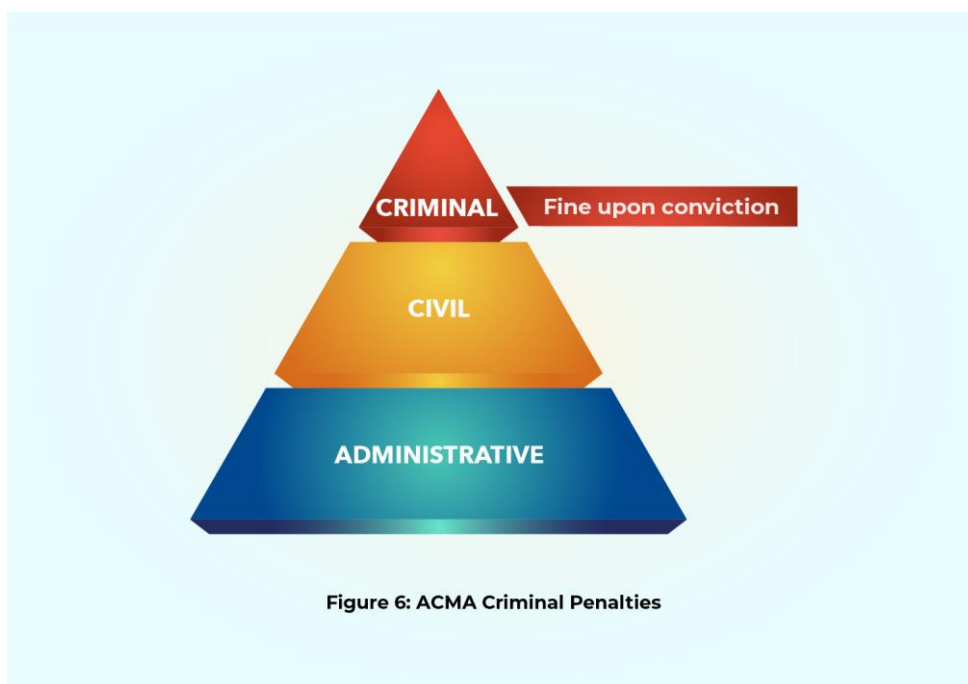
<sup>101</sup> *Ibid* ss 69(4) and 102(4).



the conditions of a carrier licence and applicable service provider rules can result in a maximum penalty of \$10 million for each contravention.<sup>102</sup> Contraventions of other civil penalty provisions attract a penalty of \$250,000 for each contravention.<sup>103</sup> A breach of the requirements to comply with the conditions of a carrier licence and applicable service provider rules by an individual and other legal entities cannot exceed \$50,000 for each contravention.<sup>104</sup> In all cases, if conduct constitutes a contravention of two or more civil penalty provisions, a person is not liable to more than one pecuniary penalty. If the conduct in question concerns a breach of the requirements to comply with the conditions of a carrier licence or applicable service provider rules and another civil penalty provision, the ACMA may only seek a penalty for contravention of that other civil penalty provision.<sup>105</sup>

### 3 Criminal Mechanisms

Section 531(1) of the Tel Act imposes an obligation on a person, including a corporate body, not to make an incorrect record in purported compliance with any record-keeping rules adopted by the ACMA.<sup>106</sup> If a person breaches that obligation, they have committed a criminal offence, and the ACMA may refer the alleged offence to the Commonwealth Director of Public Prosecutions. If the Commonwealth Director agrees to prosecute the matter and the relevant person is found guilty of the offence, the person may receive a **fine upon conviction** not exceeding 100 penalty units.<sup>107</sup> This is represented in Figure 6.



Making incorrect records in purported compliance with the Telecommunications (Consumer Complaints) Record-Keeping Rules 2018 (Cth) could therefore lead to a fine upon conviction.

<sup>102</sup> Ibid s 570(3)(a).

<sup>103</sup> Ibid s 570(3)(b).

<sup>104</sup> Ibid s 570(4)(b).

<sup>105</sup> Ibid ss 570(5) and (6).

<sup>106</sup> See Tel Act s 529 for the ACMA's power to make record-keeping rules.

<sup>107</sup> See Tel Act s 531(2).

A fine upon conviction is a monetary penalty imposed by a court for commission of an offence under Commonwealth law. As for infringement fines, the amount of a penalty unit is prescribed by the *Crimes Act 1914* (Cth) and at the time of writing is \$313 for offences committed on or after 1 July 2023. 100 penalty units equates to \$31,300.

## 4 Enforceable Undertakings

An **enforceable undertaking** is ‘a negotiated binding agreement that can be enforced in court by the ACMA’.<sup>108</sup> It is a written promise made by a person (and accepted by the ACMA) that they will take or refrain from taking specified action to comply with the Tel Act or TCPSS Act; or take specified action to ensure they do not contravene these Acts in the future.<sup>109</sup> If an enforceable undertaking is breached, the ACMA may bring legal proceedings in the Federal Court and ask the court to make one or more orders. These orders may direct the person to comply with the undertaking; to pay the Commonwealth a sum of money (up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach); and to compensate people who have suffered loss or damage.<sup>110</sup>

Enforceable undertakings have been a feature of the telecommunications regulatory framework since 2005 following the enactment of the *Telecommunications Legislation Amendment (Competition and Consumer Issues) Act 2005* (Cth).

The ACMA treats an enforceable undertaking as another type of administrative sanction. For example, it has stated it may accept an enforceable undertaking instead of issuing a remedial direction. Further, the ACMA has stated it may accept an enforceable undertaking instead of seeking civil penalties or injunctions in the Federal Court. It has also suggested that acceptable enforceable undertakings may induce the ACMA not to take any administrative or civil enforcement action.<sup>111</sup>

However, it should be noted that not everyone sees enforceable undertakings as a type of administrative sanction or as an enforcement tool. This is because the ACMA cannot impose enforceable undertakings or force providers to give enforceable undertakings. Submitting enforceable undertakings is entirely voluntary. For example, academic Arie Freiberg categorises them as a tool of ‘transactional regulation’ – the government’s use of agreements with non-governmental actors to achieve public policy objectives.<sup>112</sup>

The ACMA has said the advantages of enforceable undertakings are:

- tailored and flexible resolution of the issues of concern
- an opportunity for the undertaking party to be involved in the resolution of a matter
- a more cost-effective and timely outcome compared to litigation.<sup>113</sup>

---

<sup>108</sup> Australian Communications and Media Authority, *Regulatory Guide No. 1: Enforceable Undertakings* (Guidance No 1, February 2023) [2.1].

<sup>109</sup> Tel Act s 572B.

<sup>110</sup> Ibid s 572C.

<sup>111</sup> Australian Communications and Media Authority (n 108). See also Australian Communications and Media Authority (n 68).

<sup>112</sup> Freiberg (n 8) 276, 295–9.

<sup>113</sup> Australian Communications and Media Authority (n 108) [2.12].

Regulatory scholars have cited these advantages too.<sup>114</sup> However, enforceable undertakings have also been criticised because:

- their terms can be vague or imprecise, making them difficult to enforce
- they enable regulators to treat similarly situated parties inconsistently
- individual consumers and/or consumer organisations have no input into the terms of enforceable undertakings
- bargaining power imbalances may exist between regulators and smaller industry participants.<sup>115</sup>

An example of an enforceable undertaking is the one the ACMA accepted in March 2022 from TPG Internet Pty Limited (TPG). In that undertaking, TPG agreed to:

- 'implement and maintain effective systems, processes and practices for ensuring compliance with' two provisions of the Telecommunications Service Provider (NBN Service Migration) Determination 2018 (Cth): subsection 14(3), which relates to line capability assessment, and subsection 15(2), which prohibits charging a consumer for an NBN service in specified circumstances ('the two provisions');
- 'implement and maintain processes to ensure that material changes to the systems relied on to ensure compliance with' the two provisions were 'signed off by relevant internal TPG Internet stakeholders before being implemented, which must include an executive'; and
- appoint an independent person to audit and report in writing on: (1) the extent of TPG's compliance with the two provisions, (2) recommendations as to how TPG could improve its systems, processes, and practices for ensuring compliance with the two provisions, and (3) the implementation of a customer remediation program TPG had adopted before giving the enforceable undertaking.<sup>116</sup>

## C Which Mechanisms May be Used When?

Below we explain the different actions the ACMA is empowered to take if a telecommunications company breaches industry codes, industry standards, the select service provider rules, or the select carrier licence conditions.

### 1 Industry Codes

There are 21 Comms Alliance codes currently registered with the ACMA,<sup>117</sup> only three of which are classified by Comms Alliance as 'consumer' codes. The three consumer codes are:

- C637:2019 Mobile Premium Services (MPS) Code Incorporating Variation No 1/2021
- C628:2019 Telecommunications Consumer Protections Code Incorporating Variation No 1/2022

---

<sup>114</sup> Freiberg (n 8) 298. See also Karen Yeung, *Securing Compliance: A Principled Approach* (Hart, 2004); Marina Nehme, 'Enforceable Undertakings' Practices Across Australian Regulators: Lesson Learned' (2021) 21(1) *Journal of Corporate Law Studies* 283.

<sup>115</sup> Freiberg (n 8) 298; Yeung *ibid*; Nehme *ibid*.

<sup>116</sup> See TPG Internet Pty Ltd, *Enforceable Undertaking Given to the Australian Communications and Media Authority by TPG Internet Pty Ltd (CAN 068 383 737) under section 572B of the Telecommunications Act 1997 (Cth)* (Enforceable undertaking, March 2022).

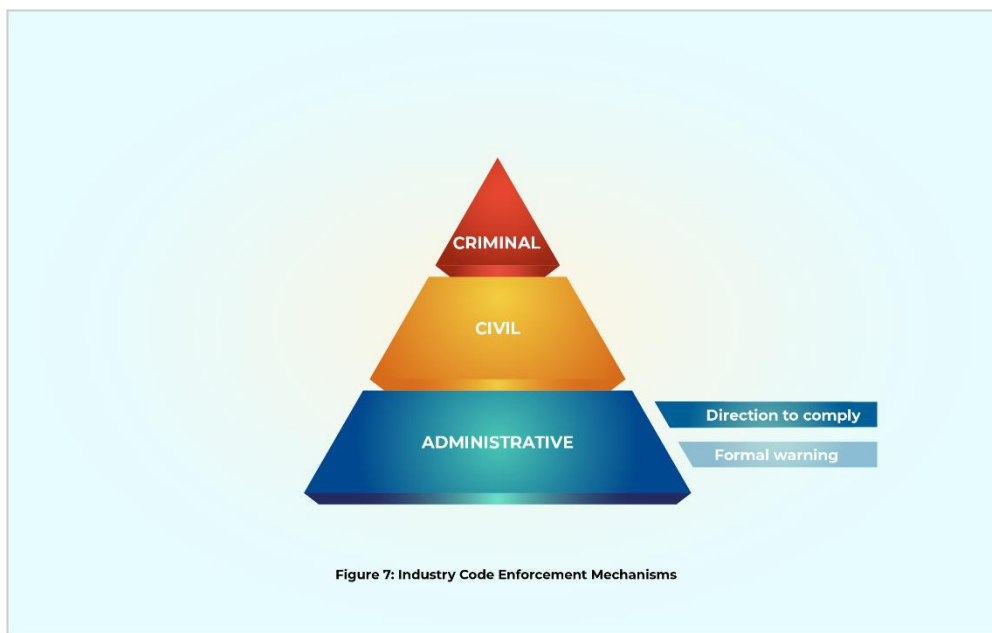
<sup>117</sup> See Annex A for the full list.

- C625:2020 Information on Accessibility Features for Telephone Equipment.

Two codes classified by Comms Alliance as ‘operational’ codes that are also particularly important to the consumer protection framework are:

- C555:2020 Integrated Public Number Database
- C661:2022 Reducing Scam Calls and Scam SMS.

Section 106 of the Tel Act states that compliance with an industry code registered by the ACMA is ‘voluntary’. However, if an industry participant breaches an applicable code, the ACMA may issue a formal warning<sup>118</sup> or a direction to comply with the code.<sup>119</sup> Figure 7 presents an illustration of these enforcement mechanisms available for breach of an industry code.



If the ACMA issues a formal warning and an industry participant fails to heed it, the ACMA may issue a direction to comply.

If an industry participant fails to comply with a direction to comply, the ACMA may:

- issue an infringement notice (within 12 months of the alleged breach) for 60 penalty units per contravention to a body corporate or for 12 penalty units per contravention to a person other than a body corporate<sup>120</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court and/or

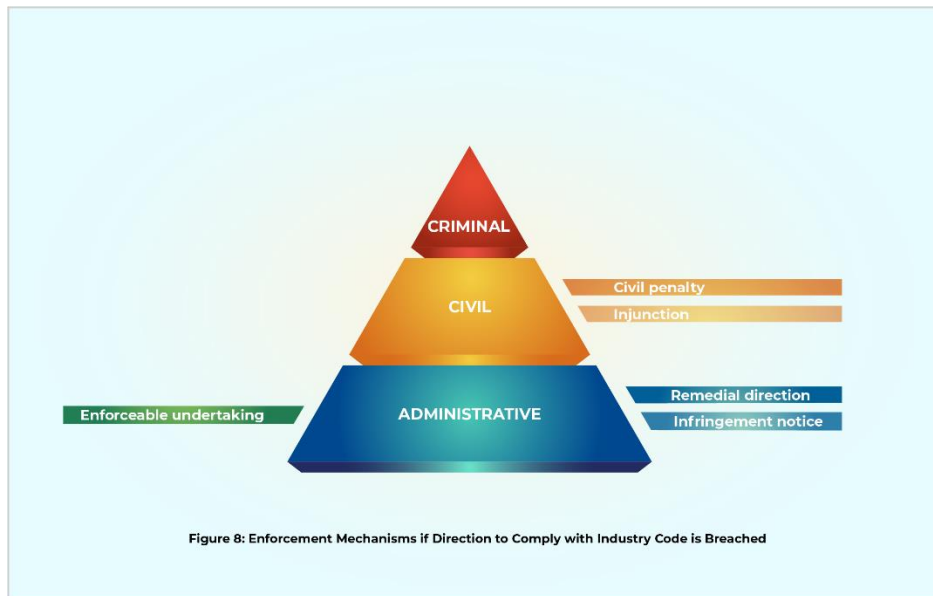
<sup>118</sup> Tel Act s 122.

<sup>119</sup> Ibid s 121.

<sup>120</sup> See *ibid* s 572G(1)(b). A direction to comply is a ‘civil penalty provision’ for the purposes of s 572E(1) of the Tel Act. See at ss 121(2), 121(4). Breach of a direction to comply also amounts to a breach of s 68 and s 101 of the Tel Act. However, an infringement notice can only be issued in relation to the breach of the direction to comply: see at s 572E(3). See also ‘Infringement Notices for Breaking the Telco Rules’, *Australian Communications and Media Authority* (Web page, 03 July 2023) <<https://www.acma.gov.au/infringement-notices-breaking-telco-rules>>.

- seek an order from the Federal Court requiring payment of a civil penalty up to \$250,000 from a corporation and \$50,000 from a person other than body corporate) for each contravention.<sup>121</sup>

Figure 8 illustrates the enforcement mechanisms available for breach of a direction to comply with an industry code.



If the ACMA issues an infringement notice and the industry participant pays the specified penalty, the ACMA cannot apply to the Federal Court for a civil penalty. However, it can accept an enforceable undertaking for the same breach. In theory, seeking an injunction would also be possible but would most likely not be appropriate.<sup>122</sup>

## 2 Industry Standards

Industry standards are standards adopted by the ACMA in accordance with ss 123, 124, 125 and 125AA of the Tel Act. At the time of writing, four relevant industry standards are in force:

- the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020
- the Telecommunications (NBN Continuity of Service) Industry Standard 2018
- the Telecommunications (NBN Consumer Information) Industry Standard 2018
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018.<sup>123</sup>

If an industry standard is breached, the ACMA may:

- issue a formal warning<sup>124</sup>

<sup>121</sup> Tel Act s 570(3)(b) and 570(4)(b). A breach of a direction to comply also amounts to a breach of s 68 and s 101 of the Tel Act. However, s 570(6) prevents the ACMA from initiating civil proceedings for both breaches. It can bring proceedings only in relation to the breach of the direction to comply.

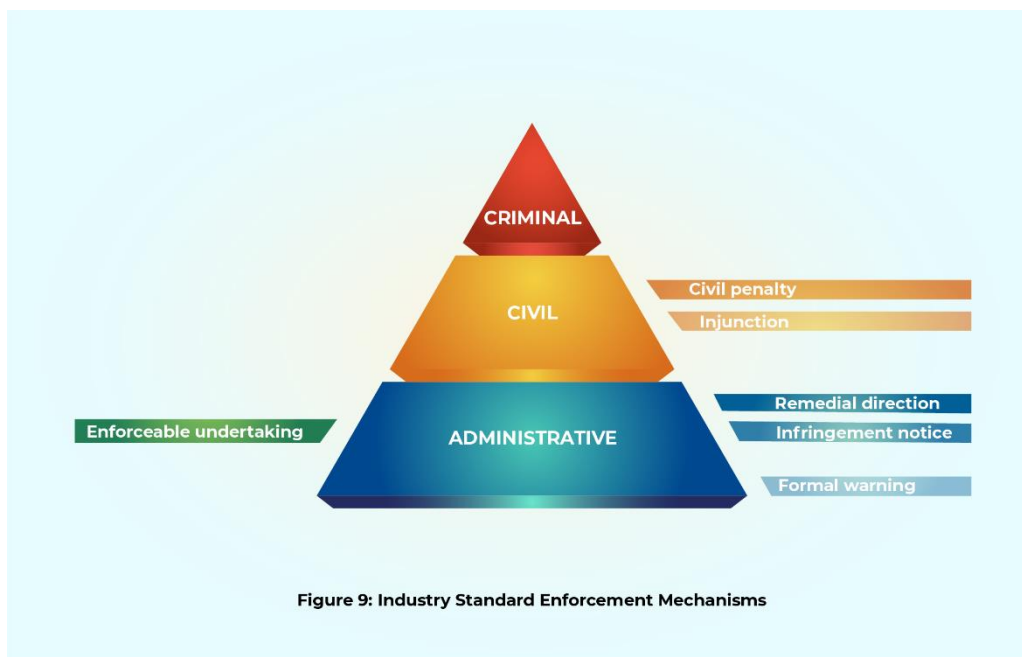
<sup>122</sup> The same applies to the application of injunctions in relation to industry standards, service provider rules and carrier licence conditions discussed in sections 3(C)(2), (3) and (4) below.

<sup>123</sup> The ACMA adopted the Telecommunications (Financial Hardship) Industry Standard on 1 February 2024. The standard comes into force on 29 March 2024. As the report covers the period between 1 January 2010 and 30 June 2023, we make no further reference to this standard.

<sup>124</sup> Tel Act s 129(2).

- issue an infringement notice (within 12 months of the alleged breach) for 60 penalty units per contravention to a body corporate or for 12 penalty units per contravention to a person other than a body corporate<sup>125</sup>
- issue a remedial direction<sup>126</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court and/or
- seek an order from the Federal Court requiring payment of a civil penalty up to \$250,000 by a corporation and up to \$50,000 by a person other than a body corporate for each contravention.<sup>127</sup>

Figure 9 presents an illustration of these enforcement mechanisms available for breach of an industry standard.



<sup>125</sup> See *ibid* 572G(1)(b). An industry standard is a civil penalty provision: at s 128(3). In addition, breach of the requirement in s 128 to comply with an industry standard may amount to a breach of ss 68 and 101 of the Tel Act. However, an infringement notice can only be issued in relation to the breach of the industry standard: at s 572E(3). Although on its webpage, 'Infringement Notices for Breaking the Telco Rules' (see n 120), the ACMA does not say breach of an industry standard is a reason for an infringement notice, the ACMA has issued infringement notices for breaches of industry standards. See, eg, the infringement notice it issued against Circles.Life for breaches of the *Telecommunications (Mobile Number Pre-porting Additional Identity Verification) Industry Standard 2020* (Cth): Australian Communications and Media Authority, *Infringement Notice* (6 July 2022) <https://www.acma.gov.au/sites/default/files/2022-08/Infringement%20Notice%20-%20Circles.PDF>.

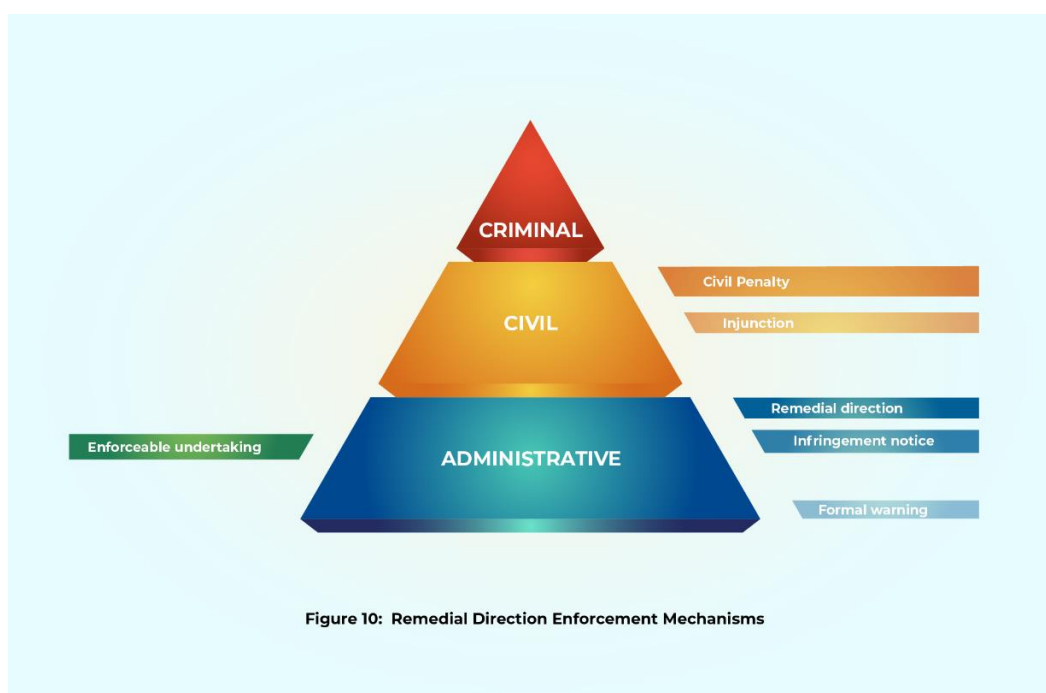
<sup>126</sup> The ACMA is able to issue a remedial direction as a result of the combination of the following provisions: s 102(2) enables the ACMA to issue a remedial direction for breach of a service provider rule; s 98 says that the rules in Schedule 2 are service provider rules; cl 1 of Schedule 2 requires a service provider to comply with the Act; s 128 requires participants in a section of the industry to comply with industry standards that apply to that section of the industry.

<sup>127</sup> Tel Act ss 570(3)(b) and (4)(b). A breach of an industry standard also amounts to a breach of s 68 (the requirement to comply with carrier licence conditions) and s 101 (the requirement to comply with service provider rules). Breaches of carrier licence conditions and the service provider rules may attract penalties of up to \$10 million: at s 570(3)(a). However, Tel Act s 570(6) prevents the ACMA from initiating civil proceedings for both a breach of an industry standard and a breach of a licence condition or service provider rule. It can bring proceedings only in relation to the breach of the industry standard: at s 570(6).

If a service provider fails to comply with a remedial direction, the ACMA may:

- issue a formal warning
- issue an infringement notice (within 12 months of the alleged breach) for 60 penalty units per contravention to a body corporate or for 12 penalty units per contravention to a person other than a body corporate<sup>128</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court
- seek an order from the Federal Court requiring payment of a civil penalty up to \$10 million (for corporations) and \$50,000 (for persons other than body corporates) for each contravention.<sup>129</sup>

Figure 10 illustrates the enforcement mechanisms available for breach of a remedial direction.



### 3 Select Service Provider Rules

If a select service provider rule is breached, the ACMA may:

- issue a formal warning<sup>130</sup>

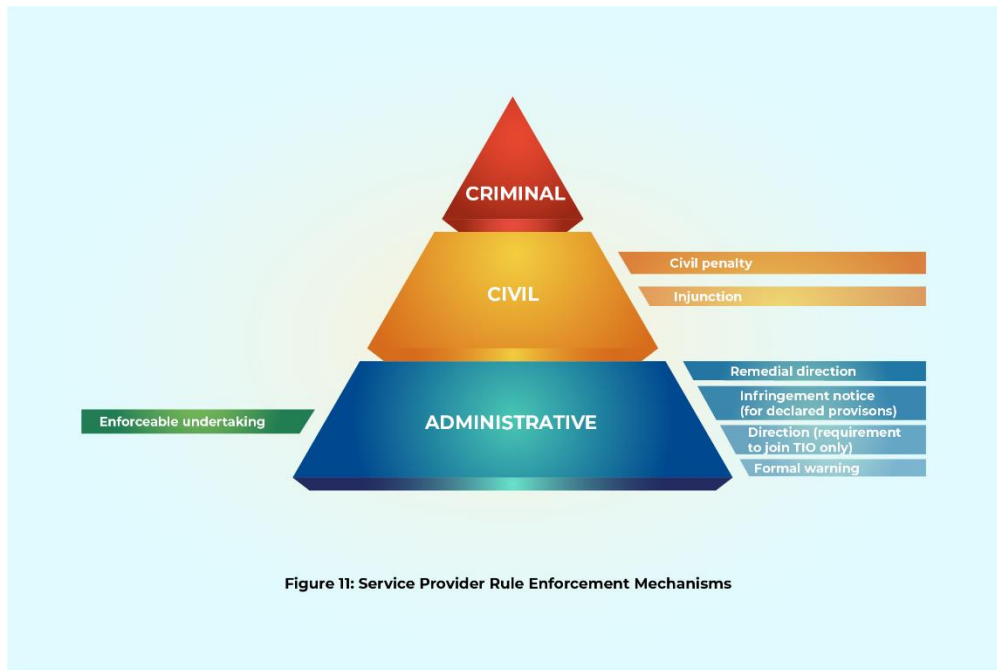
<sup>128</sup> Non-compliance with a remedial direction is a breach of ss 69(4) and 102(4) of the Tel Act and consequently a breach of Part 1 of Schedules 1 and 2 of the Tel Act respectively. The ACMA has also declared ss 69(4) and 102(4) to be listed infringement notice provisions. See *Telecommunications Listed Infringement Notice Provisions) Declaration 2022* (Cth).

<sup>129</sup> Breach of s 101(1) of the Tel Act (the requirement to comply with service provider rules) is a civil penalty provision but non-compliance with a remedial direction issued under s 102(2) of the Tel Act is not. Hence s 570(6) of the Tel Act does not apply and the ACMA can bring actions for the breach of the remedial direction as well as for breach of the industry standard itself. The same applies to the breach of a remedial direction in the context of the service provider rules and carrier licence conditions discussed in sections 3(C)(3) and (4) below.

<sup>130</sup> Ibid s 103(2).

- issue a remedial direction<sup>131</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court and/or
- seek an order from the Federal Court requiring payment of a civil penalty up to \$10 million<sup>132</sup> (for corporations) and \$50,000 (for persons other than body corporates) for each contravention.

Figure 11 presents an illustration of these enforcement mechanisms available for breach of one of the select service provider rules.



For some select service provider rules, the ACMA has the additional option of issuing an infringement notice (within 12 months of the alleged breach). The ACMA may issue an infringement notice:

- when the contravention involves a breach of Schedule 2 of the Tel Act (other than Part 1 of Schedule 2),<sup>133</sup> the TCPSS Act and related regulations, or a service provider determination made by the ACMA or the Minister;
- the ACMA has declared the specific provision to be a listed infringement notice provision; and
- the provision has been a listed infringement notice provision for at least three months before the day on which the alleged breach occurred.

As of the date of writing, the ACMA has declared only the following provisions of the select service provider rules are listed infringement notice provisions:

- subclause 10(2) of Part 4 (Integrated Public Number Database) of Schedule 2, which relates to information carriage service providers must give to Telstra

<sup>131</sup> Ibid s 102.

<sup>132</sup> Ibid s 570(3)(a). Compliance with the service provider rules is a civil penalty provision: at s 101(1).

<sup>133</sup> Here we are referring to the Schedule 2 provisions the ACMA may enforce. The ACMA does not have power to enforce all provisions of Schedule 2 of the Tel Act.



- subclause 11(2) of Part 4 (Integrated Public Number Database) of Schedule 2, which relates to information carriage service providers must give to another person or association
- subsection 521(3) of the Tel Act (the obligation to comply with the ACMA requests for information and/or documentation)
- section 530 of the Tel Act (compliance with record-keeping rules)
- section 132 of the TCPSS Act (members of scheme must comply with TIO scheme)
- certain provisions of the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* (Cth), the *Telecommunications Service Provider (NBN Service Migration) Determination 2018* (Cth), the *Telecommunications Service Provider (International Mobile Roaming) Determination 2019* (Cth), and the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (Cth).<sup>134</sup>

In the Explanatory Statement accompanying its declaration, the ACMA said it believed the declared Tel Act and TCPSS Act provisions were 'suitable for enforcement via the infringement notice regime ... because the physical elements of the contraventions are considered to be clear cut, and compliance is readily ascertainable.'<sup>135</sup>

In addition to the service provider rule enforcement mechanisms outlined above, if the provision breached concerns an eligible carriage service provider's obligation to join the TIO, the ACMA may issue a direction to a carriage service provider to join the TIO.<sup>136</sup> If a service provider fails to comply with such a direction, the ACMA may:

- issue a formal warning
- issue an infringement notice<sup>137</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court
- seek an order from the Federal Court requiring payment of a civil penalty up to \$10 million (for corporations) and \$50,000 (for persons other than body corporates) for each contravention.<sup>138</sup>

Figure 12 shows the enforcement mechanisms available for breach of a direction to join the TIO.

---

<sup>134</sup> For the complete list, see *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022* (Cth).

<sup>135</sup> Explanatory Statement, *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022* (Cth) 3.

<sup>136</sup> TCPSS Act s 130.

<sup>137</sup> The ACMA has declared that s 130(2) of the TCPSS Act is a listed infringement notice provision: see *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022* (Cth).

<sup>138</sup> Tel Act s 570(3)(a). Compliance with the service provider rules is a civil penalty provision: at s 101(1).



Finally, the ACMA may refer any person, including a corporate body, who breaches s 531 of the Tel Act — the obligation not to make an incorrect record in purported compliance of record-keeping rules adopted by the ACMA — to the Commonwealth Director of Public Prosecutions for the prosecution of an offence. A person, including a body corporate, in breach of s 531 commits an offence punishable on conviction by a fine not exceeding 100 penalty units.<sup>139</sup>

#### 4 Select Carrier Licence Conditions

If Telstra or another carrier fails to comply with one or more of the select carrier conditions, the ACMA may:

- issue a formal warning<sup>140</sup>
- issue a remedial direction<sup>141</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court
- seek an order from the Federal Court requiring payment of a civil penalty up to \$10 million (for corporations) and up to \$50,000 (for persons other than body corporates) for each contravention.<sup>142</sup>

For some select carrier conditions, the ACMA has the additional option of issuing an infringement notice (within 12 months of the alleged breach). The ACMA may issue an infringement notice for breach of a carrier licence condition set out in a Tel Act provision (other than Part 1 of Schedule 1) or declared by the Minister under s 63 of the Tel Act if:

<sup>139</sup> Tel Act s 531(2). Section 531 does not specifically exclude other enforcement action but the ACMA does not refer to other types of enforcement action for breach of s 531(1) on its website. See, eg, the ACMA, 'Report How You Comply with CSG Recordkeeping' <<https://www.acma.gov.au/report-how-you-comply-csg-recordkeeping>>.

<sup>140</sup> Tel Act s 70(1).

<sup>141</sup> Ibid s 69.

<sup>142</sup> Ibid s 570(3)(a). Breach of s 68(1) of the Tel Act is a civil penalty provision.

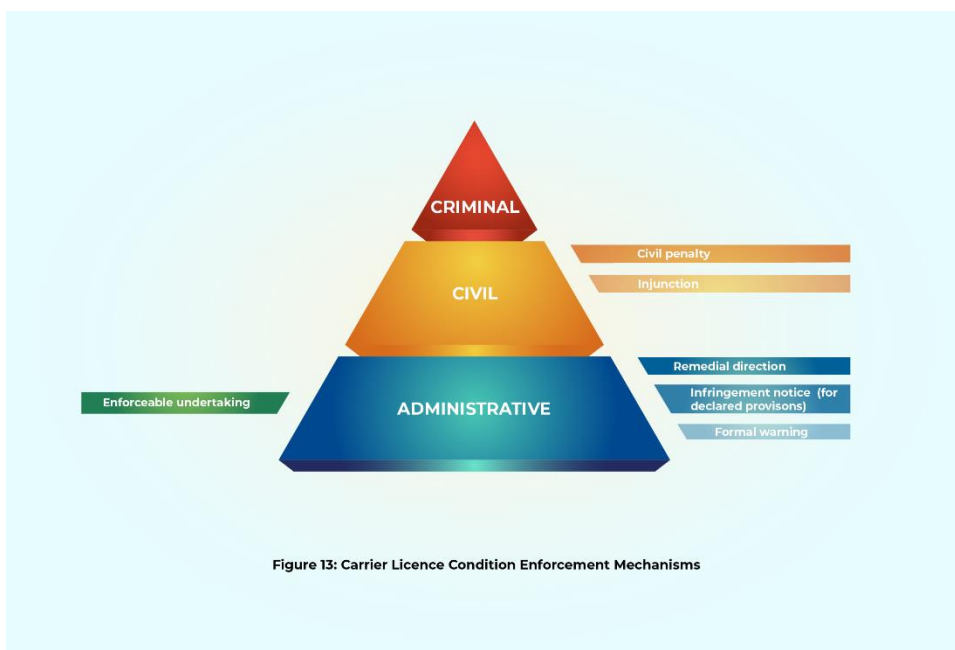
- the ACMA has declared the specific provision to be a listed infringement notice provision; and
- the provision has been a listed infringement notice provision for at least 3 months before the day on which the alleged breach occurred.

At the date of writing, the ACMA has declared the following select carrier licence conditions to be listed infringement notice provisions:

- subsection 521(3) of the Tel Act (the obligation to comply with the ACMA requests for information and/or documentation)
- section 530 of the Tel Act (compliance with record-keeping rules).<sup>143</sup>

The ACMA has not declared the carrier licence conditions in the *Telecommunications (Carrier Licence Conditions – Telstra Corporation Limited) Declaration (Cth)* that now apply to Telstra Limited because of s 63A of the Tel Act or the *Telecommunications (Carrier Licence Conditions – Telstra Infracore Limited) Declaration 2019 (Cth)* to be listed infringement notice provisions. When making its decision to declare the two carrier licence conditions listed above, the ACMA took into account the factors in the Attorney-General’s Department’s *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) discussed in section B(1) of Chapter 2, above.<sup>144</sup> It also said it believed they were ‘suitable for enforcement via the infringement notice regime ... because the physical elements of the contraventions are considered to be clear cut, and compliance is readily ascertainable.’<sup>145</sup>

Figure 13 presents an illustration of these enforcement mechanisms available for breach of one of the select carrier licence conditions.



<sup>143</sup> See *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth)*.

<sup>144</sup> Explanatory Statement, *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth)* 3; Attorney-General’s Department (n 85).

<sup>145</sup> Explanatory Statement, *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth)* (Authorised Version Explanatory Statement Registered 25 March 2022 to F2022L00387) 3.

If a carrier fails to comply with a remedial direction, the ACMA may:

- issue a formal warning
- issue an infringement notice (within 12 months of the alleged breach) for 60 penalty units per contravention to a body corporate and 12 penalty units per contravention to a person other than a body corporate <sup>146</sup>
- accept an enforceable undertaking
- seek an injunction from the Federal Court
- seek an order from the Federal Court requiring payment of a civil penalty up to \$10 million) and \$50,000 (for persons other than body corporates) for each contravention.<sup>147</sup>

Finally, like the select service provider, the ACMA may refer to the Commonwealth Director of Public Prosecutions for prosecution any person who breaches the specific provision concerning incorrect records in s 531.

---

<sup>146</sup> This is because the ACMA has also declared subsection 69(4) of the Tel Act (obligation to comply with a remedial direction) to be a listed infringement notice provision. For the complete list, see *Telecommunications (Listed Infringement Notice Provisions) Declaration 2022 (Cth)*.

<sup>147</sup> Breach of s 68(1) of the Tel Act is a civil penalty provision but non-compliance with s 69(4) of the Tel Act is not. Hence s 570(6) of the Tel Act does not apply.

## 3 Approach to Enforcement

If a carrier or service provider breaches industry codes, industry standards, select service provider rules, and/or select carrier licence conditions, the ACMA is empowered to take the various actions described in Chapter 2. However, the ACMA is not required to take any enforcement action or accept an enforceable undertaking even if a carrier or service provider breaches one or more of these rules. The decision whether and how to enforce is entirely up to the ACMA, provided it acts in accordance with Australian administrative law and the Tel Act and TCPSS Act.

Despite this, some general guidance as to whether and how the ACMA will enforce industry codes, industry standards, select service provider rules, and select carrier licence conditions can be found in the ACMA's Compliance and Enforcement Policy,<sup>148</sup> its Regulatory Guides,<sup>149</sup> and the Telecommunications (Infringement Notices) Guidelines 2022 (Cth).

We begin by explaining the ACMA's general approach to compliance and enforcement and the general factors it says influence its enforcement decisions. Next we highlight the additional factors that the ACMA says it considers before issuing an infringement notice, accepting an enforceable undertaking, or issuing a remedial direction. We then compare the ACMA's approach to responsiveness and the factors it takes into account against the concept of responsive regulation outlined in section A of Chapter 1 above. This section of the report concludes with discussion of the ACMA's enforcement priorities as they will have influenced the allocation of the ACMA's compliance and enforcement resources.

### A General Compliance and Enforcement Approach and Factors Influencing the ACMA's Approach

In its Compliance and Enforcement Policy, the ACMA states it has adopted a 'graduated and strategic risk-based approach' to compliance and enforcement – an approach that has been influenced at least in part by the statement of regulatory policy in s 4 of the Tel Act, which states that:

The Parliament intends that telecommunications be regulated in a manner that:  
(a) promotes the greatest practicable use of industry self-regulation; and  
(b) does not impose undue financial and administrative burdens on participants in the Australian telecommunications sector;  
but does not compromise the effectiveness of regulation in achieving the objects [of the Act].

The ACMA's approach has also been influenced by obligations of its chair under the *Public Governance, Performance and Accountability Act 2013* (Cth). As mentioned in section B of Chapter 1 above, all 'accountable authorities' of 'Commonwealth entities' are required 'to establish and maintain ... an appropriate system of risk oversight and management for the

---

<sup>148</sup> The ACMA Compliance and Enforcement Policy (n 68).

<sup>149</sup> See, eg, Australian Communications and Media Authority (n 108); Australian Communications and Media Authority, *Regulatory Guide No. 4: Remedial Directions* (Guidance, February 2023); Australian Communications and Media Authority (n 77).

entity'.<sup>150</sup> For the purposes of the Act, the Chair of the ACMA is an accountable authority<sup>151</sup> and the ACMA is a Commonwealth entity.<sup>152</sup>

The ACMA emphasises, for example, that it wants to 'foster industry compliance with, and contribution to, the regulatory framework without imposing undue financial or administrative burdens'. It also says enforcement action will be 'commensurate with the seriousness of the breach and the level of harm,' and the ACMA will 'generally use the minimum power or intervention necessary to achieve the desired result, which, in many cases, is compliance with the relevant obligation.'<sup>153</sup> This means that if its efforts to encourage voluntary compliance – efforts that involve 'educating and informing'<sup>154</sup> – have failed, the ACMA will consider informal resolution before resorting to administrative and civil enforcement mechanisms. Informal resolution involves approaching the regulated entity with 'issues of concern' and encouraging them to address an issue. It may also involve accepting a non-legally binding written commitment that steps 'will be taken to rectify non-compliance'.<sup>155</sup>

The ACMA's precise compliance and enforcement response, however, will be influenced by a range of factors.

In addition to all relevant facts,<sup>156</sup> these factors include:

- (1) the relevant regulatory objective;
- (2) whether the conduct was deliberate, inadvertent or reckless;
- (3) whether the conduct has caused, or may cause, detriment to another person, and the nature, seriousness and extent of that detriment;
- (4) whether the conduct involved indicates systemic issues which may pose ongoing compliance or enforcement issues;
- (5) whether the regulated entity or person has been the subject of prior compliance or enforcement action and the outcome of that action;
- (6) the personal and general educative/deterrent effect of acting;
- (7) the seniority and level of experience of the person/s involved in the conduct;
- (8) what, if any, action has been taken to remedy and address the consequences of the conduct;
- (9) whether the subject of the investigation has co-operated with [the ACMA];
- (10) whether the issues involved require urgent action or invention by [the ACMA].<sup>157</sup>

---

<sup>150</sup> *Public Governance, Performance and Accountability Act 2013* (Cth) s 16(a).

<sup>151</sup> See *Australian Communications and Media Authority Act 2005* (Cth) s 6(2)(b).

<sup>152</sup> Commonwealth entities include 'listed entities'. See *Public Governance, Performance and Accountability Act 2013* (Cth) s 10(c). See also *Australian Communications and Media Authority Act 2005* (Cth) s 6(2)(b) which states the ACMA is a listed entity for the purposes of the *Public Governance, Performance and Accountability Act 2013* (Cth).

<sup>153</sup> The ACMA Compliance and Enforcement Policy (n 68).

<sup>154</sup> Examples include publishing guidance documents, formal and informal consultation, and publication of investigation outcomes.

<sup>155</sup> The ACMA Compliance and Enforcement Policy (n 68).

<sup>156</sup> *Ibid.*

<sup>157</sup> *Ibid.*

The ACMA uses the following 'compliance pyramid' to illustrate its current approach:<sup>158</sup>

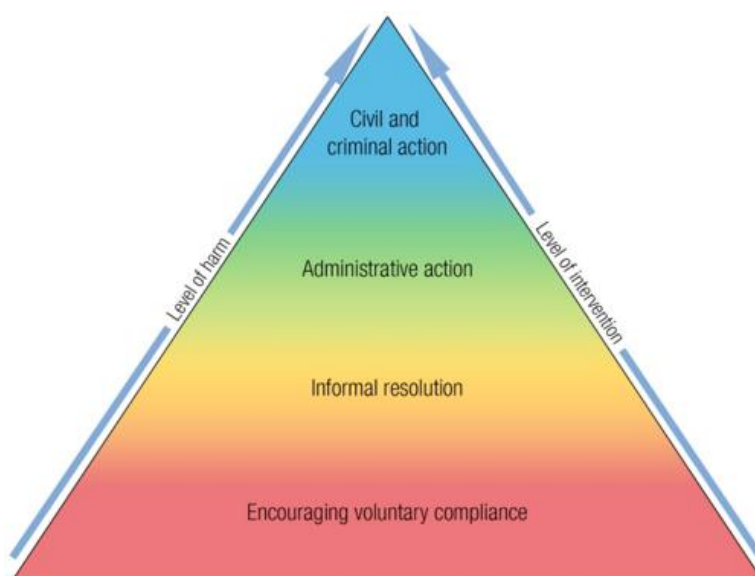


Figure 14: the ACMA's Compliance Pyramid

In section C of Chapter 4 below, we provide some examples of how the ACMA has exercised its enforcement powers to enforce various consumer protection-related provisions that are the focus of this report.

In Figure 15, we illustrate how ACMA's own 'compliance pyramid' maps onto the enforcement pyramids for the select consumer protection provisions that are the focus of this report, using the enforcement of industry standards as an example. We do so to highlight that ACMA's preferred approach is to seek to encourage voluntary compliance and informal resolution (shown as the first two bases of the pyramid), in the first instance, before utilising the enforcement mechanisms explained in the previous chapter to achieve compliance. Thus, if a provider has breached an industry standard, ACMA will first try to bring about compliance informally rather than issuing a formal warning, an infringement notice, and a remedial direction, or applying to the Federal Court for a civil penalty or an injunction. If the matter cannot be resolved informally, ACMA will then consider whether a formal warning will bring about compliance. If not, ACMA may decide to issue an infringement notice and/or a remedial direction. If neither tool yields success, ACMA might decide to escalate up the pyramid by pursuing a civil penalty and/or an injunction. ACMA's actual response in the event of breach of an industry standard will depend on the range of factors set out earlier in this section, but Figure 15 provides an indicator of how it is likely to use its enforcement mechanisms.

<sup>158</sup> This version of the pyramid is taken from the August 2010 version of the ACMA's *Compliance and Enforcement Policy*: see Australian Communications and Media Authority, *Compliance and Enforcement Policy* (Policy, August 2010). A copy can currently be found here: <<https://reia.com.au/wp-content/uploads/2017/10/Compliance-Guide.pdf>>. A later version with lower resolution and different colours (but the same content) is available through the website version: see the ACMA Compliance and Enforcement Policy (n 68).

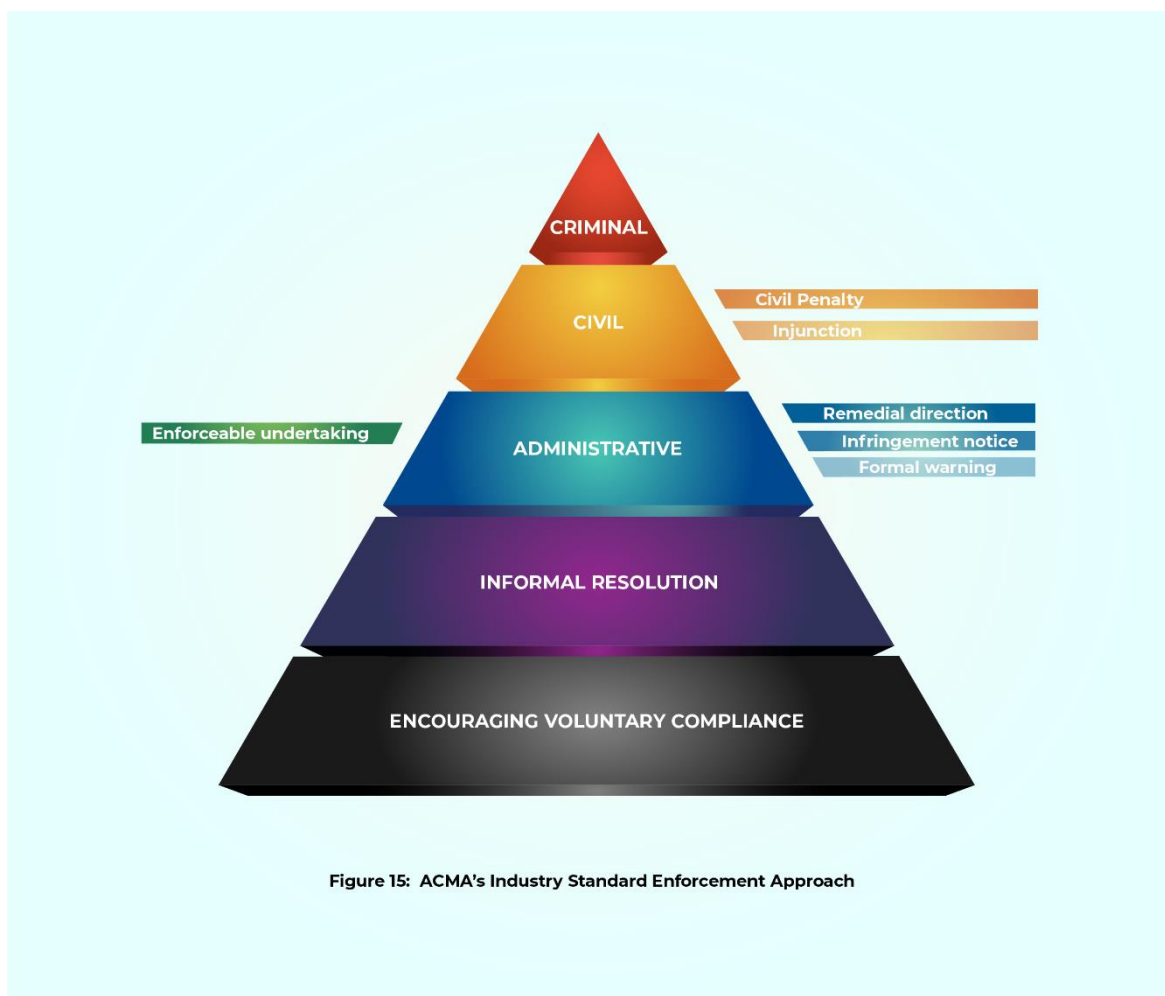


Figure 15: ACMA's Industry Standard Enforcement Approach

## 1 Infringement Notice Factors

Before issuing an infringement notice, the ACMA is required to have regard to any related guidelines it has adopted under s 572M(2) of the Tel Act. In 2022, the ACMA adopted the *Telecommunications (Infringement Notices) Guidelines 2022* (Cth) which state that, in addition to taking into account all relevant facts and circumstances and the compliance history and culture of the regulated entity, the ACMA may consider the same 10 factors listed in its Compliance and Enforcement Policy and set out above. However, it made clear that these factors were not exhaustive.

The ACMA also said it may not be appropriate to issue an infringement notice when:

- (a) the ACMA has previously taken action against the relevant person or entity for similar contraventions;
- (b) the contraventions have occurred over an extended period of time;
- (c) the person or entity has, as a consequence of the contraventions, obtained a financial or other advantage, to the detriment of others; and
- (d) the conduct should more properly be the subject of other compliance or enforcement action by the ACMA because, for example, it is not serious enough to warrant the issue



of an infringement notice or because it is too serious to be adequately dealt with by an infringement notice.<sup>159</sup>

## 2 Enforceable Undertaking Factors

When deciding whether to accept an enforceable undertaking, the ACMA has said that in addition to the compliance history and culture of the regulated entity, it will consider the same 10 factors listed in its Compliance and Enforcement Policy and set out above.<sup>160</sup>

The ACMA has also said it will consider:

- whether the person is prepared to publicly acknowledge the ACMA's concerns about the conduct and the need for corrective action
- whether the terms of the undertaking will achieve an effective outcome for those who may have been disadvantaged by the conduct (if any)
- whether it is likely that undertakings given will be fulfilled.<sup>161</sup>

When deciding when to enforce the term(s) of an enforceable undertaking in court, the ACMA has indicated that although it may proceed directly to court if an enforceable undertaking is breached, it would bring the breach to the attention of the provider in the first instance.<sup>162</sup>

## 3 Remedial Directions Factors

When deciding whether to issue a remedial direction, the ACMA has said it would consider the following non-exhaustive factors:

- the nature and seriousness of the conduct
- whether the conduct was deliberate, reckless or inadvertent
- what, if any, action was taken following the ACMA bringing the issues of concern to the person's attention (for example, through a formal warning)
- whether the remedial direction will promptly and effectively redress and address the conduct and issues of concern to the ACMA
- the impact of issuing the remedial direction on other enforcement action in progress or that may be taken by the ACMA.

## B Comparing the ACMA's Responsive Approach with Responsive Regulation Theory

In the next sub-section, we outline the ACMA's enforcement priorities. In Chapter 4, we also consider how the ACMA applies its responsive enforcement approach. However, before doing so, we highlight a few points of difference between the ACMA's approach to responsiveness and Ayres and Braithwaite's conception of responsive regulation. We do not make these comments as criticisms of the ACMA; instead, they are observations on some differences between the understanding of responsiveness advanced by Ayres and Braithwaite and the version that the ACMA has adopted for enforcement action in the telecommunications sector.

---

<sup>159</sup> Australian Communications and Media Authority (n 77) [9.2].

<sup>160</sup> Australian Communications and Media Authority (n 108) 3.

<sup>161</sup> Ibid.

<sup>162</sup> Ibid [10.1].

First, while the ACMA has embraced Ayres and Braithwaite's enforcement pyramid and some types of responsiveness described in section A(2) of Chapter 1 above, it appears to take into account (at least on paper) some factors that Ayres and Braithwaite would not consider (at least in the first instance) when confronted by a non-compliant provider. For example, like Ayres and Braithwaite, the ACMA may give consideration to the desire of regulatees to improve their behaviour (eg, 'whether the subject of the investigation has co-operated with [the ACMA]') (attitudinal responsiveness). However, the ACMA will also consider factors important for legalistic responsiveness such as the type, number and gravity of breaches committed by regulatees (eg, whether the conduct was 'deliberate, inadvertent or reckless' and 'whether the conduct involved indicates systemic issues which may pose ongoing compliance or enforcement issues'); and factors important for long-memory responsiveness or the historical performance of regulatees over time (eg, 'whether the compliance entity or person has been the subject of prior compliance or enforcement action and the outcome of that action'). These are factors that Ayres and Braithwaite have suggested can lead to less cost-efficient compliance outcomes in the longer term although, as we note in section A of Chapter 1 above, this is not a view shared by all scholars.

Second, the Tel Act and TCPSS Act make it difficult to escalate up the pyramid in the way that Ayres and Braithwaite suggest. In the case of the three consumer codes developed by Comms Alliance and registered with the ACMA – the Mobile Premium Services Code, the TCP Code and the Information on Accessibility Features for Telephone Equipment Code - the ACMA has access to a formal warning and direction to comply to enforce compliance. Only if a direction to comply with these codes is breached can the ACMA access a more fulsome range of enforcement mechanisms. In addition, in the event a provider seriously and repeatedly fails to comply with most of the consumer protection provisions discussed in this report, for example, the ACMA cannot impose criminal penalties, suspend licences and/or seek to exclude the offending provider from the market – actions that appear in the regulatory literature as a result of their presence in other industries/jurisdictions.

Third, to date, the ACMA has not incorporated a strengths-based pyramid in its Compliance and Enforcement Policy. Again, we are not suggesting here that it should; we are just observing how the ACMA's practice is different from some aspects canvassed in the regulatory literature.

## C Enforcement Priorities

In April 2019, in keeping with other regulators such as the ACCC,<sup>163</sup> the ACMA adopted annual compliance priorities for the first time.<sup>164</sup> These annual compliance priorities, once adopted, become the 'performance measures' against which it evaluates the effectiveness of its strategies to achieve the objectives adopted in its corporate plan.<sup>165</sup> It has consulted with stakeholders before adopting its annual compliance priorities since 2020.<sup>166</sup>

---

<sup>163</sup> See, eg, Michael T Schaper, 'How Australia's Franchising Regulator Establishes Its Enforcement Priorities' (2018) 16(2) *International Journal of Franchising Law* 14.

<sup>164</sup> Australian Communications and Media Authority and Office of the eSafety Commissioner, *Annual Reports 2019-2020* (Report, 9 September 2020) 37 ('the ACMA Annual Report 2019-20').

<sup>165</sup> The ACMA's Chair (an accountable authority) must prepare a corporate plan: *Public Governance, Performance and Accountability Act 2013* (Cth) s 35(1)(b). The ACMA's Chair must also prepare an annual performance statement addressing how it achieved the purpose set out in the corporate plan: s 39.

<sup>166</sup> ACMA Annual Report 2019-20 (n 164) 38.

In 2019-2020,<sup>167</sup> the ACMA's compliance priorities included:

- the industry standards adopted to help consumers moving to the NBN;
- the consumer complaints handling industry standard;
- the credit assessment and financial hardship rules in the new fourth edition of the TCP Code registered by the ACMA on 1 July 2019.

In 2020-2021,<sup>168</sup> the ACMA's compliance priorities included:

- 'monitoring how telcos follow [the TCP Code rules, including selling, credit assessment and consumer financial hardship], with a focus on how they sell to and interact with disadvantaged and vulnerable people';
- 'conduct[ing] audits, tak[ing] enforcement action and guid[ing] telco providers to follow the standards it adopted to improve the process for individuals and small businesses of moving to the NBN.'

In 2021-22,<sup>169</sup> the ACMA's compliance priorities included:

- protecting vulnerable telecommunications customers (eg, by focusing on industry compliance with the TCP code rules and assessing if they provide adequate protection);
- complaints-handling for small businesses customers;
- phone scams (eg, by enforcing the Reducing Scam Calls and Scam SMS Code registered by the ACMA on 2 December 2020 and evaluating if amendments to the rules are required).

In 2022-23,<sup>170</sup> the ACMA's compliance priorities included:

- protecting telecommunications customers experiencing financial hardship
- combatting SMS and identity theft phone scams by enforcing the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 and the Reducing Scam Calls and Scam SMS Code.

In 2023-2024,<sup>171</sup> the ACMA's compliance priorities included:

- protecting telco customers experiencing financial hardship, in particular monitoring industry direct debit and responsible selling practices;
- supporting telco customers experiencing domestic and family violence and taking action against telcos that don't follow industry rules.

---

<sup>167</sup> 'Compliance Priorities 2019–20', *Australian Communications and Media Authority* (Web page, 07 April 2020) <<https://www.acma.gov.au/compliance-priorities-2019-20>>.

<sup>168</sup> 'Compliance Priorities 2020–21', *Australian Communications and Media Authority* (Web page, 04 May 2021) <<https://www.acma.gov.au/node/467>>.

<sup>169</sup> 'Compliance Priorities 2021–22', *Australian Communications and Media Authority* (Web page, 09 January 2023) <<https://www.acma.gov.au/compliance-priorities-2021-22>>.

<sup>170</sup> 'Compliance Priorities 2022–23', *Australian Communications and Media Authority* (Web page, 30 June 2023) <<https://www.acma.gov.au/compliance-priorities-2022-23>>.

<sup>171</sup> 'Consumer Protections a Priority for the ACMA in 2023–24', *Australian Communications and Media Authority* (Article, 30 June 2023) <<https://www.acma.gov.au/articles/2023-06/consumer-protections-priority-acma-2023-24>>.

## 4 How Have the Enforcement Mechanisms Been Used?

In this chapter we set out:

- the total number of publicised enforcement actions and total amounts of publicised infringement and civil penalties imposed against telecommunications companies
- examples of how the ACMA has exercised its enforcement powers
- the telecommunications companies with the most public investigations and enforcement actions
- the most enforced provisions in publicised investigations
- the most common combinations of enforcement mechanisms used by the ACMA in publicised investigations
- the years when the ACMA engaged in the least and most publicised enforcement activity.

Again, for the avoidance of doubt, in this report, an 'enforcement action' includes:

- a formal warning, direction to comply, an infringement notice or remedial direction
- a court-ordered injunction or civil penalty; and
- acceptance of an enforceable undertaking.<sup>172</sup>

When evaluating the data presented here, especially the data on the number of investigations and enforcement actions taken, some aspects of research limitations and contextual information should be noted.

To our knowledge, there have been no previous attempts to determine and evaluate how the ACMA has exercised its discretion to enforce the consumer protection-related provisions considered in this report. Consequently, there are no existing studies and/or compilations of data on which we can draw.

### A Research Limitations and Context

#### 1. Research Limitations

Comprehensively determining how the ACMA has exercised its enforcement discretion and whether it has, in fact, exercised its discretion in a way that is consistent with the principles of responsive regulation and/or risk-based regulation outlined in Chapter 1 is a complex exercise. Such a study would require (at a minimum) access to the ACMA's enforcement files as well as interviews with and/or surveys of the enforcement officials and regulatees involved. For example, Nielsen's empirical study of whether four Danish regulators were 'responsive' involved a detailed review of their files. She also asked enforcement officials to complete questionnaires, soliciting information about their reactions to breaches and their views and perceptions of regulatees' overall compliance and willingness to improve their behaviour.<sup>173</sup> May and Winter's work on the enforcement styles of Danish agricultural regulators and May and Wood's work on

---

<sup>172</sup> See section B of Chapter 2. It also includes a single instance of a deed of agreement.

<sup>173</sup> Nielsen (n 31) 399–404.

building construction regulators equally involved extensive use of surveys of regulators and the regulated companies involved.<sup>174</sup>

Even the task of pulling together some basic, but comprehensive, information about the way the ACMA has exercised its enforcement discretion (ie, the total number of enforcement investigations the ACMA has opened and closed; the total number of enforcement investigations that the ACMA has closed with no findings of breach; the total number of investigations that the ACMA has closed with findings of breach but no enforcement action; and the total number of investigations that the ACMA has closed with findings of breach and enforcement action) is not possible for the reasons we outline below.

The ACMA is not required to prepare and publish reports about *all* investigations.<sup>175</sup> It is not required to maintain a register of all directions and other enforcement actions it may have taken against carriers or carriage service providers to secure compliance with the select consumer-protection rules. It is not required to include copies of these directions and instruments in its annual reports.<sup>176</sup> Although the ACMA has discretion to publish enforceable undertakings on its website, it is not required to publish them.<sup>177</sup> When the ACMA conducts an investigation and finds a contravention of the telecommunications consumer protection-related provisions, it will generally publish an investigation report along with copies of any formal warnings, directions to comply, infringement notices and remedial directions issued and/or enforceable undertakings accepted.<sup>178</sup> But unlike its general practice for broadcasting compliance investigations, the ACMA does not generally publish reports of investigations where there is no breach finding.<sup>179</sup> Furthermore, for all investigations, including investigations where the ACMA has found contravening conduct and has taken enforcement action, the ACMA may not publish an investigation report or otherwise publicise the outcome of an investigation if it determines publication is contrary to the public interest.<sup>180</sup> Factors the ACMA will consider in assessing if publication is in the public interest include:

- whether information about the investigation is in the public domain
- the nature and seriousness of the issues
- whether disclosure is desirable to address public concerns or protect the public from further harm or loss
- whether the investigation will be served by publicity, for example, to encourage submissions or the provision of evidence in the investigation
- fairness to the subject/s of the investigation
- protection of any private, confidential or sensitive information

---

<sup>174</sup> See, eg, Peter J May and Soren C Winter, 'Regulatory Enforcement Styles and Compliance' in Christine Parker and Vibeke Lehmann Nielsen (eds), *Explaining Compliance – Business Responses to Regulation* (Edward Elgar, 2011) 222, 227–9; Peter J May and Robert S Wood, 'At the Regulatory Front Lines: Inspectors Enforcement Styles and Regulatory Compliance' (2003) 13(2) *Journal of Public Administration Research and Theory* 117.

<sup>175</sup> Subject to some exceptions, the Tel Act gives the ACMA discretion to prepare and publish investigation reports (see ss 516(1) and 517(2)). For the exceptions, see ss 516(2), and 517(3), (4) and (5).

<sup>176</sup> See, eg, ss 57 and 67 of the *Australian Communications and Media Authority Act 2005* (Cth).

<sup>177</sup> See Tel Act s 572B(5).

<sup>178</sup> See the ACMA, *Regulatory Guide No. 6: Publication of Investigations and Enforcement Actions* (Updated February 2023) 3-4 <<https://www.acma.gov.au/publications/2019-12/guide/regulatory-guide-no-6-publication-investigations-and-enforcement-actions>>. See also <<https://www.acma.gov.au/investigations-telco-providers>>.

<sup>179</sup> *Ibid* para 4.5. We found only one instance where the ACMA publicised information about an investigation which led to a finding of no breach. See its investigation into Vodafone Network Pty and Vodafone Pty Ltd's alleged breach of cl 8.2.1(a)(xiii) of the TCP Code in July 2013, <<https://www.acma.gov.au/investigations-telco-providers-2010-2016>>.

<sup>180</sup> *Ibid* para 4.1.

- any potential adverse impact public comment may have on the conduct of the investigation or any subsequent court proceedings, including on a person's right to a fair trial.<sup>181</sup>

The ACMA does publish some information about its enforcement practices in its Annual Reports. For example, the ACMA provides information on its investigations, but its focus of reporting varies from year to year and a standard reporting format has not been used across the span of years we examine in this report. For example, some Annual Reports present information on concluded investigations while others report on investigations opened and closed, and in some years, a narrative explanation of issues arising is provided rather than overall investigations numbers. (As with any complaint-handling organisation, the number of investigations opened each year does not correspond with the number of investigations closed, as some matters run over more than one year.)

The ACMA also publishes some information about its enforcement practices in its quarterly 'Action on Telco Consumer Protection Reports'.<sup>182</sup> While informative, these reports discussing the ACMA's actions on telco consumer protection do not cover the full period examined in this report (they cover the period April 2018 until June 2023) and they only discuss or refer to the outcomes the ACMA has decided to publish.

As we do not have access to the data needed to provide a comprehensive overview, we have focused on gathering publicly available information needed to inform further academic study and consideration by industry and government. We started by compiling a table of publicised investigations and enforcement actions taken by the ACMA for non-compliance with:

- the select industry codes registered by the ACMA under Part 6 of the Tel Act
- the select industry standards determined by the ACMA under ss 125 and 125AA of the Tel Act
- the select service provider rules; and
- the select carrier licence conditions.

On its website, the ACMA publishes lists of telecommunications investigations dating back to 2017.<sup>183</sup> We analysed the data, supplementing it where appropriate and possible, with the ACMA investigation reports, enforcement instruments (where available), Annual Reports and information from other the ACMA publications and public statements, as well as from Federal Court decisions where civil penalties were imposed.

The data collected includes the names of all service providers against whom publicised enforcement action was taken between 1 January 2010 and 30 June 2023; the provisions the ACMA found they had breached when the ACMA took enforcement action; and the number and types of enforcement actions the ACMA took against each service provider. The data collected also includes the names of 26 providers that the ACMA found (and publicly announced) had engaged in contravening conduct but against whom no enforcement action was taken.<sup>184</sup>

The data covers the period 1 January 2010 to 30 June 2023 for three principal reasons. First, ACCAN provided us with a table, prepared by the ACMA, of publicly announced investigations

---

<sup>181</sup> Ibid para 2.2.

<sup>182</sup> See <<https://www.acma.gov.au/action-telco-consumer-protections>>.

<sup>183</sup> See 'Investigations into Telco Providers' (<<https://www.acma.gov.au/investigations-telco-providers>>) and 'Investigations into Telco Providers 2010-2016' (<<https://www.acma.gov.au/investigations-telco-providers-2010-2016>>).

<sup>184</sup> See section B of this chapter for an explanation of the way we define 'provider' in this chapter of the report.

listed on its website of all consumer-related enforcement action between 2017 and 2022. Second, we felt that enforcement data covering a wider time span was necessary to provide a more accurate basis for further study and discussion. Third, we had already collated information relating to the enforcement of the TCP Code for the period 1 January 2010 to 31 December 2016 for another research project. The methodology used to collect the data is fully explained in Annex B.

When reading the statistics and other information provided below, it is important to keep in mind the following limitations of the research.

- The data is not comprehensive because:
  - it is based on publicised investigations concerning breaches of the select consumer-protection rules that are the focus of this report;
  - it is based on investigations and enforcement actions that the ACMA has chosen to publicise on its website and/or in its Annual Reports and does not include investigations that the ACMA has decided are not in the public interest to publicise;
  - many investigation reports (and related enforcement actions) that the ACMA has prepared and published since its establishment in 2005 are no longer available on its website.<sup>185</sup>
- Where there were inconsistencies between the ACMA's website and its Annual Reports, we generally deferred to the information in its Annual Reports. Our approach is explained further in Annex B.
- The data collected does not enable us to determine if the ACMA staff adopted a 'tit for tat' understanding of responsiveness or a 'restorative justice' understanding of responsiveness (as explained in Chapter 1 above); the attitudes telecommunications providers displayed at the time of breach; whether and how that attitude influenced the enforcement response of the ACMA staff; and the extent to which the ACMA may have opted to take alternative enforcement action had the mechanisms within Tel Act been different.

Further research is required to begin to make a thorough assessment of the ACMA's enforcement practices.

## 2. Contextual Information

When reading this chapter, there are also three aspects of contextual information to consider.

First, we note above that the ACMA does not report each year on the total number of investigations opened and closed, and as a result, we are unable to describe how the ACMA has exercised its discretion to open and close investigations without making a finding of breach. Having said that, below are examples of the ACMA's reporting on total numbers of investigations:<sup>186</sup>

---

<sup>185</sup> Although some material is available from the Australian National Library's Trove service, and pages from earlier versions of the ACMA's website can be retrieved via the Internet Archive's WayBack Machine, many resources are not available from Trove and many web pages with potentially pertinent enforcement information and investigation reports have not been archived or indexed by the WayBack Machine.

<sup>186</sup> See, respectively, Annual Report 2009-10, p.86; Annual Report 2016-17, 19, 70-72; Annual Report 2021-22, 10, 39.

- In 2009-10, the ACMA recorded 159 'code compliance matters affecting telecommunications consumers'. Of these, 21 proceeded to a formal investigation and 5 resulted in a breach finding.
- In 2016-17, the ACMA recorded 122 preliminary inquiries into TCP Code compliance with 36 formal investigations concluded. It also opened 4 investigations into TIO scheme membership and 2 investigations into TIO scheme compliance.
- In 2021-22, the ACMA finalised 36 investigations into 'telecommunications consumer safeguards'. It opened 32 such investigations as well as 7 investigations into numbering and IPND obligations.

Second, the ACMA undertook numerous compliance audits of communications providers between 1 July 2009 and 30 June 2023, finding high levels of compliance in several instances. The targeted rules included: the MPS and TCP codes, IPND rules, the NBN consumer experience safeguards, and the Telecommunications (Consumer Complaints Handling) Industry Standard 2018. Further details of some of the ACMA's compliance audits during this period, based on information in the ACMA's Annual Reports, is set out in Annex C. As an example, one of these, in 2013-14, concerned compliance with the TCP Code:

Following its March 2013 audit of critical information summaries, the ACMA conducted a follow-up audit of 46 providers in March 2014 to check that they have critical information summaries and these are in the prescribed format. Of the 46 providers assessed, only two per cent failed to have a critical information summary; 90 per cent were immediately compliant ...

In December 2013, the ACMA commenced an audit of seven large and medium-sized providers of included value plans to assess their compliance with the usage alert requirements. The ACMA found that most providers had a small incidence of failure to send notifications or the correct information at the 100 per cent notification level. However, all providers aside from one (discussed below) addressed systemic issues and were deemed compliant. The audit found that Dodo Services Pty Ltd (Dodo) did not comply with the required usage notification requirements, as it failed to send alerts to customers about their data use. The failure affected certain Dodo customers with a fixed broadband service during October and November 2013. In May 2014, the ACMA issued Dodo with a formal warning for failing to comply with the usage alert requirements of the TCP Code.<sup>187</sup>

More recently, the ACMA has conducted extensive work on hardship policies, with three annual 'state of play' reports and a further substantial report published in 2023 that noted 'In December 2022, we completed an audit of 15 telcos' compliance with financial hardship and disconnection notification requirements in the TCP Code. As a result of the audit findings, we are undertaking some investigations.'<sup>188</sup>

Third, there are two 'regulatory intermediaries' whose functions assist in securing telecommunications companies' compliance with the various consumer-protection rules discussed in this report: the TIO and CommCom. Regulatory intermediaries are third parties

<sup>187</sup> Australian Communications and Media Authority, *Annual Report 2013-14* (Report, 30 September 2014) 80-81.

<sup>188</sup> Australian Communications and Media Authority, *Financial Hardship in the Telco Sector: Keeping the Customer Connected* (Report, May 2023) 16. Information, research and other reports on this topic over the period 2018-2023, including three annual 'state of play reports', is available at <https://www.acma.gov.au/financial-hardship-telco-sector-keeping-customer-connected>.



that act on behalf of, or directly or indirectly in conjunction with, regulators or targets of regulation (and not necessarily at their behest) to achieve regulatory objectives.<sup>189</sup> The TIO, for example, undertakes systemic investigations into various matters that fall within its jurisdiction, including the TCP Code, in response to consumer complaint trends and works with providers to address issues of concern. Only when providers fail to cooperate with the TIO will it refer the matters to the ACMA and/or another appropriate regulator. CommCom also contributes to industry compliance when evaluating the robustness of providers' compliance attestation documentation.

## B Total Publicised Enforcement Actions and Amounts of Publicised Infringement and Civil Penalties

In this section, where we look at investigations, breach findings and enforcement actions in relation to telecommunications service providers, we use the term 'provider' to refer to companies including subsidiaries and associated companies that essentially use the same name in the market. For example, we classify Optus Internet Pty Limited, Optus Networks Pty Limited, Singtel Optus Pty Ltd and Optus Mobile Pty Ltd as 'Optus'. Except where otherwise indicated, we have not included companies within the same corporate group that used different entities to offer differently branded services to consumers. For example, even though iiNet was acquired by TPG in 2015, it remains as a separate 'provider' in our overall results.<sup>190</sup>

Of the investigations, breach findings and enforcement actions about our selected consumer protection rules in the period from 1 January 2010 to 30 June 2023 that the ACMA has made public, we found:

- there were 487 investigations, all but one of which resulted in a finding of at least one breach;
- 320 providers were the subject of these breach findings, 309 of which had at least one enforcement action taken against them;<sup>191</sup>
- there were 502 enforcement actions in total.

While the information published by the ACMA does not allow us to determine the total number of investigations that resulted in no finding of breach, we found that no more than 26 publicised investigations resulted in breach findings but no formal enforcement action.

Of the 502 enforcement actions we found over this period, the range of actions was as follows (see also Figure 16):<sup>192</sup>

- 296 formal warnings
- 119 directions to comply
- 41 remedial directions
- 24 infringement notices with a total value of \$6,143,160.

---

<sup>189</sup> Kenneth W Abbott, David Levi-Faur and Duncan Snidal, 'Theorizing Regulatory Intermediaries: The RIT Model' (2017) 670(1) *Annals of the American Academy of Political and Social Science* 14, 14–5.

<sup>190</sup> In recognition of the market share of the TPG group, we do provide a separate note at the end of section D below that collates the results of the various companies that now constitute TPG.

<sup>191</sup> This number excludes one entry for an unidentified provider. This is because of the possibility that the unidentified provider had already been counted elsewhere in the data.

<sup>192</sup> Some investigations resulted in more than one associated enforcement action. See Table 1 in section G below and the notes to that table for a breakdown of the total number of enforcement actions by year, and assumptions made in the compilation of the data.

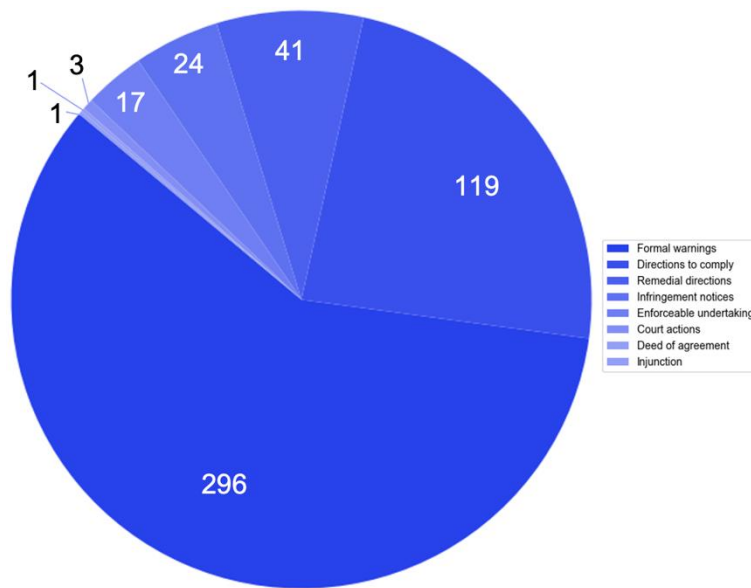


Figure 16. Breakdown of Enforcement Actions Taken by Type

The ACMA accepted 17 enforceable undertakings.

The ACMA also obtained from the Federal Court three civil penalty orders: one against Bytecard for failure to comply with the TIO scheme in 2013;<sup>193</sup> one against TPG Internet for breach of the Telecommunications (Emergency Call Service) Determination 2009 (Cth) in 2014;<sup>194</sup> and one against Limni Enterprises (formerly known as Red Telecom) for failure to comply with the TIO scheme in July 2022.<sup>195</sup> The penalties imposed by the Federal Court on the three companies totalled \$1,077,625. Bytecard was required to pay \$112,500 of which \$75,000 was apportioned to Bytecard itself and \$37,500 to its director, Brian Morris. TPG Internet was required to pay \$400,000. Limni Enterprises was required to pay \$565,125, \$450,000 of which was apportioned to Limni itself, and \$115,125 to its sole director and shareholder, Nicholas Kontaxis.

In addition to the civil penalty order, the ACMA obtained an injunction against Bytecard which required Bytecard to establish and maintain a compliance program relating to its obligations under the TIO scheme and required Mr Morris to engage in compliance training.<sup>196</sup> This was the only injunction obtained by the ACMA.

## C Examples of How the ACMA has Exercised its Enforcement Powers

In the text boxes below, we provide some recent examples of when the ACMA issued formal warnings to comply, directions to comply, remedial directions, and infringement notices. We also explain the three instances where the ACMA sought civil penalties in the Federal Court. These case studies provide some further insight into how the ACMA applies the Tel Act's enforcement provisions and its own policies mentioned in section A of Chapter 3 above. Two examples (ie, the examples involving Telstra and SpinTel) refer to action in response to

<sup>193</sup> *Australian Communications and Media Authority v Bytecard Pty Ltd* [2013] FCA 38.

<sup>194</sup> *Australian Communications and Media Authority v TPG Internet Pty Ltd* [2014] FCA 382.

<sup>195</sup> *Australian Communications and Media Authority v Limni Enterprises Pty Ltd (formerly known as Red Telecom Pty Ltd)* [2022] FCA 795.

<sup>196</sup> *ACMA v Bytecard* (n 193) (iii)-(iv).

breaches of the TCP Code – a co-regulatory instrument that imposes consumer protection obligations on telecommunications providers. It comprises a set of rules that apply to all carriage service providers that supply telecommunications products to residential and small business consumers.

## 1 Administrative Enforcement Actions

### Case Study: Formal Warning: Telstra (March 2023)<sup>197</sup>

- **Telstra’s breach:** the ACMA found Telstra contravened clause 6.7.1 of the **TCP Code** (Prior Notice of Restriction, Suspension, or Disconnection Action) by not giving customers a minimum of 5 working days’ notice before restricting or suspending their services for credit and/or debt management reasons. 5,245 customers had their services restricted. 165 customers had their services suspended.
- **Telstra’s response:** Telstra reported that the issue affected customers who received notice by mail and an intermittent system error prevented the correct customer dataset from being uploaded and forwarded to its mail house provider. Although 1,030 customers were without service or had restricted service for an average of 31 days, 4,283 customers had their services restored 7 days after their services had been restricted or suspended. The remaining 97 customers were more advanced in the debt collection process and had been provided with further, valid collection notices.
- **Enforcement action:** the ACMA issued a formal warning.<sup>198</sup>

In this first example, the ACMA does not publicly explain its rationale for issuing a formal warning instead of a direction to comply, which it was entitled to do following its finding Telstra had breached the TCP Code (as explained in section C(1) of Chapter 2, above). In this instance, however, the ACMA’s response could have been influenced by four factors discussed in Chapter 3, section A:

- the harm experienced by Telstra’s customers (here, the loss of customers’ telecommunications services)
- the duration of that harm (for most customers the harm was relatively short-lived)
- the cause of the notification error being unintentional
- Telstra’s actions to remedy the situation.

The case study also illustrates how the ACMA seeks to use the minimum enforcement power necessary to achieve compliance, notwithstanding consumer harm, and apply the Tel Act’s policy of fostering industry compliance without imposing undue financial or administrative burdens on regulated entities.

<sup>197</sup> Australian Communications and Media Authority, *Investigation Report* (Investigation, ACMA2022/771, 24 March 2023) <<https://www.acma.gov.au/sites/default/files/2023-04/Final%20investigation%20report%20-%20Telstra%20Corporation%20Limited.pdf>>.

<sup>198</sup> Australian Communications and Media Authority, *Formal warning issued under subsection 122(2) of the Telecommunications Act 1997* (24 March 2023) <<https://www.acma.gov.au/sites/default/files/2023-04/Formal%20Warning%20to%20Telstra%20Corporation%20Limited%20%28signed%2024%20March%2023%29.pdf>>.

Our second example focuses on a breach of another TCP Code provision. Unlike the first example involving Telstra, this second example led the ACMA to issue a direction to comply against SpinTel.

[Case Study: Direction to comply: SpinTel \(June 2022\)](#)<sup>199</sup>

- **SpinTel's breach:** the ACMA found SpinTel breached clause 4.1.2(b) of the **TCP Code** which aims to protect consumers from misleading or deceptive selling practices. In its SIM Only Mobile Plans advertising, SpinTel used the term 'unlimited' in an unqualified manner even though the service was not genuinely unlimited and subject to exclusions.
- **SpinTel's response:** SpinTel accepted the ACMA's preliminary findings that it had breached clause 4.1.2(b) and told the ACMA it was an unintentional error. SpinTel also amended its Acceptable Use Policy (AUP) so that its plans could correctly be described as unlimited.
- **Enforcement action:** The ACMA issued SpinTel with a **direction to comply** with clause 4.1.2(b) of the **TCP Code**.<sup>200</sup>

Again, the ACMA does not explain its rationale for issuing a direction to comply instead of a formal warning, which it could have done following its finding that Telstra breached of the TCP Code. (See Chapter 2, section C(1) above). However, in this instance, the ACMA may have considered:

- the nature of the TCP code obligation
- the harm experienced by SpinTel's customers
- the cause of the breach being unintentional
- SpinTel's cooperative behaviour
- SpinTel's prompt amendment of its AUP policy.

It is possible the purpose of the TCP code obligation – to protect consumers against misleading and deceptive selling practices – also contributed to the ACMA electing to use more forceful enforcement action.

Our third example involves a situation where the ACMA issued a remedial direction against Optus.

<sup>199</sup> Australian Communications and Media Authority, *Investigation Report* (Investigation, ACMA 2022/121) <<https://www.acma.gov.au/sites/default/files/2022-06/SpinTel%20Pty%20Ltd%20-%20Investigation%20Report%20-%20June%202022.pdf>>.

<sup>200</sup> Australian Communications and Media Authority, *Direction under subsection 121 (1) of the Telecommunications Act 1997* (15 June 2022) <<https://www.acma.gov.au/sites/default/files/2022-06/SpinTel%20Pty%20Ltd%20Direction%20-%20June%202022.pdf>>.

[Case Study: Remedial direction: Optus \(March 2022\)](#)<sup>201</sup>

- **Optus's breaches:** the ACMA found Optus had contravened s 101(1) of the Tel Act (obligation to comply with service provider rules) by breaching three subsections of the **Telecommunications Service Provider (NBN Service Migration) Determination 2018**. It breached subsections 14(3) and 15(1) of the Determination on 34,258 occasions by failing to notify customers of their maximum attainable speed (MAS) on next-generation NBN broadband services and incorrectly charging them. It also breached section 14(2) the Determination on 24,039 occasions by failing to either confirm the MAS or perform, or arrange to perform, line capability testing within 20 days of each service becoming operational.
- **Optus's response:** Optus self-reported the issues it had identified in its compatibility testing to the ACMA in July 2021. Optus explained the failures, at least with respect to the breaches of subsection 14(2), resulted from technical difficulties. Optus cooperated with requests from the ACMA, and it was the information provided by Optus that informed the ACMA's view of the breaches found.
- **Enforcement action:** the ACMA issued a **remedial direction**. It directed Optus to implement and maintain effective systems, processes, and practices for complying with the Determination, appoint an independent auditor to audit and report on its compliance and contact and offer remedies to affected customers.<sup>202</sup>

Looking at the criteria highlighted in section A of Chapter 3 above that the ACMA will consider in determining the most appropriate enforcement approach, on this occasion, the following factors likely contributed to the ACMA's chosen approach:

- the nature of the obligation in the Determination
- the detriment experienced by a large number of customers
- the fact that the breach was not deliberate but due to issues with Optus's IT systems
- the fact that Optus told the ACMA about the issue
- Optus's cooperative behaviour, including admissions of breach to the ACMA after conducting its own internal investigation.

Despite the large number of impacted customers, and the fact that this matter arose from a problem with Optus's systems, Optus's decision to self-report the breaches and its cooperative behaviour may have influenced the ACMA's decision to issue a remedial direction instead of pursuing a civil penalty or an infringement notice (breach of ss 14(3) and 15(1) of the Telecommunications Service Provider (NBN Service Migration) Determination 2018 are listed infringement notice provisions). Pursuit of a civil penalty or an infringement notice would arguably create strong disincentives to report non-compliance.<sup>203</sup>

<sup>201</sup> Australian Communications and Media Authority, *Investigation Report* (Investigation, ACMA2021/561) <<https://www.acma.gov.au/sites/default/files/2022-03/Optus%20Investigation%20report.PDF>>.

<sup>202</sup> Australian Communications and Media Authority, *Direction in relation to subsections 14(2), 14(3) and 15(1) of the Telecommunications Service Provider (NBN Service Migration) Determination 2018* (11 March 2022) <<https://www.acma.gov.au/sites/default/files/2022-03/Optus%20Remedial%20direction.PDF>>.

<sup>203</sup> See section A of Chapter 3, above.

Our fourth and final example (above) of administrative enforcement action taken by the ACMA involves its decision to issue two infringement notices to Lycamobile in May 2022. This action followed enforcement action taken a year earlier for breach of the same obligations.

#### [Case Study: Infringement notice: Lycamobile Pty Ltd \(May 2022\)](#)<sup>204</sup>

##### **The first investigation**

- On 3 December 2020, the ACMA found that Lycamobile had contravened:
  - section 101(1) of the Tel Act (obligation to comply with service provider rules) by not complying with the **Telecommunications (Service Provider— Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 (Prepaid Determination)**, and the IPND service provider rule set out in subclause 10(2) of Part 4 of Schedule 2 to the Tel Act (**IPND Service Provider Rule**), and
  - the **Integrated Public Number Database (IPND) Code (IPND Code)**.
- As a result of these contraventions, in January 2021 the ACMA gave Lycamobile a **remedial direction** (varied in March 2021) for the **Prepaid Determination** and a **direction to comply** with the **IPND Code**. In March 2021, it also gave Lycamobile an **infringement notice** for \$604,800 in relation to the IPND service provider rule (a listed infringement notice provision). In May the ACMA also **accepted** an **enforceable undertaking** from Lycamobile regarding its IPND obligations.

##### **The second investigation**

- Following this first round of enforcement action, the ACMA became aware that Lycamobile had continued to be in contravention of its obligations relating to the IPND. The ACMA commenced a second investigation in December 2021. In an investigation report issued in February 2022, the ACMA found that Lycamobile had on multiple occasions breached the IPND Code and IPND service provider rule (again), the direction to comply, and the remedial direction. The ACMA said Lycamobile had undermined the intention of the remedial direction by failing to meet multiple deadlines for key deliverables, despite numerous reminders from the ACMA relating to its obligations. The ACMA noted that even in instances where Lycamobile had proposed alternative dates for deliverables, these were not always met.
- **Enforcement action:** The ACMA issued two infringement notices on 13 May 2022. The first was for \$159,840 for 12 contraventions of s 121(2) of the Tel Act which required compliance with the **direction to comply with the IPND Code**.<sup>205</sup> The second was for \$26,640 for two contraventions for failing to adhere to the timeframe and commitments of the **remedial direction** (a listed infringement notice provision).<sup>206</sup>

<sup>204</sup> Australian Communications and Media Authority, *Investigation Report* (Investigation, 24 February 2022) <[https://www.acma.gov.au/sites/default/files/2022-06/Investigation%20Report%20-%20Lycamobile\\_Redacted.pdf](https://www.acma.gov.au/sites/default/files/2022-06/Investigation%20Report%20-%20Lycamobile_Redacted.pdf)>.

<sup>205</sup> Australian Communications and Media Authority, *Infringement Notice* (13 May 2022) <[https://www.acma.gov.au/sites/default/files/2022-06/Infringement%20notice%20-%20Direction%20to%20comply%20with%20IPND%20Code%20contravention\\_s\\_Redacted.pdf](https://www.acma.gov.au/sites/default/files/2022-06/Infringement%20notice%20-%20Direction%20to%20comply%20with%20IPND%20Code%20contravention_s_Redacted.pdf)>.

<sup>206</sup> Australian Communications and Media Authority, *Infringement Notice* (13 May 2022) <[https://www.acma.gov.au/sites/default/files/2022-06/Infringement%20Notice%20-%20remedial%20direction%20contraventions\\_Redacted.pdf](https://www.acma.gov.au/sites/default/files/2022-06/Infringement%20Notice%20-%20remedial%20direction%20contraventions_Redacted.pdf)>.

Some explanation of the IPND obligations is helpful when considering this example. The IPND database is an essential tool for emergency services and a source of information for law enforcement and national security agencies. It is also used for authorised research purposes. When a call is made to Australia's emergency call service, Triple Zero, the caller's number is checked against the IPND Database, allowing for the dispatching of emergency services, even if callers do not provide or are unable to provide their physical location to emergency operators. The information that telcos obtain from customers under the Prepaid Determination is uploaded to the IPND. Accordingly, the seriousness of the obligation likely influenced the ACMA's enforcement response (at least in part) in this case study. In January 2021, the ACMA moved straight to issuing a remedial direction (its strongest administrative power) alongside a direction to comply and an infringement notice for \$604,800.

However, even though Lycamobile again breached its IPND obligations in 2022 and the remedial direction, the ACMA chose to issue two additional infringement notices (May 2022), instead of moving up the enforcement pyramid and pursuing civil sanctions.

In this example, the ACMA may have considered:

- the relevant regulatory objective
- the nature of the code and IPND-related obligations
- the potential detriment caused by the conduct
- Lycamobile's prior history of non-compliance
- its lack of action to remedy the issue
- the ongoing effect of the remedial direction and enforceable undertaking.

In a media release provided alongside the infringement notices, the ACMA stated that the remedial direction and enforceable undertaking would remain in place for a further two years and, should Lycamobile breach its obligations again, the ACMA could commence civil sanction proceedings.<sup>207</sup>

As noted in section A of Chapter 3 above, the ACMA has stated that it will 'generally use the minimum power or intervention necessary to achieve the desired result'.<sup>208</sup> That approach may have informed the ACMA's decision in this instance, with the ACMA signalling in its associated media release that it 'will continue to watch Lycamobile closely' and flagging the prospect of court action in the case of further contraventions.<sup>209</sup>

---

<sup>207</sup> 'Lycamobile Pays \$186,480 Penalty for Public Safety Failures', *Australian Communications and Media Authority* (Article, 23 June 2022) <<https://www.acma.gov.au/articles/2022-06/lycamobile-pays-186480-penalty-public-safety-failures>>.

<sup>208</sup> This is set out in the ACMA's Compliance and Enforcement Policy – see (n 68) and the discussion above in Chapter 3, section A.

<sup>209</sup> ACMA (n 207).

## 2 Civil Penalty Enforcement Actions

### *Civil Penalty Case Study 1: Australian Communications and Media Authority v Bytecard Pty Ltd*<sup>210</sup>

#### **The ACMA's claims against Bytecard and Brian Morris:**

- The ACMA alleged that Bytecard and its director, Brian Morris, breached the Tel Act by failing to comply with the **TIO Scheme**, a **service provider rule** of the Tel Act, **clause 6.1 of the TIO Constitution**, and **two remedial directions from the ACMA**.
- The ACMA sought a **civil penalty** against Bytecard of \$90,000 and against Mr Morris of \$45,000.

On 1 February 2013, the court imposed a **civil penalty of \$75,000 against Bytecard and \$37,500 against Mr Morris**. It also granted a mandatory injunction imposing a compliance program on Bytecard and Mr Morris. (See further chapter 4, section F).

#### **The ACMA's actions before going to court:**

- conducting investigations into Bytecard's conduct and obtaining information from the TIO and the complainants;
- issuing **two remedial directions** to Bytecard under **s 102(2) of the Tel Act**, dated 29 August 2007 and 13 September 2011, requiring Bytecard to take specified action to ensure that it did not contravene the service provider rules in the future.

Some factors that may have led to the ACMA pursuing a civil penalty in this case include:

- Bytecard's persistent failure to comply with TIO determinations and the two the ACMA remedial directions; the lack of cooperation and communication with the ACMA and the TIO; and Bytecard's refusal to provide any satisfactory explanation or justification for its non-compliance
- the important function of the TIO scheme
- Bytecard's unprofessional and inappropriate behaviour towards its customers, the TIO and the ACMA, as evidenced by its rude, insulting and offensive remarks, and its use of foul language.

This first example provides an illustration of the ACMA escalating its enforcement actions up the pyramid. In 2011, the ACMA used its strongest administrative powers and issued the remedial directions under s 102(2) of the Tel Act. When these were not complied with, the ACMA applied to the Federal Court for civil penalties.

---

<sup>210</sup> [2013] FCA 38.



Civil Penalty Case Study 2: Australian Communications and Media Authority v TPG Internet Pty Ltd<sup>211</sup>

**The ACMA's claims against TPG Internet:**

- The ACMA sought a civil penalty against TPG Internet Pty Ltd (TPG) for failing to provide access to emergency services for some of its customers.
- TPG admitted that it breached the **Telecommunications (Emergency Call Service) Determination 2009 (the ECS Determination)** by not ensuring that its systems and networks enabled end users of its home phone service to access the '000' emergency call service.

On 16 April 2014, the Federal Court found that TPG contravened both **sections 13 and 19 of the ECS Determination** and s 148(1) of the **TCPSS Act** and ordered TPG to pay a total of **\$400,000 in civil penalties**.<sup>212</sup> The Court considered the nature and extent of the contraventions, the loss or damage suffered, the circumstances of the contraventions, and TPG's previous conduct.

**The ACMA's actions before going to court:**

- The ACMA investigated TPG's compliance with the **ECS Determination** after receiving a complaint from a customer who was unable to connect with emergency services. As a result of its investigation, the ACMA initiated court proceedings.

This case was the first time the ACMA had initiated court proceedings for breaches of the ECS Determination. The ACMA most likely decided to pursue civil penalties in the first instance because of the following factors:

- the harm and detriment that was or could have been caused by non-compliance with the ECS Determination
- the regulatory objective of ensuring end users have access to emergency services
- TPG's systems issues that gave rise to the breaches
- the deterrent effect of seeking a civil penalty.

TPG did cooperate with the ACMA, and the breaches were not deliberate. However, in deciding to initiate court proceedings for this breach, the ACMA presumably gave greater weight to 'the seriousness of the breach and the level of harm'.<sup>213</sup>

---

<sup>211</sup> [2014] FCA 382.

<sup>212</sup> The maximum penalty for each contravention of the ECS Determination is \$250,000. See Tel Act s 570(3)(b).

<sup>213</sup> This is set out in the ACMA's Compliance and Enforcement Policy – see (n 68) and the discussion above in Chapter 3, section A.

Civil Penalty Case Study 3: Australian Communications and Media Authority v Limni Enterprises Pty Ltd (formerly known as Red Telecom Pty Ltd)<sup>214</sup>

**The ACMA's claims against Red Telecom and Nicholas Kontaxis:**

- The ACMA took action against Limni Enterprises Pty Ltd (formerly Red Telecom Pty Ltd) and its sole director Nicholas Kontaxis for breaching the **TCPSS Act** and the **Tel Act** by failing to comply with seven determinations made by the **TIO**.
- The ACMA sought civil penalties against both defendants, as well as leave to continue the proceedings against Red Telecom in liquidation.

The Federal Court considered the nature, extent and duration of the conduct, the circumstances in which the contraventions took place, the loss or damage caused by the conduct, the size and financial position of the respondents, their prior conduct, any cooperation and corrective action, and the need for deterrence.

On 11 July 2022, the Federal Court decided to impose total **penalties of \$450,000 on Red Telecom and \$115,125 on Mr Kontaxis**.

**The ACMA's actions before going to court:**

- After a referral from the TIO, the ACMA conducted an investigation into Red Telecom's compliance with the TIO scheme. This investigation led to the ACMA directly initiating the court proceedings.

Possible factors that may have influenced the ACMA's decision to pursue civil penalties in the first instance after its initial investigation include:

- the nature, extent and duration of Red Telecom's conduct, which involved failing to comply with seven TIO determinations over a period of 12 to 23 months, causing loss or damage to the affected customers and undermining the integrity of the TIO scheme;
- the circumstances in which the contraventions took place – it was found that Mr Kontaxis deliberately decided not to comply with the TIO determinations, despite being aware of his obligations under the Tel Act;
- the lack of cooperation and remedial action by Red Telecom and Mr Kontaxis;
- the need for deterrence, both specific and general, to ensure that Red Telecom, Mr Kontaxis and other industry participants comply with their obligations under the Tel Act;
- the need to maintain industry respect for the TIO's authority and finality of its determinations.

The prolonged non-compliance and disrespect towards the TIO determinations, paired with apparent disregard for the harm caused to customers, may have indicated to the ACMA that a 'light touch' regulatory approach would be ineffectual in this case, prompting it to immediately escalate its response and seek civil penalties.

---

<sup>214</sup> [2022] FCA 795.

The decision of the Federal Court indicates that the penalties imposed—\$450,000 on Red Telecom and \$115,125 on Mr Kontaxis—were not solely punitive. Their aim was to deter both specific and general non-compliance.<sup>215</sup>

The TIO is regarded as a significant protector of consumer rights, and promoting compliance with TIO determinations is important. The ACMA's enforcement action can therefore be seen as supporting the effectiveness of the scheme.

## D Telcos with the Most Investigations and Enforcement Actions

In this section we examine which providers have been the subject of the most investigations and enforcement actions. As in section A, here we are referring only to the investigations and enforcement action that the ACMA has made public. The data is taken from the ACMA publications including annual reports and online listings. And as noted in the introduction to this chapter, the ACMA does not generally publicise investigations where it concludes no breach has occurred.

Our research shows that out of 320 providers that were the subject of investigations with breach findings, the majority faced a single investigation. Specifically, 247 providers were the subject of one investigation, while 73 encountered multiple. Similarly, enforcement actions predominantly targeted providers once, with only 79 providers being the subject of more than one enforcement action. Not all breach findings resulted in the ACMA undertaking enforcement action. Our research found 26 instances of no recorded enforcement action arising from a publicised investigation. These instances of no recorded enforcement action included investigations into 11 providers that were not the subject of any other enforcement action by the ACMA over the study period.<sup>216</sup>

The full breakdown of enforcement actions against numbers of providers was as follows:

- 230 providers were the subject of one enforcement action
- 45 providers were the subject of two actions
- 15 providers were the subject of 3 actions
- 5 providers were the subject of 4 actions
- 3 providers were the subject of 5 actions
- 4 providers were the subject of 6 actions
- 1 provider was the subject of 7 actions
- 3 providers were the subject of 8 actions
- 1 provider was the subject of 11 actions
- 1 provider was the subject of 12 actions
- 1 provider was the subject of 24 actions.

---

<sup>215</sup> Ibid [142].

<sup>216</sup> Further, as noted above, multiple enforcement actions can stem from a single investigation (eg, a direction to comply with a code of practice and an enforceable undertaking given in relation to a related breach of a service provider rule), meaning that the total number of providers that are the subject of publicised investigations is not the same as the total number of providers that were the subject of enforcement action.

While it is impractical to identify all the individual providers by name here, Figure 17 provides an indication of the ‘top 10’ providers in terms of enforcement action.<sup>217</sup> In keeping with our approach (explained in section B above) we treat as separate ‘providers’ companies within the same corporate group that used different entities to offer differently branded services to consumers. Vodafone and TPG are both listed in Figure 17, even though they were the subject of a merger on 13 July 2020. As the merged TPG-Vodafone parent entity carried on the TPG brand, for the purpose of this section, post-merger enforcement actions that the ACMA has taken against this parent entity have been counted against TPG – this included two entries, one in relation to the Vodafone brand,<sup>218</sup> and the other in connection with the Lebara brand.<sup>219</sup> (See the separate note on TPG Group following the notes on the top 10 providers below for further information.) For context, it should be noted that the customer base of some of these providers (most notably, Telstra, Optus, Vodafone and TPG) is substantially greater than others.



Figure 17. Breakdown of Providers with the Most Enforcement Actions Taken Against Them

<sup>217</sup> The chart and the corresponding list below include eleven companies as some were the subject of the same number of actions. As noted in section D above, we use the term ‘provider’ to refer to companies including subsidiaries and associated companies investigated by the ACMA that essentially use the same name in the market. Accordingly, in Figure 17 and throughout this chapter: references to Telstra are to Telstra Corporation Ltd; reference to Optus include Optus Internet Pty Ltd, Optus Mobile Pty Ltd, Optus Networks Pty Ltd and Singtel Optus Pty Ltd; references to Vodafone include Vodafone Australia Pty Ltd, Vodafone Hutchison Australia Pty Ltd, Vodafone Network Pty Ltd and Vodafone Pty Ltd and Vodafone Network Pty Ltd; and references to TPG include TPG Telecom Limited and TPG Internet Limited.

<sup>218</sup> ‘Investigation Report and Direction to Comply: TPG Telecom Limited (Vodafone) – July 2023’, *Australian Communications and Media Authority* (Web Page, 26 July 2023) <<https://www.acma.gov.au/publications/2023-07/report/investigation-report-and-direction-comply-tpg-telecom-limited-vodafone-july-2023>>. The report lists the carriage service provider as ‘TPG Telecom Limited (in connection with Vodafone brand)’.

<sup>219</sup> ‘Investigation Report and Enforceable Undertaking: TPG Telecom Limited – December 2022’, *Australian Communications and Media Authority* (Web Page, 26 July 2023) <<https://www.acma.gov.au/publications/2022-12/report/investigation-report-and-enforceable-undertaking-tpg-telecom-limited-december-2022>>. The report lists the carriage service provider as ‘TPG Telecom Limited (trading as Lebara Australia, Lebara Mobile and Lebara) (CAN: 096 304 620)’.

The providers the ACMA publicly investigated the most were:

- Telstra: 23 investigations
- Optus: 12 investigations
- Lycamobile: 8 investigations
- TPG: 8 investigations
- SpinTel: 7 investigations
- Aussie Broadband: 6 investigations
- Dodo: 6 investigations
- Exetel: 6 investigations
- iTalkBB: 6 investigations
- Vodafone: 6 investigations.

The ACMA publicly took the most enforcement actions against:

- Telstra: 24 enforcement actions
- Lycamobile: 12 enforcement actions
- Optus: 11 enforcement actions
- SpinTel: 8 enforcement actions
- TPG: 8 enforcement actions
- Vodafone: 8 enforcement actions
- Dodo: 7 enforcement actions
- Exetel: 6 enforcement actions
- iTalkBB: 6 enforcement actions
- MyRepublic: 6 enforcement actions
- Southern Phone Company: 6 enforcement actions.

A short summary of the enforcement actions against each provider follows.

## 1 Enforcement Actions Against Telstra

The 24 enforcement actions against Telstra consisted of 7 formal warnings, 6 directions to comply, 3 remedial directions, and 4 infringement notices (totalling \$4,559,160). The ACMA also accepted 4 enforceable undertakings. There were no civil penalties.

These 24 enforcement actions were taken in 2012-13 (1), 2013-2014 (2), 2018-19 (6), 2019-20 (2), 2020-21 (4), 2021-2 (5) and 2022-23 (4).<sup>220</sup>

The enforcement actions against Telstra concerned breaches of:

- the TCP Code, including directions to comply with this code
- the Local Number Portability Code
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- Tel Act IPND obligations and the IPND Code

---

<sup>220</sup> The numbers in parentheses reflect the total number of enforcement actions in that year. The same applies to the equivalent numbers in each of these provider summaries below.

- number portability-related obligations, including Tel Act provisions relating to the Telecommunications Numbering Plan and the Telecommunications (Mobile Number Pre-porting Additional Identity Verification) Industry Standard 2020
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018 and Telecommunications (NBN Continuity of Service) Industry Standard 2018
- the Telecommunications (Emergency Call Service) Determination 2009
- the Telecommunications (Carrier Licence Conditions Telstra Corporation Limited) Declaration 2019 (arrangements for priority assistance).<sup>221</sup>

The largest infringement penalty notice issued to Telstra was in December 2021 for \$2.53 million. It was issued after the company failed to comply with its IPND obligations in almost 50,000 instances for its Telstra brand and in over 65,000 instances for its Belong brand. This notice followed previous the ACMA findings in 2019 that Telstra had breached the same obligations. In a December 2021 media release,<sup>222</sup> the ACMA acknowledged that Telstra had self-reported the issue. However, it suggested the infringement notice (along with a direction to comply) were issued because it was not the company's first major breach of the IPND rules. The same media release mentioned that the action was part of an ongoing campaign to improve IPND compliance and that the ACMA had taken similar action against a total of 26 telcos for non-compliance.

## 2 Enforcement Actions Against Lycamobile

The 12 enforcement actions against Lycamobile consisted of 2 formal warnings, 3 directions to comply, 1 remedial direction, and 4 infringement notices (totalling \$803,880). The ACMA also accepted 2 enforceable undertaking. There were no civil penalties.

The enforcement actions were taken in 2013-14 (2), 2015-16 (2), 2018-19 (1), 2020-21 (4), 2021-22 (2) and 2022-23 (1).

The enforcement actions against Lycamobile concerned breaches of:

- the TCP Code
- Tel Act IPND obligations and the IPND Code, as well as directions to comply with this code
- the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017, along with a remedial direction to comply with this determination
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

The TCP Code provisions breached included complaint handling obligations, the requirement to submit compliance attestation documentation, and billing accuracy.

---

<sup>221</sup> This list and equivalent lists in the remaining 'top 10' providers section exclude consequential breaches of the Tel Act (eg, a breach of s 101(1) of the Tel Act for failure to comply with a service provider rule). Note: the arrangements for priority assistance now apply to Telstra Limited because of s 63A of the Tel Act.

<sup>222</sup> 'Telstra Pays \$2.5 Million Penalty for Customer Privacy and Public Safety Failures', *Australian Communications and Media Authority* (Article, 16 December 2021) <<https://www.acma.gov.au/articles/2021-12/telstra-pays-25-million-penalty-customer-privacy-and-public-safety-failures>>.

As discussed in section C(1) above, in two separate but related investigations the ACMA found that Lycamobile committed numerous breaches of its IPND obligations between 2020-2022. These breaches resulted in six separate enforcement actions, including a direction to comply, an enforceable undertaking and an infringement notice resulting from the first investigation, along with a remedial direction for breach of the Prepaid Determination. The ACMA issued two infringement notices after the second investigation.

### 3 Enforcement Actions Against Optus

The 11 enforcement actions against Optus consisted of 5 formal warnings, 3 directions to comply and 2 remedial directions. The ACMA also accepted 1 enforceable undertaking.

Like Telstra and Lycamobile, no civil penalties were imposed on Optus. However, unlike Telstra and Lycamobile, Optus received no infringement notices. As such, it was not subject to any financial penalties for non-compliance with telecommunications consumer protection provisions during the period 1 January 2010 to 30 June 2023.

The enforcement actions were taken in 2010-11 (1), 2013-14 (1), 2018-19 (4), 2019-20 (1), 2020-21 (1), 2021-22 (2) and 2022-23 (1).

The enforcement actions against Optus concerned breaches of:

- the TCP Code, including rules relating to billing accuracy
- the Mobile Premium Services Code
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018
- the Telecommunications (NBN Continuity of Service) Industry Standard 2018
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- Telecommunications (Mobile Number Pre-porting Additional Identity Verification) Industry Standard 2020
- Tel Act IPND obligations and the IPND Code.

These breaches occurred for several reasons, including difficulties ensuring operational Next-Generation NBN Broadband Services, and deficiencies in information provision and number porting processes.

Optus had two investigations opened against it for contraventions of the Telecommunications Service Provider (NBN Service Migration) Determination 2018. Two enforcement actions were taken for these contraventions, including the remedial direction discussed in the case study in section C(1) relating to failures to fulfil obligations to provide consumers with accurate speed capacities for NBN broadband services and to refrain from charging for non-operational offerings. This remedial direction was one of two Optus received over the period, the other being for contraventions of the IPND Code.

### 4 Enforcement Actions Against SpinTel

The 8 enforcement actions against SpinTel consisted of 4 formal warnings and 3 directions to comply. The ACMA accepted one enforceable undertaking from SpinTel.

The five enforcement actions were taken in 2013-14 (1), 2014-15 (1), 2015-16 (2), 2018-19 (2), 2021-22 (1) and 2022-23 (1).

The enforcement actions SpinTel concerned breaches of:

- the IPND Code
- the TPC Code
- the Tel Act IPND rules
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- priority assistance-related obligations.

Two of these actions arose out of the same investigation involving the IPND obligations, after SpinTel failed to ensure that the phone numbers and name and address details of 426 customers were classified as silent lines when uploading data to the IPND. As a result, the details were published in online public number directories and, in some cases, hard copy directories. In October 2015 the ACMA issued a direction to comply with the IPND Code. It also accepted an enforceable undertaking.

## 5 Enforcement Actions Against TPG

The 8 enforcement actions against TPG included 2 formal warnings, 2 directions to comply and 1 civil penalty. The ACMA also accepted 3 enforceable undertakings. The ACMA did not issue any infringement notices against TPG.

The enforcement actions were taken in 2009-10 (1), 2013-14 (1), 2018-19 (2), 2019-20 (1), 2021-22 (1) and 2022-23 (2).

The enforcement actions against TPG concerned breaches of:

- the TCP Code, including provisions relating to complaint handling and to credit and debt management
- the Telecommunications (Emergency Call Service) Determination 2009
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- the Telecommunications (Service Provider Identity Checks for Prepaid Mobile Carriage Services) Determination 2017
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018
- priority assistance-related obligations.

Two enforceable undertakings related to the Telecommunications Service Provider (NBN Service Migration) Determination 2018. The third enforceable undertaking related to the Telecommunications (Service Provider Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

The reasons for the civil penalty are explained in section C(2) above.

It is important to note that the 8 enforcement actions described here exclude all enforcement actions taken against AAPT, Soul Communications Pty Ltd, iiNet, Internode, TransACT Capital Communications, and TransACT Communications – providers that TPG acquired between 9 December 2013 and 13 March 2015. Further, as noted at the beginning of section D, the 8 enforcement actions described here exclude all actions against Vodafone made before its merger with TPG in 2020 (see separate note on TPG Group below).



## 6 Enforcement Actions Against Vodafone

The 8 enforcement actions against Vodafone included 3 formal warnings, 3 directions to comply and 1 remedial direction. The ACMA also accepted 1 enforceable undertaking from Vodafone. No civil penalties were imposed.

The enforcement actions were taken in 2011-12 (2), 2012-13 (1), 2017-18 (1) and 2018-19 (4).

The enforcement action against Vodafone concerned breaches of:

- the TCP Code
- Tel Act IPND obligations and the IPND Code
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013.

Vodafone's breaches involved failures to:

- provide charging information
- submit updated data for the IPND manager
- establish effective complaints-handling processes; and
- provide accurate consumer information and descriptions of telecommunications products.

Vodafone's breaches of the IPND-related obligations resulted in both a direction to comply and a remedial direction. Vodafone also contravened the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 by failing to include matters such as timeframes, escalation, and consumer rights in its compliant complaints-handling process. To date, breaches of the Complaints Standard often result in formal warnings from the ACMA, which was also the case for Vodafone's breach.

As mentioned earlier, Vodafone merged with TPG in 2020, but we have treated them as separate providers here due to their independence from one another for most of the report's timespan. It should be noted, however, that since the merger, one action made against TPG Telecom was in relation to the Vodafone brand.<sup>223</sup> As noted above, this has been counted against the overall TPG numbers and is not reflected in the count of enforcement actions against Vodafone in this section. This enforcement action was a direction to comply, given for failing to adhere to the TCP Code's debt and credit management provisions. See the separate note on TPG Group below for more information.

## 7 Enforcement Actions Against Dodo

The 7 enforcement investigations against Dodo included 6 formal warnings. The ACMA accepted 1 enforceable undertaking from Dodo.

The 7 enforcement actions were taken in 2013-14 (1), 2014-15 (1), 2018-19 (2) and 2019-20 (3).

The enforcement actions concerned breaches of:

---

<sup>223</sup> See ACMA (n 218).

- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- the Tel Act IPND rules and the IPND Code
- the TCP Code
- the priority assistance requirements
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018.

The enforceable undertaking was accepted following Dodo's breach of the Telecommunications Service Provider (NBN Service Migration) Determination 2018. In the undertaking, among other things, Dodo promised to maintain the voluntary and remedial improvements it had already made to its systems and processes prior to the ACMA issuing its findings and to review the effectiveness of those improvements for four consecutive quarters.

## 8 Enforcement Actions Against Exetel

The 6 enforcement actions against Exetel consisted of: 2 formal warnings, 2 directions to comply and 2 infringement notices (totalling \$25,920). The ACMA did not accept enforceable undertakings from Exetel.

The enforcement actions were taken in 2018-19 (2), 2019-20 (2) and 2022-23 (2).

The enforcement actions concerned breaches of:

- the TCP Code and a direction to comply with this code
- the Telecommunications (Consumer Complaints) Record-Keeping Rules 2018
- the priority assistance requirements.

The infringement notices were issued following breaches of a direction to comply with the TCP Code and the Telecommunications (Consumer Complaints) Record-Keeping Rules 2018.

## 9 Enforcement Actions Against iTalkBB

The ACMA took 6 enforcement actions against iTalkBB: 2 formal warnings, 3 directions to comply and 1 infringement notice with the value of the infringement notice being unknown. The ACMA did not accept any enforceable undertakings from iTalkBB.

The 6 enforcement actions were taken in 2012-13 (1), 2013-14 (1), 2014-15 (1), 2015-16 (2), and 2017-18 (1).

It appears that all enforcement actions against iTalkBB concerned breaches of the TCP Code, including the provision of compliance documentation to CommCom, the provision of critical information summaries to consumers, and direct debt payment obligations. The infringement notice was issued following breach of a direction to comply with the TCP Code.<sup>224</sup>

## 10 Enforcement Actions Against MyRepublic

The ACMA took 6 enforcement actions against MyRepublic: all 6 actions were formal warnings.

---

<sup>224</sup> According to the ACMA's online list of investigations into telecommunications providers, the infringement notice was given for failure to provide compliance statements to CommCom pursuant to TCP Code Chapter 9. We were unable to find any further information on this enforcement action. As infringement notices cannot be given for code of practice breaches alone, this infringement notice is most likely related to a breach of a previous direction to comply with these TCP provisions.

The 6 enforcement actions were taken in 2018-19 (3), 2019-20 (2) and 2022-23 (1).

The enforcement actions concerned breaches of:

- the TCP Code, including the provision of compliance documentation to CommCom
- the Tel Act IPND rules and the IPND Code
- the priority assistance requirements
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018.

## 11 Enforcement Actions Against Southern Phone Company

The ACMA took 6 enforcement actions against Southern Phone Company: 1 formal warning and 4 directions to comply. The ACMA accepted 1 enforceable undertaking from Southern Phone Company.

The 6 enforcement actions were taken in 2014-15 (2), 2017-18 (1), 2018-19 (1), 2021-22 (1) and 2022-23 (1).

The enforcement actions concerned breaches of:

- the TCP Code
- the Tel Act IPND obligations and the IPND code
- the priority assistance requirements.

### Additional Note on the TPG Group

In June 2020, TPG Telecom and Vodafone Hutchison Australia merged by way of a scheme of arrangement. In view of the significant market share now held by the merged entity (referred to here as the TPG group for simplicity), here we provide a short summary of the enforcement actions taken against providers that make up the TPG group during the period of this report. This includes the enforcement actions against the pre-merger TPG and Vodafone companies, their subsidiaries, and the other service providers they acquired over the period. The companies they acquired, and which were the subject of enforcement actions, are AAPT, Agile, Chime, iiNet, Internode, PowerTel, Soul Communications, TransACT Capital Communications, TransACT Communications, and Westnet. Most of these companies were acquired by TPG or a company that was later acquired by TPG, such as iiNet.

We conduct this analysis in an effort to present an overall picture of the ACMA's enforcement activities in relation to what is now the TPG group. The data reflects the number of enforcement actions taken against each company since it was acquired by TPG or Vodafone. This means enforcement actions while the company was independent or owned by a non-TPG Group company are not counted. For example, TPG acquired control of AAPT's consumer division in August 2015 when TPG purchased iiNet – which at the time controlled AAPT. As enforcement actions against AAPT are only counted in this section if occurring after August 2015, a formal warning issued to AAPT in 2012-13 is not included here.<sup>225</sup>

We start this analysis by addressing the enforcement actions against the post-merger TPG group (item 1). We then highlight the pre-merger enforcement actions made against TPG and

---

<sup>225</sup> Lebara is also in the group of companies acquired during the period (it was acquired by Vodafone in September 2016: see 'Our History', *iiNet* (Web Page) <<https://www.iinet.net.au/about-us/history>>) but enforcement actions taken against it occurred before the acquisition by Vodafone and after the merger of Vodafone and TPG.

Vodafone – the main providers making up the group (items 2 & 3). We follow this by providing the enforcement actions made against companies acquired by TPG and Vodafone over the reporting period (items 4 onwards). A count and breakdown of enforcement actions across the group is provided at the end of this section.

1. **TPG group (post-merger):** Since the merger in 2020, the ACMA has taken a total of 3 enforcement actions against the merged entity. This includes 2 enforcement actions against TPG Telecom (the group's Australian parent company) and 1 enforcement action against TPG Internet (a subsidiary providing internet and mobile services under the TPG brand). The enforcement actions against TPG Telecom include an enforceable undertaking accepted by the ACMA in December 2022 for contraventions of the Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 in connection with the group's Lebara brand (acquired by Vodafone in 2016) and a direction to comply with the TCP code in June 2023 for services provided by the Vodafone brand. The ACMA also accepted an enforceable undertaking from TPG Internet to address contraventions of the Telecommunications Service Provider (NBN Service Migration) Determination 2018.
2. **TPG (pre-merger):** the ACMA took 5 enforcement actions against TPG prior to the merger. These included 2 formal warnings, 1 direction to comply and 1 civil penalty order by the Federal Court. The ACMA also accepted 1 enforceable undertaking.
3. **Vodafone (pre-merger):** as detailed above, the ACMA took 8 enforcement actions against Vodafone, including 3 formal warnings, 3 directions to comply and 1 remedial direction. The ACMA also accepted 1 enforceable undertaking. Since Vodafone formed the TPG Telecom Group with its merger with TPG in June 2020, enforcement actions tied to the Vodafone brand have been directed against TPG Telecom, the group's parent company.
4. **Soul Communications** resulted from the merger of TPG and Soul in 2008-09.<sup>226</sup> The ACMA has taken 2 enforcement actions against Soul since its acquisition by TPG. The first was an enforceable undertaking in May 2010 after the ACMA determined Soul Communications had breached the Tel Act's IPND rules. The second action was a direction to comply with the TCP Code in April 2010.
5. **PowerTel** was acquired by TPG in December 2013 when it purchased Telecom New Zealand Australia Pty Limited.<sup>227</sup> The ACMA took 2 enforcement actions against PowerTel in February 2019: 1 direction to comply and 1 remedial direction. PowerTel had contravened the IPND Code and the Tel Act's IPND rules.
6. **iiNet** has been owned by TPG since August 2015.<sup>228</sup> In total, the ACMA has taken 2 enforcement actions against iiNet since its acquisition by TPG. They consisted of 1 formal warning and 1 remedial direction. In December 2018, iiNet was found to have breached the Telecommunications (Consumer Complaints Handling) Industry Standard 2018, which resulted in the formal warning. In November 2019, it was found to have breached the Telecommunications (NBN Continuity of Service) Industry Standard 2018 and Telecommunications Service Provider (NBN Service Migration) Determination 2018, which resulted in the remedial direction.

---

<sup>226</sup> See, eg, 'Telco Giant Formed After Soul Merges with TPG', iNews (8 February 2008) <<https://www.itnews.com.au/news/telco-giant-formed-after-soul-merges-with-tpg-102956>>.

<sup>227</sup> TPG, 'TPG Telecom Announces Acquisition of AAPT' (Media Release, 9 December 2013) <[https://www.tpg.com.au/about/pdfs/TPG\\_Telecom\\_Announces\\_Acquisition\\_of\\_AAPT.PDF](https://www.tpg.com.au/about/pdfs/TPG_Telecom_Announces_Acquisition_of_AAPT.PDF)>.

<sup>228</sup> ACMA, *Communications Report 2015-16* 35.

7. **AAPT's** consumer division was acquired by iiNet in October 2010<sup>229</sup> and was then acquired by TPG with TPG's purchase of iiNet. The ACMA took 2 enforcement actions against AAPT in February 2019: 1 direction to comply and 1 remedial direction. AAPT had contravened the IPND Code and the Tel Act's IPND rules.
8. **Agile** was acquired by iiNet in December 2011<sup>230</sup> and by TPG in August 2015 when TPG purchased iiNet. The ACMA took 2 enforcement actions against Agile in February 2019: 1 direction to comply and 1 remedial direction. Agile had contravened the IPND Code and the Tel Act's IPND rules.
9. **Chime** was launched by iiNet in 2001<sup>231</sup> and was acquired by TPG in August 2015 when TPG purchased iiNet. The ACMA took 2 enforcement actions against Chime in February 2019: 1 direction to comply and 1 remedial direction. Like Agile, Chime had contravened the IPND Code and the Tel Act's IPND rules.
10. **Internode** was acquired by iiNet in December 2011<sup>232</sup> and by TPG in August 2015 when it purchased iiNet. Since then, the ACMA has taken 1 enforcement action against Internode. It issued the company with a formal warning in December 2018 for breaching the Telecommunications (Consumer Complaints Handling) Industry Standard 2018.
11. **TransACT Capital Communications** and **TransACT Communications** were acquired by iiNet in December 2011<sup>233</sup> and by TPG in August 2015 when TPG purchased iiNet. The ACMA took 4 enforcement actions in total against the two TransACT companies: 2 directions to comply and 2 remedial directions. Like Agile, Chime, and Powertel, 1 direction to comply and 1 remedial direction were issued against each TransACT company in February 2019 for contravention of the IPND Code and the Tel Act's IPND rules.
12. **Westnet** was acquired by iiNet in 2008<sup>234</sup> and by TPG in August 2015 when TPG purchased iiNet. Since then, the ACMA has taken 1 enforcement action against Westnet. It issued the company with a formal warning in December 2018 for breaching the Telecommunications (Consumer Complaints Handling) Industry Standard 2018.

Our review of ASX, ASIC and other data suggests that the number of enforcement actions against the TPG group, including actions against all subsidiaries while under TPG or Vodafone ownership, is 34. These 34 enforcement actions comprise:

- 8 formal warnings
- 12 directions to comply
- 8 remedial directions
- 1 civil penalty
- 5 enforceable undertakings.

The enforcement actions were taken in 2009-10 (3), 2011-12 (2), 2012-13 (1), 2013-14 (1), 2017-18 (1), 2018-19 (21), 2019-20 (2), 2021-22 (1) and 2022-23 (2).

In summary, the enforcement actions against the TPG group of companies concerned breaches of:

- the IPND Code and the Tel Act's IPND rules

<sup>229</sup> ACMA, *Communications Report 2010-11* 97.

<sup>230</sup> ACMA, *Communications Report 2010-11* 97.

<sup>231</sup> iiNet, *Our History* <<https://www.iinet.net.au/about-us/history>>.

<sup>232</sup> 'Our History', *iiNet* (Web Page) <<https://www.iinet.net.au/about-us/history>>.

<sup>233</sup> *Ibid.*

<sup>234</sup> 'About Westnet', *Westnet* (Web Page) <<https://www.westnet.com.au/about/>>.

- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018
- the Telecommunications (NBN Continuity of Service) Industry Standard 2018
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018
- the Telecommunications (Emergency Call Service) Determination 2009
- the Telecommunications (Service Provider Identity Checks for Prepaid Mobile Carriage Services) Determination 2017
- priority assistance-related obligations
- the TCP Code, including provisions relating to complaint handling and to credit and debt management.

## E Provisions with the Most Enforcement Actions in Published Investigations

The provisions (or combinations of provisions) that attracted the most enforcement actions in published investigations involved the following.

- The obligation to provide Communications Compliance with compliance attestation documentation.<sup>235</sup> Attestation documentation explains if and how service providers are compliant with the TCP Code. The documentation must be endorsed by the company's CEO or some other senior manager. There were 240 enforcement actions relating to these requirements.
- Provision of IPND-related information.<sup>236</sup> The Tel Act requires carriage service providers to give certain information to Telstra which is required by its carrier licence to provide and maintain the integrated public number database. Under Industry Code (C555) Integrated Public Number Database, carriage service providers must (among other things) provide specified customer data for each public telephone number they assign to a customer to the Integrated Public Number Database Manager (IPND Manager).<sup>237</sup> The IPND Manager stores this information in a register which can be used by emergency services. There were 73 enforcement actions relating to IPND requirements. Of these, 38 are related to the Tel Act obligations and 35 are related to the IPND Code obligations.
- Provisions relating to complaints handling.<sup>238</sup> Telecommunications providers are required to establish complaints handling mechanisms and to have proper mechanisms in place to handle and resolve customer complaints. There were 49 enforcement action relating to these requirements.
- Provisions in the TCP Code relating to advertising and the provision of information to customers.<sup>239</sup> For example, clause 4.1 of the current code imposes rules around the content of advertising, such as the use of terms 'unlimited' or 'free', while clause

<sup>235</sup> This requirement came into effect from March 2013. It was in Chapter 9 of the 2012 version of the TCP Code which became Chapter 10 in the 2019 version.

<sup>236</sup> This is required by Tel Act sch 2, cl 10 and Industry Code (C555) Integrated Public Number Database.

<sup>237</sup> See cls 4.2.1, 4.2.11 and 4.2.25.

<sup>238</sup> See s 128(1) of the Tel Act and the Telecommunications (Consumer Complaints Handling) Industry Standard 2018. Before the standard was introduced, complaints handling rules were found in Chapter 9 (until 2012) and then Chapter 8 (until 2019) of the TCP Code.

<sup>239</sup> These provisions are found in cls 4.1 to 4.4 of the current 2019 version of the TCP Code. In previous versions, at least cls 4.1 and 4.2 dealt with advertising and the provision of information.

4.2 requires the provision of a Critical Information Summary of current offers. There were 35 enforcement actions relating to these requirements.

- Requirements relating to the TIO scheme. Carriers and service providers are required to join the TIO scheme and to comply with it.<sup>240</sup> There were 28 enforcement actions relating to these obligations. 19 of these related to requirements to join the scheme, while 9 related to failure to comply with scheme determinations.

The high number of actions relating to the first of these – the requirement to provide compliance attestation documentation – is perhaps explained by the involvement of Communications Compliance in receiving the documentation and reporting on compliance with this obligation. In 2013, after the establishment of Communications Compliance and the commencement of the Code Compliance Framework in (what was then) Chapter 9 of the TCP Code, the ACMA undertook a major audit of compliance with these requirements, which resulted in 99 enforcement actions, 95 formal warnings and 4 directions to comply.<sup>241</sup>

The other obligations that are most actively enforced likely appear in the list due to their importance to public safety (such as those related to IPND) or the potential scale of their impact on consumer experiences (those related to the TIO scheme, complaints handling, and advertising and information requirements).

It is also important to keep in mind that the ACMA has considerable discretion in exercising its powers. For lower-priority matters involving minor harm or non-compliance, the ACMA may choose to pursue informal resolutions or undertake activities to encourage voluntary compliance, such as education, guidance, persuasion, or negotiation. As the ACMA does not comprehensively report on all of these activities, it is hard to draw further insights into the attention these matters receive from the ACMA.

## F Most Common Enforcement Actions in Published Investigations

Figure 18 below provides a visual breakdown of how each enforcement action related to the provisions breached. The most common enforcement actions were formal warnings and directions to comply. 296 of the 502 enforcement actions were formal warnings; 119 were directions to comply.

The **formal warnings** involved warnings to comply with:

- the TCP Code rules relating to offers, advertising, billing, customer service (ie, the privacy of customer billing and related personal information), credit and debt management, including financial hardship<sup>242</sup> and spend management tools, changing suppliers, complaints handling (when those rules were included in the TCP Code), implementation and compliance with the Code compliance framework and registration with Comms Alliance for compliance purposes, and the provision of compliance attestation documentation to CommCom;

---

<sup>240</sup> See ss 128 and 132 of the TCPSS Act. Note that under cl 1 of Schedule 2 of the Tel Act, compliance with the requirements of the TCPSS Act is a service provider rule.

<sup>241</sup> See, eg, Australian Communications and Media Authority, *Annual Report 2013-2014* (Report, 30 September 2014) 80, Table 26.

<sup>242</sup> At the time of writing the TCP Code has not yet been amended to remove and/or reflect any consequential changes to the chapter dealing with financial hardship rules required because of the ACMA's decision to adopt the Telecommunications (Financial Hardship) Industry Standard 2024. This is likely to change on 29 March 2024, when the standard commences.

- the obligation in the TCPSS Act to join the TIO scheme;<sup>243</sup>
- industry standards, including the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 and Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020;
- IPND rules in the IPND Code and Tel Act;<sup>244</sup>
- priority assistance rules (ie, the obligation to notify residential customers they do not offer priority assistance and inform them of the providers who do);<sup>245</sup> and
- the Reducing Scam Calls and Scam SMS Code.

Of the 296 formal warnings, 215 were in relation to the TCP Code; 9 concerned the TCPSS Act obligation to join the TIO scheme; 33 concerned industry standards; 15 concerned the IPND Code; 10 concerned the Tel Act IPND rules; 11 concerned the priority assistance rules; and 3 concerned the Reducing Scam Calls and Scam SMS Code.

The **directions to comply** concerned:

- the TCP Code rules, including the general rules, and the offers, advertising, billing, credit and debt management, financial hardship,<sup>246</sup> complaint handling (when those rules were included in the TCP Code), compliance and monitoring, changing supplier obligations, implementation and compliance with the Code compliance framework and registration with Comms Alliance for compliance purposes, and the provision of compliance attestation documentation to CommCom;
- various provisions in the Mobile Premium Services Code, especially those relating to advertising and providing information to customers;
- provisions in the Reducing Scam Calls and Scam SMS Code concerning improving number and alphanumeric sender ID accuracy;
- rules in the IPND Code for data provision to IPND manager and data accuracy;<sup>247</sup> and
- rules in the Local Number Portability Code involving the number porting process.<sup>248</sup>

Of the 119 directions to comply, 86 were in relation to the TCP Code; 10 to the MPS Code; 3 to Reducing Scan Calls and Scam SMS Code, 18 to the IPND Code, 1 to the LNP Code and 1 for both the TCP and IPND codes.

The ACMA has not exercised its s 130 TCPSS Act power to issue a direction to comply with the requirement to join the TIO. Instead, it has elected to issue formal warnings and remedial directions in its efforts to secure industry compliance with the obligation.

---

<sup>243</sup> See ss 128 and 132 of the TCPSS Act. Note that under cl 1 of Schedule 2 of the Tel Act, compliance with the requirements of the TCPSS Act is a service provider rule.

<sup>244</sup> For example, clauses 4.2.1 and 4.2.25 of the IPND Code; Tel Act sch 2 cl 10(2).

<sup>245</sup> Tel Act Schedule 2 para 19(2).

<sup>246</sup> See n 242.

<sup>247</sup> Communications Alliance, *Integrated Public Number Database (IPND) Industry Code* (at March 2020) cls 4.2.1, 4.2.11, 4.2.16, 4.2.25, 5.1.11.

<sup>248</sup> Communications Alliance, *Local Number Portability Code* (at May 2023) cls 4.3.9, 4.4.6, 7.1.4, 7.1.7.



**Remedial directions** concerned:

- the obligation to provide to the IPND Manager information needed to provide and maintain the IPND;<sup>249</sup>
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018;
- the Telecommunications (NBN Continuity of Service) Industry Standards 2018;
- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018;
- the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination;
- the TCPSS Act obligations to join and to comply with the TIO scheme;<sup>250</sup> and
- Telstra’s priority assistance obligations in its carrier licence.

Of the 41 remedial directions:

- 16 concerned the Tel Act IPND obligations;
- 9 concerned the TCPSS Act obligations to join the TIO;
- 6 concerned the TCPSS Act obligations to comply with the TIO scheme;
- 4 concerned the Telecommunications (Consumer Complaints Handling) Industry Standard 2018;
- 2 concerned the Telecommunications Service Provider (NBN Service Migration) Determination 2018;
- 1 concerned both the Telecommunications (NBN Continuity of Service) Industry Standard 2018 and the Telecommunications Service Provider (NBN Service Migration) Determination 2018;
- 1 concerned the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination;
- 1 concerned both the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 and the Telecommunications (NBN Consumer Information) Industry Standard 2018; and
- 1 concerned Telstra’s priority assistance obligations in its carrier licence.

Remedial directions to comply with the Tel Act IPND obligation to provide information to Telstra were often accompanied by directions to comply with the IPND Industry Code. This was the case in February 2019 when the ACMA took enforcement action against AAPT Limited, Agile, Chime Communications, Optus, PowerTel, Primus Telecommunications, Symbio Networks, Telstra, and TransACT Communications for breach of the IPND Industry Code. As seen in the enforcement actions against Telstra, Lycamobile, Optus and Vodafone in section 4(D) above, the ACMA has maintained a focus on industry compliance with IPND rules (regardless of whether they are set out in direct regulation or a co-regulatory instrument like the IPND Code).

Telstra was issued with the most remedial directions: 3. Netfast, Optus and TransAct Communications were each issued with 2. Thirty-two other providers were issued with 1.

---

<sup>249</sup> Tel Act sch 2 cl 10(2).

<sup>250</sup> TCPSS Act ss 128 and 132.

Without access to all published investigation reports and enforcement instruments, it is not possible to make any further observations about the way in which the ACMA has exercised its powers to issue formal warnings, directions to comply and remedial directions.

**Infringement notices** were issued for breaches of:

- the IPND service provider rules in Schedule 2 of the Tel Act;
- the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020;
- the Telecommunications (Consumer Complaints) Record-Keeping Rules 2018;
- the Telecommunications (NBN Consumer Information) Industry Standard 2018, the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017;
- the Telecommunications Numbering Plan 2015;
- directions to comply with the TCP and IPND codes, a remedial direction relating to the TCPSS Act obligations to join the TIO scheme, and a remedial direction relating to the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

Infringement notices were issued less frequently than any other administrative enforcement mechanism. This is most likely because of the relatively limited circumstances, outlined in Chapter 2, in which the ACMA may issue them. For an example of an occasion on which a large fine was imposed, see the Lycamobile *Case Study: Infringement notice* in section C(1) above.

Telstra and Lycamobile were issued with the most infringement notices: 4. Exetel, Aussie Broadband and Circles Australia each received 2. Ten other providers each received 1.<sup>251</sup> In the case of a single infringement fine, the amount increased over the period covered in this report from \$10,200 in March 2014 to \$13,320 in July 2022. This increase is reflective of changes over time in the value of the standard penalty unit.<sup>252</sup> The total amount of infringement notices issued by the ACMA between 1 January 2010 and 30 June 2023 was \$6,143,160.

The infringement notices with the highest and second highest value - \$2,530,800 and \$1,512,000, respectively - were made against Telstra. This result may be because breaches by larger providers, especially those involving any automated systems, affect more customers and have the potential to cause greater harm. This provider also has access to significant resources, meaning more severe action is likely to be less burdensome.<sup>253</sup>

As explored in the case studies in section C(2), three **civil penalties** have been issued by the Federal Court. These primarily related to situations where there were repeated failures to comply with determinations made by the TIO or where issues of public safety were concerned. TPG, for example, failed to ensure that its controlled networks and/or controlled facilities gave the end users of 5,979 standard telephone services access to the Triple Zero emergency service. The Bytecard litigation followed two remedial directions regarding non-compliance with

---

<sup>251</sup> The ten other service providers were: iTalkBB, Australian Private Networks (trading as active8me), Netfast, Business Service Brokers (trading as TeleChoice), Simply NBN, David John Esmonde, Flip TV, Exceed Connect, MyNetFone, and Mate Communicate.

<sup>252</sup> 572G Tel Act; Telecommunications (Infringement Notice Penalties) Determination 2012.

<sup>253</sup> On the regulatory policy of not imposing undue financial and administrative burdens on industry participants, see Chapter 3, section A.

five determinations made by the TIO. The Limni litigation followed a failure to comply with seven TIO determinations.

A single **mandatory injunction** was also issued by the Federal Court against Bytecard and Brian Morris.<sup>254</sup> It granted the ACMA's request to impose a compliance program on Bytecard and Mr Morris. As part of the case, the ACMA had also requested for the court to impose an additional injunction requiring compensation payments to affected customers. However, this was deemed unnecessary as Bytecard had compensated the affected customers prior to the date of the hearing.<sup>255</sup>

Seventeen **enforceable undertakings** have been accepted by the ACMA for breaches of the following regulatory instruments:

- IPND service provider rules in Schedule 2 of the Tel Act;
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018;
- the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 2019;
- the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017;
- the Telecommunications (Emergency Call Service) Determination 2009;
- the Telecommunications (NBN Continuity of Service) Industry Standard 2018; and
- the Telecommunications Service Provider (NBN Service Migration) Determination 2018.

Enforceable undertakings were accepted most frequently for Tel Act IPND-related breaches. IPND-related enforceable undertakings were accepted by the ACMA on 6 occasions, once each from Circles Australia, Lycamobile, Macquarie Telecom, Southern Phone Company, SpinTel and Soul Communications. Enforceable undertakings were accepted on three occasions, twice from TPG and once from Dodo, for breaches of the Telecommunications Service Provider (NBN Service Migration) Determination 2018. Lycamobile, TPG, and Vodafone each gave one enforceable undertaking for breaches of the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017. The ACMA also accepted three enforceable undertakings, two from Telstra and one from Optus, for breaches of both the Telecommunications Service Provider (NBN Service Migration) Determination 2018 and the Telecommunications (NBN Continuity of Service) Industry Standard 2018. Breaches of the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 2019 and the Telecommunications (Emergency Call Service) Determination 2009 gave rise to one enforceable undertaking each, both of which were given by Telstra.

The ACMA accepted 4 enforceable undertakings from Telstra. It accepted 3 from TPG, 2 from Lycamobile and 1 from each of Circles Australia, Dodo, Macquarie Telecom, Vodafone, Optus, Soul Communications, Southern Phone, and SpinTel.

Finally, one outlier in the data was the enforcement of a 'Deed of Agreement' from the 2012-13 reporting period against Startel. This was in relation to a breach of the TCP Code (presumably Clause 5.5.1 relating to Charging and Billing Accuracy) after Startel admitted to the ACMA that there was a billing system error that was rectified within 24 hours of being demonstrated. The deed required Startel to contact all affected customers within 30 days and reimburse them within three weeks of notification. Although the ACMA is not empowered to accept an enforceable undertaking for breach of a code of practice, it is able to enter a deed with a provider.

---

<sup>254</sup> *Australian Communications and Media Authority v Bytecard Pty Ltd* [2013] FCA 38.

<sup>255</sup> *Ibid.* See para 72.

Figure 18 provides a breakdown of enforcement actions by type and regulatory instruments breached. Where multiple enforcement actions arise from the breach of one instrument, these are attributed to that original breach. For example, a breach of an industry code may lead to a direction to comply, and a breach of that direction (also a breach of the Tel Act) may lead to an infringement notice being issued. In Figure 18, both the direction to comply and the infringement notice would be attributed to the breach of the industry code. This approach is adopted even if the direction only imposed reporting or similar obligations that did not relate directly to the rules that were the subject of the original breach.

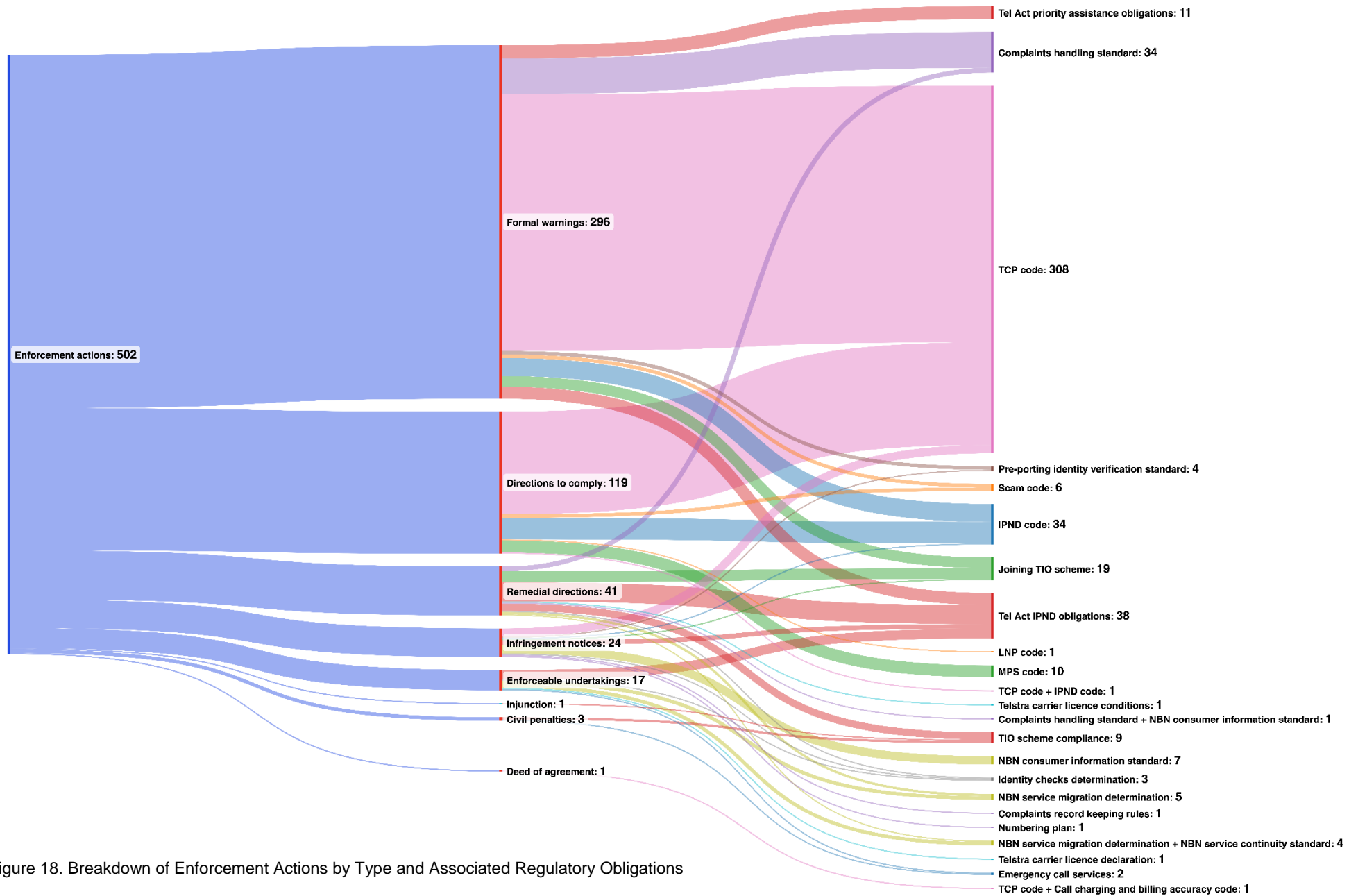


Figure 18. Breakdown of Enforcement Actions by Type and Associated Regulatory Obligations

## G Years When the ACMA Engaged in the Least and Most Enforcement Activity

Within the set of publicised enforcement actions, the least number of enforcement actions were taken in 2011-12 when the ACMA took only 4. The highest number of actions were taken in 2013-14 (115), followed by 2018-19 (79) and 2014-15 (64). If the total of 502 enforcement actions is averaged over the 13.5-year period examined here, the ACMA took just over 37 actions per year.

Each of the 26 directions to comply issued in 2012-13, 2013-14, and 2014-15 related to the TCP Code and might be a consequence of the ACMA's interest in that code following its Reconnecting the Customer Inquiry, which began in 2010 and concluded in September 2011 with the publication of the *Reconnecting the Customer: Final Public Inquiry Report*. Within that period, 104 formal warnings were issued in 2013-14, 95 of which can be attributed to the ACMA's review of compliance with TCP Code requirements for information to be provided to CommCom.

In the five-year period 2018-19 to 2022-23, the ACMA took 211 enforcement actions; while this is lower than the 259 actions it took in the previous five years, the results for the earlier period are affected by the compliance audits (following the establishment of Communications Compliance and the introduction of the Compliance Framework under the TCP Code) which led to the 95 formal warnings mentioned above.

It should be noted that a count of enforcement actions does not provide an indication of the complexity of the matters concerned including the obligations breached or severity of breaches. Since 1 July 2018, the ACMA has issued remedial directions and infringement notices and accepted enforceable undertakings more frequently; this could suggest a stronger approach to enforcement than in previous years. It may also reflect the specific types of regulatory rules breached.

	<i>Formal warning</i>	<i>Enforceable undertaking</i>	<i>Direction to comply</i>	<i>Remedial direction</i>	<i>Infringement notice</i>	<i>Deed of agreement</i>	<i>Civil penalty action</i>	<i>Injunction</i>	<i>Total for reporting period</i>
<b>2009-10</b>	0	1	6	0	0	0	0	0	<b>7</b>
<b>2010-11</b>	0	0	7	1	0	0	0	0	<b>8</b>
<b>2011-12</b>	0	0	3	1	0	0	0	0	<b>4</b>
<b>2012-13</b>	6	0	3	2	0	1	1	1	<b>14</b>
<b>2013-14</b>	104	1	7	1	1	0	1	0	<b>115</b>
<b>2014-15</b>	42	1	16	5	0	0	0	0	<b>64</b>
<b>2015-16</b>	27	2	10	1	4	0	0	0	<b>44</b>
<b>2016-17</b>	15	0	9	1	0	0	0	0	<b>25</b>
<b>2017-18</b>	5	1	4	0	0	0	0	0	<b>10</b>
<b>2018-19</b>	49	1	11	16	2	0	0	0	<b>79</b>
<b>2019-20</b>	27	4	11	8	7	0	0	0	<b>57</b>
<b>2020-21</b>	8	1	3	1	2	0	0	0	<b>15</b>
<b>2021-22</b>	2	2	5	3	4	0	0	0	<b>16</b>
<b>2022-23</b>	11	3	24	1	4	0	1	0	<b>44</b>
<b>Total for enforcement type</b>	<b>296</b>	<b>17</b>	<b>119</b>	<b>41</b>	<b>24</b>	<b>1</b>	<b>3</b>	<b>1</b>	<b>502</b>

**Table 1: Total Number of the ACMA Enforcement Actions Each Year**

Note: Dates were unable to be found for two enforcement actions.

- An entry relating to an infringement notice for Exceed Connect published on the ACMA's website had no specified date. The current website list does not provide dates for matters that occurred between December 2015 and March 2017. It does not appear on an earlier list of the ACMA's 'Telecomms investigation reports' available from the WayBack machine. It does not appear in the ACMA's Annual Reports. We have assumed it was issued in 2015-16 because of its close proximity to the infringement notice issued to the online entry for David John Esmonde trading as Aunix. The ACMA's *Annual Report 2015-16* indicates the infringement notice against David John Esmonde was issued in 2015-2016.<sup>256</sup>
- Similarly, an entry relating to an infringement notice for iTalkBB was listed on the ACMA's website as having occurred between 2010-2016. It also does not appear in earlier website material or in the ACMA's Annual Reports. We have allocated it to 2015-16 for the same reasons as the above Exceed Connect entry.

<sup>256</sup> See 'Investigations into Telco Providers 2010-2016' (<<https://www.acma.gov.au/investigations-telco-providers-2010-2016>>) for the page on the current the ACMA website and 'Telecomms investigation reports' (<<https://web.archive.org/web/20160229032612/http://acma.gov.au/theACMA/ACMAi/Investigation-reports/Telco-investigations/acma-telecommunications-investigation-reports>>) for the page archived by the WayBack Machine on 29 February 2016. Both pages were accessed on 15 February 2024.

## Conclusion

In this report, we have provided an overview of the two highly influential strategies of regulation that have informed and continue to inform the ACMA's approach to enforcement and compliance: responsive regulation and risk-based regulation. The former is often associated, including in the work of the ACMA, with the enforcement pyramid which aims to ensure compliance with minimum standards. The latter is widely adopted in Australia and is embedded in public governance legislation that applies to all Commonwealth entities.

We have explained that the ACMA has a range of administrative, civil and criminal mechanisms to enforce the consumer protection-related provisions that are the focus of this report. Its administrative mechanisms comprise formal warnings, directions to comply, infringement notices and remedial directions, and it also has the power to accept enforceable undertakings. Its civil mechanisms include injunctions and civil penalties. The criminal mechanism is the fine upon conviction. We have highlighted that the precise enforcement mechanisms available to the ACMA depend on the specific rule in question. The enforcement mechanisms for select service provider rules and select carrier licence conditions are identical. However, the tools available to enforce industry codes and industry standards differ from each other. They also differ from the tools available to enforce the select service provider rules and select carrier licence conditions. The tools available to enforce industry codes are the weakest.

We have summarised the ACMA's general approach to compliance and enforcement, the factors that influence its decisions to take enforcement action (including infringement notices and remedial directions), and its enforcement priorities. In addition, we have noted that there are some differences between the ACMA's understanding of responsiveness and the understanding of responsiveness advanced by Ayres and Braithwaite and other regulatory scholars.

The data we have been able to collect for this report — the names of service providers against whom the ACMA has taken enforcement action between 1 January 2010 and 30 June 2023, the provisions the ACMA found they had breached, when the ACMA took enforcement action, and the types of enforcement actions the ACMA took against service providers — do not enable us to engage in a comprehensive review of how the ACMA has exercised its enforcement discretion and whether it has acted consistently with the principles of responsive regulation and risk-based regulation. Comprehensive assessment of the ACMA's enforcement practices would require access to all investigation reports, a much richer understanding of context, and consideration of other data accessible via methods such as interviews with key stakeholders and surveys of regulators and the regulated companies.

Nevertheless, the data collected suggests that when the ACMA does take enforcement action, it acts in accordance with and subject to the limitations of the Tel Act. It also suggests that the ACMA broadly acts in a way that is consistent with its Compliance and Enforcement Policy, its Regulatory Guides, and the Telecommunications (Infringement Notices) Guidelines 2022 (Cth) outlined in Chapter 3.

However, the data provokes questions (outside the scope of this report) about the adequacy of the ACMA's Tel Act enforcement powers – in particular, whether the ACMA needs additional tools (used in isolation or combination) to secure or motivate industry compliance. These



questions would include the following, all of which are questions for government policy rather than the ACMA's implementation of current regulation.

- When a code of practice is breached, should the ACMA be limited to issuing a formal warning or direction to comply, or should it have access to other tools such as the issuing of infringement fines and accepting an enforceable undertaking, if one is offered? While the current approach is consistent with the 'voluntary' status of registered codes, this report mentions two important areas of consumer protection – complaint handling and hardship policies – where the rules have been given additional weight through the transfer from the code environment to the ACMA-formulated standards that are directly enforceable on a first breach.
- Should the value of an infringement fine be increased to cover situations where a relatively serious single breach attracts a heavier fine?
- Should the ACMA be able to seek – as canvassed in the regulatory literature (and noted in Chapter 1, section A), based on experience in other industries or jurisdictions – the imposition of criminal penalties on providers who seriously and repeatedly fail to comply with consumer protection rules and to exclude temporarily or permanently from the market service providers who serially breach their consumer protection obligations with the result of serious consumer harm?

The data also points to aspects of compliance and enforcement that deserve additional consideration in order to better understand how responsive and risk-based regulation can best be achieved. The ACMA has a long history of conducting compliance audits. From the data available to us, we can identify some correlation of the ACMA's self-initiated audits with enforcement outcomes, but we are unable at this stage to make any definitive findings. A study of the relationship, over time, of the ACMA's monitoring and compliance activities, its enforcement actions, and subsequent compliance levels and consumer outcomes may help to highlight the value of the various components of the ACMA's work.

In addition, further inquiry into the circumstances of the enforcement actions mentioned in this report – including, for example, consideration of how the degree of consumer harm might have affected the ACMA's decisions on enforcement actions – could help to provide industry, government and the community with the means of assessing the regulator's overall enforcement approach. This is not to suggest that the ACMA has not used its available powers in a way that promotes consumer protection outcomes. Indeed, over the period examined here, the ACMA, on two occasions (in 2011 and again in 2018), publicly declared that it was reassessing its approach to key consumer protection measures in light of evolving industry practice and consumer experience. Our point here is that an independent consideration of the ACMA's regulatory practice might reasonably take account of aspects such as the following:

- the extent to which the degree of consumer harm is an element in decisions on enforcement action;
- the relative merits of using available alternative enforcement mechanisms (eg, formal warnings or directions to comply for code breaches; remedial directions or infringement fines for breaches of standards, determinations and service provider rules), having regard to specific examples and case studies;
- the targeting of available enforcement resources to service providers with demonstrated compliance problems;

- the additional deterrence value of civil penalties (only three of which were obtained in the period reviewed in this report) as well as injunctions, taking account of the additional cost to the regulator of these forms of enforcement actions and industry's likely response to them.

Our case studies, presented in section C of Chapter 4, provide an illustration of how additional explanation of enforcement choices could help industry and the community assess the effectiveness of regulation.

Finally, the material considered in this report highlights the importance of publicly available data on enforcement of consumer protection rules. As we noted in the introduction to Chapter 4, subject to some exceptions under the Tel Act, the ACMA is not required to prepare and publish investigation reports. Nor is it required to maintain a register of all enforcement action it may have taken against carriers or carriage service providers to secure compliance with the select consumer-protection rules. It is also not required to include copies of these directions and instruments in its annual reports. The absence of such obligations means that, at the time we conducted this research, we did not have any and/or easy access to the following data for the period under review:

- numbers of investigations opened and closed (our dataset is based on published investigations where there was a breach finding);
- investigation reports with no breach findings (we found 26 published investigation reports with a finding of no breach);
- investigation reports with breach findings that the ACMA may not have published because of public interest concerns;
- records of the dates on which investigations were concluded and enforcement action taken (eg, a website listing of 2010 to 2016 investigations refers to 60 investigations without listing a month or year in which enforcement action was taken);
- explanations for why enforcement action was not taken in relation to some matters that were the subject of breach findings;
- copies of enforcement instruments (eg, copies of the instruments issued before 2017 are no longer provided on the online lists, and some instruments for later years are not available).

It may be reasonable to assume that it is not in the public interest for some of the information to be withheld from publication. Much of it, however, is unlikely to have this character, and some will have been public at some stage. For example, the ACMA regularly publishes information in its media releases that notes the importance of compliance and these statements sometimes explain its decision to pursue a certain enforcement action, but media releases are removed from the public record after three or four years. Similarly, reports on investigations prior to March 2017 are no longer available from the ACMA website, even though they were once published on the site.

While we are grateful to the ACMA staff for the assistance they provided in reviewing a draft of this report and helping to improve its accuracy, the report cannot be comprehensive because there is so much data that has never been made public or is no longer on the public record. Without resorting to formal methods such as freedom of information requests, only the ACMA can review the nature and extent of its enforcement action in relation to these telecommunications consumer protection rules.

The absence of any obligations to publish registers or other repositories of key data on telecommunications regulation shows a gap in the regulatory settings for which Parliament, not the ACMA, is responsible. To address this problem, amendments could be made to the Tel Act and the TCPSSA to require the establishment of a formal register of completed investigations and enforcement actions. Inclusion of information in the register could be made subject to the ACMA being satisfied that publication is in the public interest, drawing on the factors such as those set out in its existing policy.<sup>257</sup> In our view, the added level of transparency that would flow from the publication of this data on telecommunications compliance and enforcement would help the community to assess the adequacy of current consumer protection regulatory obligations and to provide confidence in the effectiveness of their enforcement.

---

<sup>257</sup> See the ACMA, *Regulatory Guide No. 6: Publication of Investigations and Enforcement Actions* (Updated February 2023) <<https://www.acma.gov.au/publications/2019-12/guide/regulatory-guide-no-6-publication-investigations-and-enforcement-actions>>. See also <<https://www.acma.gov.au/investigations-telco-providers>>. For example, entries of prior approval of temporary beaches of the statutory media control rules in the *Broadcasting Services Act 1992* (Cth) must be entered into the register that the ACMA is required to maintain under s 75 of that Act, but in order to protect commercially sensitive information, under s 75(2) the ACMA is instructed not to enter an approval give under s 67 until the transaction or agreement has taken place or been entered into.

# ANNEX A

## Industry Codes Registered by the ACMA under Part 6

- Cabling Requirements for Business
- C617:2017 Connect Outstanding Incorporating Variation No 1/2023
- C513:2015 Customer and Network Fault Management
- C536:2020 Emergency Call Services Requirements
- C519:2004 End-to-end Network Performance
- C525:2023 Handling of Life Threatening and Unwelcome Communications
- C657:2015 Inbound Number Portability
- C555:2020 Integrated Public Number Database
- C625:2020 Information on Accessibility Features for Telephone Equipment
- C540:2023 Local Number Portability
- C570:2009 Mobile Number Portability
- C564:2020 Mobile Phone Base Station Deployment
- C637:2019 Mobile Premium Services (MPS) Code- Incorporating Variation No 1/2021
- C647:2023 NBN Access Transfer
- C658:2019 Next-Generation Broadband Systems Deployment in Customer Cabling
- C515:2015 Pre-selection
- C609:2007 Priority Assistance for Life Threatening Medical Conditions
- C661:2022 Reducing Scam Calls and Scam SMS
- C566:2023 Number Management: Use of Numbers by Customers
- C628:2019 Telecommunications Consumer Protections Code Incorporating Variation No 1/2022
- C559:2012 ULLS Network Deployment

This list is current as at the time of writing.

# ANNEX B

## Data Collection Methodology

The starting point for the data that informs this report was a table prepared by the ACMA and provided by ACCAN to UTS ('the ACMA table'). In February 2023, ACCAN had requested a list of the ACMA's enforcement actions over the last five years. The ACMA gave ACCAN a spreadsheet comprising the data published on the 'Investigations into Telco Providers' page of its website over the period March 2017 to December 2022.<sup>258</sup> The data in the ACMA table included: the names of the service providers concerned; the outcome of the investigation; the date the investigation report was published; the type of enforcement action taken (eg, formal warning, enforceable undertaking, direction to comply, remedial action, infringement notice, civil penalties); the total number of enforcement actions taken against the service provider; and the amount specified in an infringement notice (if any).

We then modified the ACMA table to exclude breaches that were not relevant to the study (mainly concerning breaches of the *Spam Act 2003* (Cth) and the Do Not Call Register). We also expanded the time period of the enforcement actions, adding consumer-related enforcement information for the period of 1 January 2010 to 31 December 2016 and any consumer-related enforcement actions taken between the last enforcement action in the ACMA table and June 30, 2023. We sourced the more recent entries from the ACMA website 'Investigations into Telco Providers', noted above. We chose 2010 as the starting point because the ACMA publishes on its website a list of telecommunications investigations from that year on.<sup>259</sup> The website only includes information on the name of the service provider, the provisions breached, and (in all but 60 matters) the month and year that the investigation report was published. As the page for the older matters does not link to a copy of the investigation report or the enforcement outcome, we then searched the ACMA's Annual Reports (2009-10 to 2016-17 inclusive). Information from the Annual Reports was cross-checked with the information published on the ACMA website. In some instances, the Annual Reports and the ACMA web page omitted information such as the provision breached. Often this missing information related to breaches of the TCP Code. In these instances, the breached provision was deduced from the date of the breach and the description of the breach. For instance, where the breach was listed as a 'failure to submit compliance statements to code compliance' in 2016, clause 9.4 was identified as the relevant clause based on an examination of the TCP Code that was registered at the time. We also drew on our own research data concerning the enforcement of the TCP Code to provide a more detailed summary of the provisions breached. Finally, we added information on the amount of civil penalties and a 'deed of agreement' which had been used on one occasion.

We also identified a few discrepancies between the ACMA's Annual Reports and breaches for those periods on the ACMA's website. These mostly related to statements in Annual Reports indicating breaches occurred, but the names of relevant service providers were not identified, or the type of enforcement action taken was not specified. When gaps in the Annual Reports arose, we first cross-referenced the breaches for those periods on the ACMA's website. If no matches could be identified or no enforcement action could be discerned, other materials, such

---

<sup>258</sup> See 'Investigations Into Telco Providers' <<https://www.acma.gov.au/investigations-telco-providers>>. Note that this page now contains additional information published in 2023 and 2024.

<sup>259</sup> 'Investigations Into Telco Providers 2010-2016' <<https://www.acma.gov.au/investigations-telco-providers-2010-2016>>.

as other the ACMA publications (eg, its Communications Report series, bulletins and media releases) as well as news reports and academic journal articles, were searched for any references. As the ACMA no longer publishes its investigations reports and related enforcement actions prior to 2017, we relied in part on copies of the ACMA website that have been archived by the National Library of Australia on Trove and/or by the WayBack Machine. In the one instance where further investigation was unable to clarify the service provider, the entry was included in the data with the service provider as 'Unknown'. This entry is included in enforcement action tallies but has been excluded in our count of total service providers investigated as it was impossible to determine if this unknown service provider overlapped with known service providers. Where the nature of the enforcement action (if any) could not be ascertained, this data was included as 'no enforcement action taken'.

# ANNEX C

## Examples of the ACMA Compliance Audits

The following outline of some the ACMA Compliance Audits is taken from the ACMA Annual Reports.

Year	Audits conducted
2009-2010	<p><b>Mobile Premium Services Code:</b> Throughout the reporting period, and following the registration of the Mobile Premium Services Code, the ACMA has undertaken an extensive and rigorous program of monitoring compliance by mobile premium services with the code. Using compliance audits, the ACMA has identified potential contraventions of the code and brought the problem to the attention of the supplier of the mobile premium service. In the majority of cases, changes to services to achieve future compliance have been readily volunteered. The ACMA noted that due to the compliance monitoring, the number of complaints about mobile premium services recorded by the TIO fell.<sup>260</sup></p> <p><b>Telecommunications Code Compliance:</b> In 2009-10, the ACMA revised its approach to code compliance, undertaking a smaller number of audits but focusing these more closely on providers with increasing complaint numbers, rather than making broad industry assessments. The assessments undertaken were more deeply analytical than those of past years and made more frequent use of the ACMA's formal powers.<sup>261</sup></p> <p><b>Integrated Public Number Database:</b> The ACMA conducted its fourth audit of IPND address data during the reporting period. The snapshot of the IPND for the audit was taken in November 2009, with the ACMA releasing the aggregate industry-wide results in April 2010. The quality of address data in the IPND has improved significantly since the first audit was conducted in 2004. The ACMA will continue to work with data providers in 2010 to make further corrections and/or implement system improvements where necessary. The ACMA will consider at a later time whether to conduct a fifth audit.<sup>262</sup></p> <p><b>Mobile Premium Services:</b> The ACMA's primary monitoring activity for mobile premium services has been to undertake audits of the compliance of services with the obligations in the code. Services have been identified for auditing through the print media and television. Audit activity has included the inspection of advertisements, shadow shopping for services and examination of records of complaints received by the Telecommunications Industry Ombudsman. Where audit activity has identified potential contraventions of the code, the ACMA has generally brought the problem to the attention of the supplier of the mobile premium service. In the majority of cases, changes to services to achieve future compliance have been readily volunteered.<sup>263</sup></p>
2010-2011	<p>the ACMA noted that it was "changing its approach to addressing consumer issues and complaints" asserting that "this is evident from our quarterly consumer bulletin, which reports on a range of proactive initiatives, including audits and compliance education."<sup>264</sup></p> <p><b>Mobile Premium Services:</b> Throughout the reporting period, the ACMA continued its extensive and rigorous program of monitoring compliance by mobile premium services with the Mobile Premium Services Code. Using compliance audits, the ACMA has identified potential contraventions of the code and brought the problem to the attention</p>

<sup>260</sup> Australian Communications and Media Authority, *Annual Report 2009-10* (Report, 30 September 2010) 19.

<sup>261</sup> Ibid 86.

<sup>262</sup> Ibid 112.

<sup>263</sup> Ibid 125.

<sup>264</sup> Australian Communications and Media Authority, *Annual Report 2010-11* (Report, 30 September 2011) 12.

---

of the mobile premium service suppliers. In the majority of cases, changes to services to achieve future compliance have been readily volunteered.<sup>265</sup>

**Telecommunications Code Compliance:** The ACMA continued a range of activities to promote compliance with the Telecommunications Consumer Protections Code (the TCP Code) and achieve better outcomes for consumers. This included regular audits of the compliance of providers with particular TCP Code obligations to identify non-compliance and working with providers to address issues.<sup>266</sup>

- Elaborates on Page 91: The ACMA undertakes a range of activities to promote compliance with the Telecommunications Consumer Protections Code (the TCP Code) and achieve better outcomes for consumers. Many of these activities are educational. For example, the ACMA regularly audits the compliance of providers with particular TCP Code obligations to identify non-compliance and then works with them to address issues.

**Auditing of Information Available on providers' websites:** During the reporting period, the ACMA undertook four audits of providers' websites, reviewing the information provided to consumers on landline, broadband, post-paid mobile and prepaid mobile products. The audits followed continuing high levels of complaints from customers that their bills were different from what they had expected and about point-of-sale information. The audits found a high level of compliance with clause 3.3.3 of the TCP Code.<sup>11</sup> Providers promptly remedied non-compliance when it was identified. Despite this high level of compliance with clause 3.3.3, consumers complain that the available information does not prepare them for the bills they receive. This suggests that website information alone is not enough to educate consumers about the practical workings of their contracts and billing arrangements. The outcome of the audits (discussed below) has informed the ACMA's input into the current review of the TCP Code and the recommendations of its Reconnecting the Customer public inquiry.<sup>267</sup>

- Website information on landline products: Clause 4.2.4 of the TCP Code requires that suppliers provide information to customers before a customer signs a contract. This includes information about contract terms, product descriptions and minimum total charges. Thirty providers were audited across the industry, including all the major providers. Information about how call charges are calculated was found on all provider websites. However, details about service connection fees, early termination fees and minimum contract terms were sometimes unclear or difficult to locate. This confirmed the ACMA's opinion—expressed to CA in advance of the TCP Code review—that providers need to improve their methods of providing important information to consumers. The ACMA contacted four of the audited providers about the availability of landline website information. Two have made improvements to their websites, one supplied further information to demonstrate compliance and the other is no longer offering a landline product.<sup>268</sup>
- Website information on broadband products: Twenty-five providers, including all the major providers, were audited across the industry for website information on broadband products. In most cases, key information about broadband products was found within one click of the main product page. Peak and off-peak time limits typically apply to all internet plans except mobile broadband products. The majority of providers gave clear information on time limits, information on the product page about what happens if a data limit is exceeded, and information on service connection fees and termination fees on the main product page. While most information could be found within one click of the main product page, the ACMA was concerned that, in a number of instances, important information was only available in the standard form of agreement (SFOA) or three clicks from the main product page.<sup>269</sup>

---

<sup>265</sup> Ibid 20.

<sup>266</sup> Ibid 21.

<sup>267</sup> Ibid 93.

<sup>268</sup> Ibid 93.

<sup>269</sup> Ibid 93.



- **Website information on post-paid mobile products:** Twenty providers of post-paid mobile products, including all the major providers, were audited across the industry. Generally, it was found that key information about post-paid products was found within one click of the product page. While information about roaming charges was also readily found for the majority of providers, the level of information provided about credit control and usage-monitoring tools offered by providers was inconsistent. The ACMA contacted some of the audited providers about the availability of website information or their unclear disclaimers. These providers either made prompt improvements to their website or supplied further information to demonstrate compliance.<sup>270</sup>
- **Website information on prepaid mobile products:** Twenty providers of prepaid mobile products, including all the major providers, were audited across the industry. A satisfactory level of compliance with the requirement to provide information on charges and credit expiry for prepaid mobile services was found, with this information obtainable within one to three clicks from the product information web page. The ACMA found that some suppliers provide information on mobile network coverage on request but do not state the same information on the product web pages. Most of the smaller providers who onsell the services of the major mobile networks do not have an online coverage map. However, most providers refer to the network provider's coverage map through a hyperlink. The main areas for improvement for prepaid mobile services are the provision of consistent and clear information about international roaming charges and comprehensive information about available usage monitoring tools.<sup>271</sup>

**Auditing the Privacy of Billing Information:** The TCP Code and Telecommunications Act impose obligations on providers about the disclosure and use of information gathered in the course of conducting their businesses.<sup>12</sup> In October 2010, Telstra announced that certain customer details had inadvertently been disclosed to other customers following a mail-merge error. In early 2011, media reports suggested that Vodafone had mistakenly disclosed the personal information of its customers. The Office of the Information Commissioner (Oaic) took the lead in investigating this alleged disclosure. His published report into Vodafone is available on the Oaic website. The ACMA was concerned that these incidents may have been symptomatic of a broader problem within the industry. The ACMA requested information from the top 10 providers (based on TIO complaints) on the measures that each has in place to safeguard the personal information of customers and the adequacy of these measures. All providers have been given the information that is currently being assessed to determine areas of best practice and those that require clarification or rectification. The ACMA will liaise with the Oaic on its findings.<sup>272</sup>

**Mobile Premium Services:** During the reporting period the ACMA continued its extensive and rigorous program of monitoring and enforcing industry compliance with the MPS Code. The program identified potential breaches of the code and recurring and systemic problems with services. The ACMA audited services identified through print, online and television advertisements. Audit activity included inspecting advertisements, 'shadow shopping' for services and examining information about the nature of complaints received by the TIO. Where audits identified potential contraventions of the code, the ACMA has brought the problems to the attention of the suppliers of the mobile premium services concerned. In the majority of cases, changes to services to achieve future compliance have been readily volunteered. The ACMA Annual report 2010–11 | 97 In cases where compliance with the code was not otherwise able to be procured, the ACMA has initiated investigations under paragraph 510(1)(c) of the Telecommunications Act. During the reporting period, 11 such investigations were initiated.<sup>273</sup>

**Integrated Public Number Database:** As part of its IPND compliance program, in February 2011 the ACMA commenced an investigation into whether CSPs are complying

<sup>270</sup> Ibid.

<sup>271</sup> Ibid.

<sup>272</sup> Ibid 94.

<sup>273</sup> Ibid 96.

	<p>with their obligations to provide accurate customer data to the IPND. The ACMA requested 600 records from the IPND Manager for 30 CSPs to ascertain whether the records contained in the IPND matched the customer records held by the providers. The CSPs selected include both the large and small end of the market and take into account the results of the ACMA's 2009–10 IPND audit. The ACMA's investigation is continuing.<sup>274</sup></p>
2011-12	<p><b>the ACMA's approach to telecommunications code compliance:</b> Notes that the ACMA's main areas of focus during the reporting period have included undertaking code 'audit' programs of provider compliance with financial hardship and privacy of billing information.<sup>275</sup></p> <p><b>Auditing the privacy of billing information:</b> The TCP Code and Telecommunications Act impose obligations on providers about the disclosure and use of information gathered in the course of conducting their businesses.<sup>9</sup> The ACMA continued its audit of the 10 large providers to determine the measures that each has in place to safeguard the personal information of customers and the adequacy of these measures. The ACMA's analysis of initial responses indicated that for eight providers, there were areas that required more detailed investigation. These investigations commenced in September 2011. The ACMA was satisfied that all providers investigated had appropriate measures in place to meet their requirements under the Act and the TCP Code. However, recommendations were made to two of these providers on areas for improvement.<sup>276</sup></p> <p><b>Mobile Premium Services Code:</b> Using advertising, market intelligence, referrals from other agencies and information provided by industry, the ACMA identified services and providers to audit for compliance with the Mobile Premium Services Code (MPS Code). Using compliance audits, the ACMA identified potential contraventions of the MPS Code and brought the problem to the attention of the premium service providers. In most cases, informal action has resulted in changes to services to achieve future compliance<sup>277</sup> .... The ACMA also audited industry compliance with the two service provider determinations that apply to mobile premium services. It found that all mobile CSPs complied with the Telecommunications Service Provider (Mobile Premium Services) Determination 2010 (No. 1) by offering barring of mobile premium services and providing information about barring to their customers at the required intervals. It also found that all mobile content aggregators complied with Telecommunications Service Provider (Mobile Premium Services) Determination 2010 (No. 2) by having contracts only with content providers that were listed on the CA register.<sup>278</sup></p>
2013-14	<p><b>Enquiries and Investigations about compliance with the TCP Code:</b> Following its March 2013 audit of critical information summaries, the ACMA conducted a follow-up audit of 46 providers in March 2014 to check that they have critical information summaries and these are in the prescribed format. Of the 46 providers assessed, only two per cent failed to have a critical information summary; 90 per cent were immediately compliant<sup>279</sup> ..... In December 2013, the ACMA commenced an audit of seven large and medium-sized providers of included value plans to assess their compliance with the usage alert requirements. The ACMA found that most providers had a small incidence of failure to send notifications or the correct information at the 100 per cent notification level. However, all providers aside from one (discussed below) addressed systemic issues and were deemed compliant. The audit found that Dodo Services Pty Ltd (Dodo) did not comply with the required usage notification requirements, as it failed to send alerts to customers about their data use. The failure affected certain Dodo customers with a fixed broadband service during October and November 2013. In May 2014, the ACMA issued Dodo with a formal warning for failing to comply with the usage alert requirements of the TCP Code.<sup>280</sup></p>

<sup>274</sup> Ibid 119.

<sup>275</sup> Australian Communications and Media Authority, *Annual Report 2011-12* (Report, 27 September 2012) 88

<sup>276</sup> Ibid 90.

<sup>277</sup> Ibid.

<sup>278</sup> Ibid 91.

<sup>279</sup> Australian Communications and Media Authority, *Annual Report 2013-14* (Report, 30 September 2013) 80.

<sup>280</sup> Ibid 80–1.

2015-16	<b>Financial Hardship Review:</b> In 2015–16, the ACMA conducted an audit of providers’ compliance with financial hardship provisions in the TCP Code. No investigations or enforcement action were considered necessary as a result of the audit. <sup>281</sup>
2017-18	<b>Financial Hardship Review:</b> In 2017–18, we audited providers’ compliance with the requirement to publish a financial hardship policy on their website. The audit found a high level of compliance, with no enforcement action taken. <sup>282</sup>
2018-19	<b>NBN Consumer Experience Safeguards:</b> <ul style="list-style-type: none"> <li>• <u>Consumer Information Standard</u>—we concluded an audit of 25 CSPs, relating to advertising and information provided to consumers about NBN plans, resulting in eight investigations being undertaken.<sup>283</sup></li> <li>• <u>Service Continuity Standard and Service Migration Determination</u>: the first in a series of audits was undertaken to assess compliance.</li> </ul>
2019-20	<p><b>NBN Consumer Experience Rules:</b> Monitoring compliance with the rules designed to help consumers move to the NBN was a 2019–20 telco consumer safeguards compliance priority. We utilised complaints data received under our Telecommunications (Consumer Complaints) Record-Keeping Rules 2018 (record-keeping rules) and data from other sources such as the Telecommunications Industry Ombudsman (TIO) to focus our compliance activities. These activities included compliance audits, investigations of potential non-compliance and enforcement action (where necessary). We also published the outcomes of our compliance activities concerning the NBN migration rules.<sup>284</sup></p> <ul style="list-style-type: none"> <li>• we completed investigations into the compliance by four providers with requirements in the Service Continuity Standard and Service Migration Determination following audits conducted early in the reporting period. The COVID-19 pandemic caused delays in finalising enforcement actions for these investigations. These will now be finalised in the next reporting period.<sup>285</sup></li> <li>• we commenced an audit of the compliance of six providers with requirements under the Service Continuity Standard and Service Migration Determination for parallel migrations (where the legacy service can remain operational while the NBN is connected), including whether postmigration testing is being completed and numbers are ported appropriately. The COVID-19 pandemic impeded our finalisation of this audit in the reporting period.<sup>286</sup></li> </ul> <p><b>Mobile network operators’ notification and consultation requirements:</b> We audited mobile network operators’ consultation and notification requirements set out under the Deployment Code. This compliance activity aimed to determine whether the carriers are complying with their obligations under the Deployment Code, which are intended to: &gt; allow the community and local councils to have greater participation in decisions made by carriers when deploying a mobile phone base station &gt; provide greater transparency to the public when a carrier is planning, selecting sites for, installing and operating mobile phone base station infrastructure. The audit assessed: &gt; 28 Telstra small cell sites &gt; 17 Optus small cell sites &gt; one Vodafone small cell site. The results of the audit indicated that the carriers have established processes and information materials to ensure compliance with the notification and consultation requirements in the Deployment Code. The local community, including councils, property owners and occupiers and those community members in sensitive locations are customarily being notified and consulted prior to the commencement of construction.<sup>287</sup></p>

<sup>281</sup> Australian Communications and Media Authority and Office of the Children’s eSafety Commissioner, *Annual Reports 2019-2020* (Report, 19 September 2020) 74.

<sup>282</sup> Australian Communications and Media Authority and Office of the eSafety Commissioner, *Annual Reports 2017-18* (Report, 18 September 2018) 75.

<sup>283</sup> Australian Communications and Media Authority and Office of the eSafety Commissioner, *Annual Reports 2018-19* (Report, 4 September 2019) 34.

<sup>284</sup> ACMA Annual Report 2019-20 (n 281) 38.

<sup>285</sup> Ibid.

<sup>286</sup> Ibid 39.

<sup>287</sup> Ibid 68.

2020-21	<p><b>Strategic Priority 2: Public confidence in communications and media services through the provision of regulatory safeguards, information and advice.</b></p> <ul style="list-style-type: none"> <li>• We continued monitoring and conducted audits of: online rules to protect children from exposure to gambling advertising during live sports events broadcast on television and radio, and streamed online</li> <li>• rules about responsible approaches to selling, credit assessment and financial hardship in the Telecommunications Consumer Protections (TCP) Code.<sup>288</sup></li> </ul> <p><b>Monitoring compliance with the NBN consumer experience rules: a better move to the NBN:</b></p> <ul style="list-style-type: none"> <li>• commenced investigations into 3 CSPs for potential non-compliance with the NBN Service Continuity Rules following the receipt of negative audit findings, with Optus Internet Pty Ltd found to have breached the service continuity rules.<sup>289</sup></li> <li>• completing an audit to assess the compliance of 31 CSPs with requirements for key facts sheets in the NBN Consumer Information Standard. The audit found that the majority of the CSPs were complying with these requirements. Clear Networks Pty Ltd was found to have breached the requirements and has subsequently addressed this non-compliance.<sup>290</sup></li> </ul> <p><b>Protecting Telco Consumers:</b> In April 2021, we completed an audit into CSPs' compliance with the TCP Code rules. These rules require CSPs to tailor their dealings with vulnerable consumers, including by ensuring that their sales representatives sell their products in a responsible manner and interact appropriately with disadvantaged and vulnerable consumers. The audit involved reviewing information collected from 9 CSPs about: how they identify vulnerable consumers the actions they take to appropriately train and monitor their sales representatives in responsibly selling to vulnerable consumers whether they have identified any emerging or systemic deficiencies in the conduct of their sales representatives and, if so, what steps (if any) have been taken to address these issues the oversight arrangements and level of senior management engagement in ensuring sales representatives are interacting appropriately with vulnerable consumers.<sup>291</sup></p> <p><b>Other telecommunications matters:</b> In 2020–21, we monitored telecommunications' industry compliance through TIO referrals, self-reported breaches by telcos, and audits on telco consumer protection obligations. We completed 19 telecommunications investigations.<sup>292</sup></p>
2021-22	<p><b>Decisions to open investigations are informed by risk assessments and consideration of potential harm to consumers:</b> Other compliance activities included conducting 2 audits: &gt; one that assessed whether 8 telcos were complying with the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 (the Complaints Handling Standard) in relation to small business customers &gt; the second reviewed data from 11 telcos over a 6-month period in relation to customer contact and compliance with the Telecommunications Consumer Protections Code (C628: 2019) (TCP Code) and Complaints Handling Standard. Overall, the results of both audits were positive, with the ACMA finding telcos were largely compliant with relevant rules under the TCP Code and the Complaints Handling Standard.<sup>293</sup> Overall, the results of both</p>

<sup>288</sup> Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2020-21* (Report, 17 September 2021) 26.

<sup>289</sup> *Ibid* 49.

<sup>290</sup> *Ibid*.

<sup>291</sup> *Ibid* 56.

<sup>292</sup> *Ibid* 64.

<sup>293</sup> Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2021-22* (Report, 19 September 2022) 38.

	audits were positive, with the ACMA finding telcos were largely compliant with relevant rules under the TCP Code and the Complaints Handling Standard.
<b>2022-23</b>	<p><b>Financial Hardship</b></p> <p>Over the last 4 years, the ACMA has had a strong focus on consumers that may be facing financial pressures in paying their telco bills. This culminated in our major report – Financial hardship in the telco sector – being published in the reporting period. This report found that in the previous 12 months, a significant number of Australians had experienced difficulty paying for, or had concerns with, their telco bills.<sup>294</sup></p> <p>[The report included the following explanation: In December 2022, we completed an audit of 15 telcos’ compliance with financial hardship and disconnection notification requirements in the TCP Code. As a result of the audit findings, we are undertaking some investigations. The investigation reports, including any breach findings, will be published on our website.<sup>295</sup>]</p> <p><b>Combatting SMS Scams</b></p> <ul style="list-style-type: none"> <li>• As of 30 June 2023, the ACMA had audited, or were in the process of auditing, the compliance of 42 SMS aggregators (telecommunications providers that send bulk text messages with the Reducing Scam Call and Scam SMS Code.</li> <li>• It completed audits of 54 telco providers into their compliance processes with the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 and Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Standard 2020.</li> </ul>

<sup>294</sup> Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2022-23* (Report, 27 September 2023) 8. Information, research and other reports on this topic over the period 2018-2023, including three annual ‘state of play reports’, is available at <https://www.acma.gov.au/financial-hardship-telco-sector-keeping-customer-connected>.

<sup>295</sup> Australian Communications and Media Authority, *Financial Hardship in the Telco Sector Keeping the Customer Connected* (Report, May 2023) 16.