



Australian Government

ASIC Enforcement Review Taskforce Report

December 2017





18 December 2017

The Hon Kelly O'Dwyer MP
Minister for Revenue and Financial Services
Parliament House
CANBERRA ACT 2600

Dear Minister

ASIC ENFORCEMENT REVIEW TASKFORCE REPORT

In accordance with the Terms of Reference and on behalf of the other members, I am pleased to present the Report of the ASIC Enforcement Review Taskforce.

Among other things, the Report makes recommendations to improve ASIC's ability to gather information, strengthen ASIC's licensing and banning powers, increase penalties for corporate misconduct generally and encourage greater use of industry codes of conduct. The recommendations enhance ASIC's regulatory regime while also seeking to maintain necessary checks and balances to ensure fair treatment of the regulated population.

The Report has been informed by extensive industry and community consultation. In arriving at its final recommendations, the Taskforce considered 149 submissions received in response to 8 published position papers and met with many stakeholders individually.

I wish to thank the members of the Panel and the Expert Group and to acknowledge their expertise in corporate, financial, and consumer law, their insights, engagement with the issues, and the substantial contribution each made of their personal time and resources to the Taskforce over the past 14 months, and in finalising this report and position papers.

The Panel comprised Messrs Shane Kirne (CDPP), Tim Mullaly (ASIC) and representatives from the Attorney-General's Department (Ms Brooke Hartigan, Messrs Owen Lodge, Graeme Gunn and Tom Sharp). The Expert Group comprised Messrs Gerard Brody (Consumer Action Law Centre), Stuart Clark (Law Council of Australia; Clayton Utz), Ross Freeman (Minter Ellison), Professor Pamela Hanrahan (UNSW), Professor Ian Ramsay (University of Melbourne), and Professor Dimity Kingsford Smith (UNSW).

Finally, I wish to acknowledge the outstanding support provided by the Secretariat within Treasury (in particular, Jerome Davidson, Melanie Preziuso, Wendy Hau, Kevin Zhang and Hannah Denson) and ASIC officers (especially Chris Rowe, Rowena Park, Breshna Ebrahimi, and Anthony Vardy) who assisted with the development of position papers, and preparation of the final report.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Kate Mills'.

Kate Mills
Chairman
ASIC Enforcement Review Taskforce

© Commonwealth of Australia 2017

This publication is available for your use under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.



Use of Treasury material under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used 'as supplied'.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics — then Treasury prefers the following attribution:

Source: The Australian Government the Treasury.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on The Australian Government the Treasury data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the It's an Honour website (see www.itsanhonour.gov.au).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Editorial, Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: medialiaison@treasury.gov.au

Contents

- Contentsiv**
- Foreword viii
- Executive summaryx
- Summary of recommendations by chapterxiv**
- Principles guiding the ASIC Enforcement Review xix
- Summary of recommendations2**
- 1. Self-reporting of contraventions by financial services and credit licensees3**
- Overview3
 - Current obligation to self-report.....3
- Nature of the significance test4
 - Recommendation 16**
- Scope of application6
 - Recommendation 27**
 - Recommendation 37**
- Timing and process.....8
 - Recommendation 49**
 - Recommendation 510**
- Encouraging compliance10
 - Recommendation 611**
 - Recommendation 711**
 - Recommendation 812**
- Related matters.....13
 - Recommendation 913**
 - Recommendation 1013**
- Summary of recommendations16**
- 2. Harmonisation and enhancement of search warrant powers17**
- Overview17
 - Current search warrant powers17
- Nature of search warrants18
 - Recommendation 1119**
 - Recommendation 1220**
 - Recommendation 1320**
- Issuing warrants21
 - Recommendation 1421**
- Use of seized material21
 - Recommendation 1522**
 - Recommendation 1623**

Summary of recommendations	25
3. ASIC’s access to telecommunications intercept material	26
Overview	26
Current status of ASIC’s access to telecommunications intercept material	27
Receiving telecommunications intercept material	27
Recommendation 17	27
Summary of recommendations	30
4. Industry codes in the financial sector	31
Overview	31
Current status of industry codes	31
Approval of codes	32
Recommendation 18	33
Subscribing to codes	34
Recommendation 19	34
Recommendation 20	35
Code compliance	35
Recommendation 21	35
Recommendation 22	35
Summary of recommendations	38
5. Strengthening ASIC’s licencing powers	39
Overview	39
Current licencing powers	40
Granting licences	40
Recommendation 23	41
Recommendation 24	42
Recommendation 25	42
Recommendation 26	43
Recommendation 27	43
Control obligations	44
Recommendation 28	45
Recommendation 29	46
Relevant matters	46
Summary of recommendations	48
6. ASIC’s power to ban individuals in the financial sector	49
Overview	49
Current status of ASIC’s banning powers	50
Expanding the scope of banning powers	51
Recommendation 30	51
Revising the banning threshold	52
Recommendation 31	52

Summary of recommendations	56
7. Strengthening penalties for corporate and financial sector misconduct	58
Overview	58
Quantum of penalties: Criminal	59
Recommendation 32	60
Defective disclosure and false or misleading statements to consumers	60
Failure to comply with corporate obligation	62
Unlicensed conduct.....	63
Failure to comply with financial services licensee obligations	64
Defective disclosure to ASIC.....	65
Increases to maximum criminal pecuniary penalties.....	66
Recommendation 33	66
Corporate fraud offences	67
Recommendation 34	68
Dishonesty test.....	68
Recommendation 35	69
Strict and absolute liability offences	69
Recommendation 36	70
Recommendation 37	70
Recommendation 38	71
Recommendation 39	72
Quantum: Civil penalties	72
Recommendation 40	73
Disgorgement in civil penalty proceedings	75
Recommendation 41	76
Priority for compensation	77
Recommendation 42	77
Pathways: Civil penalties.....	77
Recommendation 43	79
Pathways: Infringement Notices	80
Recommendation 44	81
Recommendation 45	83
Peer Disciplinary Review Panels.....	84
Table A: list of recommended increases to imprisonment penalties	85
Table B: Complete list of new ordinary offences	89
Table C: Complete list of new civil penalty provisions	90
Table D: Complete list of new infringement notice provisions.....	92
Appendix A: Principles for the review of penalties	94
Summary of recommendations	99
8. ASIC’s directions power	100
Overview	100
Current status of ASIC’s directions powers.....	100
Triggering the directions power	101
Recommendation 46	103
Recommendation 47	104

Interim directions105
 Recommendation 48105
Licensee compliance with directions106
 Recommendation 49106
 Recommendation 50106

Foreword

On 19 October 2016, the Minister for Revenue and Financial Services, the Hon Kelly O’Dwyer MP, announced a taskforce to review the enforcement regime of the Australian Securities and Investments Commission (ASIC). The Minister provided the Taskforce with the Terms of Reference outlined on the next page.

The Taskforce was led by a Panel chaired by Treasury, and included senior representatives from ASIC, the Attorney-General’s Department, and the office of the Commonwealth Director of Public Prosecutions. The Panel was supported by an Expert Group drawn from academia and legal experts recognised for their expertise in corporations, consumer, financial and credit law. The Expert Group provided ongoing advice and feedback to the Panel in preparing its report and recommendations. Conclusions and recommendations in this report do not necessarily reflect the views of all of the members of the Taskforce. The Taskforce was assisted by a secretariat provided by the Treasury, and received additional support and assistance from staff of ASIC.

Panel: Kate Mills (Treasury), Shane Kirne (CDPP), Tim Mullaly (ASIC) and representatives from the Attorney-General’s Department (Brooke Hartigan, Owen Lodge, Graeme Gunn and Tom Sharp).

Expert Group: Gerard Brody (Consumer Action Law Centre), Stuart Clark (Law Council of Australia; Clayton Utz), and Ross Freeman (Minter Ellison), Professor Pamela Hanrahan (UNSW), Professor Ian Ramsay (University of Melbourne), and Professor Dimity Kingsford Smith (UNSW).

Finally, the Taskforce wishes to acknowledge the support provided by all members of the Secretariat, staff at ASIC and external support from Oliver Wyman.

Secretariat: Jerome Davidson, Melanie Preziuso, Wendy Hau, Kevin Zhang, Hannah Denson, Harvey Singh, Jenny Leo, and Daniel McAuliffe.

ASIC: Chris Rowe, Rowena Park, Breshna Ebrahimi, and Anthony Vardy.

Oliver Wyman: Jacob Hook, David Howard-Jones, and Alexandra Biggs.

ASIC Enforcement Review Taskforce Terms of Reference

The Taskforce will review the enforcement regime of the Australian Securities and Investments Commission (ASIC), to assess the suitability of the existing regulatory tools available to it to perform its functions adequately.

The review will include an examination of legislation dealing with corporations, financial services, credit and insurance as to:

- The adequacy of civil and criminal penalties for serious contraventions relating to the financial system (including corporate fraud);
- The need for alternative enforcement mechanisms, including the use of infringement notices in relation to less serious contraventions, and the possibility of utilising peer disciplinary review panels (akin to the existing Markets Disciplinary Panel) in relation to financial services and credit businesses generally;
- The adequacy of existing penalties for serious contraventions, including disgorgement of profits;
- The adequacy of enforcement related financial services and credit licensing powers;
- The adequacy of ASIC's power to ban offenders from occupying company offices following the commission of, or involvement in, serious contraventions where appropriate;
- The adequacy of ASIC's information gathering powers and whether there is a need to amend legislation to enable ASIC to utilise the fruits of telephone interception warrants or to grant the equivalent of Federal *Crimes Act* search warrant powers under ASIC's enabling legislation for market misconduct or other serious offences;
- The adequacy of ASIC's powers in respect of licensing of financial services and credit providers, including the threshold for granting or refusing to grant a license, the circumstances in which ASIC may vary, suspend, or cancel licenses; and its coercive powers (including whether there is a need for ASIC to have a power to direct licensees to take, or refrain from taking, particular action);
- The adequacy of the frameworks for notifying ASIC of breaches of law, including the triggers for the obligation to notify; the time in which notification is required to be made; and whether the obligation to notify breaches should be expanded to a general obligation (currently confined under the Corporations Act to auditors, liquidators, and licensees, and noting that obligations to report offences exist under other Federal or State statutes); and
- Any other matters, which arise during the course of the Taskforce's review of the above, which appear necessary to address any deficiencies in ASIC's regulatory toolset.

Upon completion of the Review, the Taskforce will identify any gaps in ASIC's powers and make recommendations to the Government which it considers necessary to strengthen any of ASIC's regulatory tools and as to the policy options available that:

1. address gaps or deficiencies identified in a way that allows more effective enforcement of the regulatory regime;
2. foster consumer confidence in the financial system and enhance ASIC's ability to prevent harm effectively;
3. do not impose undue regulatory burden on business, and promote engagement and cooperation between ASIC and its regulated population;
4. promote a competitive and stable financial system that contributes to Australia's productivity growth; and
5. relate to other matters that fall within this Terms of Reference.

Executive summary

The ASIC Enforcement Review Taskforce was established in response to a recommendation of the Financial System Inquiry and in an environment of much public and political scrutiny of the financial sector. This scrutiny intensified during the period in which the review has been conducted, and culminated in the calling of the Royal Commission into the alleged misconduct of Australia's banks and other financial services entities. In working through the matters outlined in its terms of reference, the Taskforce has been mindful of the fact that community confidence in the sector has declined, and of its terms of reference which included developing policy options that:

- address gaps or deficiencies identified in a way that allows more effective enforcement of the regulatory regime;
- foster consumer confidence in the financial system and enhance ASIC's ability to prevent harm effectively;
- do not impose undue regulatory burden on business, and promote engagement and cooperation between ASIC and its regulated population;
- promote a competitive and stable financial system that contributes to Australia's productivity growth; and
- relate to other matters that fall within this Terms of Reference.

Using this as its point of departure, the Taskforce has formulated the more expansive principles set out below to guide its deliberations. Within this framework, the Taskforce has proceeded by analysing the findings of other reviews and inquiries, and worked intensively with ASIC, to identify any perceived gaps or deficiencies in the regulatory framework. Where these were identified, the Taskforce consulted broadly with stakeholders and the community, before finalising policy positions consistent with the principles set out below.

The Taskforce has grouped the matters raised in the terms of reference into 8 chapters and the recommendations in each of these are summarised below.

Self-reporting of contraventions by financial services and credit licensees

The self-reporting regime for Australian Financial Services (AFS) licensees has come under scrutiny over the last decade in the media and in a series of inquiries into banking or banking and financial services related misconduct. Concurrently, ASIC has publicly outlined concerns about the effectiveness of aspects of the existing regime.

The Taskforce considers that financial services and credit licensees should be required to report significant breaches to ASIC. The 'significance test' should be retained but clarified to ensure that the significance of breaches is determined objectively.

The time for reporting would be extended from 10 to 30 days, but licensees should be required to make a report if they are investigating a breach and have not determined, within 30 days, whether it meets the significance threshold.

This would strengthen the reporting regime by ensuring that failures to report, objectively determined as such, can be more effectively sanctioned and increasing the incidence of reports, by requiring a report to be made within 30 days, even if a breach investigation has not been finalised.

Harmonisation and Enhancement of Search Warrant Powers

A key aspect of an effective enforcement regime is the adequacy of the information gathering powers of the corporate regulator. The Terms of Reference specifically asked the Taskforce to examine the merit of granting ASIC the equivalent of Crimes Act search warrant powers.

After careful consideration and noting current deficiencies with ASIC search warrant powers, the Taskforce makes a number of recommendations designed to harmonise and strengthen ASIC's powers by aligning them with those available to other law enforcement agencies and regulators (such as the Australian Competition and Consumer Commission), and making other adjustments to ensure the scope of material that may be subject to search and seizure activity is not limited by narrow or outdated terms in legislation.

Specifically, *Australian Securities and Investments Commission Act 2001* (ASIC Act) search warrants in various Acts should be consolidated into the ASIC Act and ASIC's powers will be more consistent with those in the Crimes Act and the Competition and Consumer Act. Material seized under ASIC Act search warrants should also be available for use in criminal, civil and administrative proceedings (ensuring that ASIC is not unduly constrained from using material seized pursuant to its search warrant powers).

These proposed changes will ensure that the regulator has adequate access to effective investigative tools while balancing the risk to the rights of individuals.

ASIC's access to telecommunications intercept material

Commonwealth legislation prohibits access to material sourced from live stream communications over a telecommunications service and sets out a regime for specified agencies to apply for telephone intercept warrants and/or receive telephone intercept material for the purposes of investigating and prosecuting offences.

Currently, ASIC cannot seek a warrant to obtain or receive intercept material when investigating serious contraventions of the *Corporations Act 2001* (Corporations Act) unless another agency is authorised to share such material with ASIC for the purposes of its (the other agency's) investigation.

To enhance ASIC's access to telephone intercepts for the investigation and prosecution of serious corporate law offences, the Taskforce recommends that ASIC should be able to receive telephone intercept material to investigate and prosecute serious offences.

Industry codes in the financial sector

In her announcement of the Terms of Reference, the Minister for Revenue and Financial Services made clear that the Taskforce should include in its consideration, the adequacy of ASIC's enforcement in relation to industry Codes of Conduct.

The Taskforce has examined this and recommended that ASIC's ability to influence the effectiveness of codes could be enhanced by shifting to a co-regulatory model – at least for codes in relation to key services provided to retail and small business customers. Under a co-regulatory model, industry participants would be required to subscribe to an ASIC approved code, and in the event of non-compliance with the code an individual customer would be entitled to seek appropriate redress through the participant's internal and external dispute resolution arrangements. This model would operate only in sectors where ASIC considered its application appropriate having regard to all the circumstances.

Strengthening ASIC's licencing powers

The final report of the Financial System Inquiry flagged the need to toughen licensing powers to address poor behaviour and misconduct. The Taskforce has made recommendations to strengthen

ASIC's licensing powers by ensuring ASIC can refuse to grant a licence and, for existing licensees, can suspend or cancel a licence in appropriate circumstances.

The Taskforce's recommendations would establish a fit and proper test for new licensees, create a statutory obligation to notify ASIC about changes of control and align how applications for credit licences and financial service licences are assessed.

ASIC's power to ban individuals in the financial sector

ASIC must be adequately empowered to remove offending individuals from continued involvement in the financial sector, particularly those in senior positions of control and influence. The need for an enhanced banning power was highlighted in the final report of the Financial System Inquiry.

The Taskforce's recommendation would allow ASIC to ban individuals from managing financial services businesses in addition to their current power to ban individuals from providing financial services. The Taskforce has also recommended broadening the criteria for enlivening the banning power to include circumstances where an individual is unfit or improper for their role. This enhanced banning power seeks to increase manager accountability and to improve corporate culture in the financial services and credit sectors.

Strengthening penalties for corporate and financial sector misconduct

The effect of the Taskforce recommendations on penalties would be to expand the range of civil penalty provisions and to increase maximum civil penalty amounts in the Corporations Act and *National Consumer Credit Protection Act 2009* (Credit Act) to:

- for individuals, 2,500 penalty units (\$525,000); and
- for corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (\$210 million)).

This would increase fines from \$200,000 (individuals) and \$1 million (corporations) under the Corporations Act and 2,000 penalty units (\$420,000) for individuals and 10,000 penalty units (\$2.1 million) for corporations under the Credit Act.

In addition to increasing civil penalties ASIC would be able to seek disgorgement remedies (removal of benefits illegally obtained or losses avoided) in civil penalty proceedings brought under the Corporations, Credit and ASIC Acts.

Maximum terms of imprisonment would be increased for a range of offences. The most serious Corporations Act offences, given the nature and/or consequences of the offending conduct (many involving dishonesty) would become equivalent to the highest penalties currently available under the Act (10 years imprisonment, 4,500 penalty units (\$945,000) or 3 times benefits (individuals) and 45,000 penalty units (\$9.45 million) or 3 times benefits or 10% annual turnover (corporations)), which would also be increased slightly so that all serious offences attract the same penalties.

Maximum fine amounts for other criminal offences would also increase, and be standardised by reference to a formula based on length of available prison term: Maximum term of imprisonment in months multiplied by 10 = penalty units for individuals, multiplied by a further 10 for corporations.

For strict liability offences, the lowest level fines would increase and ASIC would be able to deal with these offences through the existing penalty notice regime as an alternative to prosecution.

ASIC would also be able to deal with a wider range of offences through infringement notice regimes.

ASIC's directions powers

ASIC's existing powers to modify an AFS or credit licensee's systems and conduct after the licence has been granted requires significant time, resources and costs in investigating and preparing a case to the required standard to commence court proceedings or licensing action. A directions power could aid ASIC in graduated engagement, as the directions power can be triggered by a lower threshold of evidence and carries less serious consequences compared to a licence variation, suspension or cancellation.

Public consultation on an ASIC directions power highlighted the importance of clear procedural fairness for licensees and assisted the Taskforce in arriving at its final recommendations. The Taskforce considers that ASIC should be able to require compliance with AFS or credit licence obligations in real time, and that the regulator should be given powers to direct licensees to take or refrain from taking actions where appropriate for this purpose, subject to procedural fairness.

Summary of recommendations by chapter

Chapter 1: Self-reporting of contraventions by financial services and credit licensees	
Number	Description
1	The 'significance test' in section 912D of the <i>Corporations Act 2001</i> should be retained but clarified to ensure that the significance of breaches is determined objectively
2	Introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees under section 912D of the <i>Corporations Act 2001</i>
3	The obligation for licensees to report should expressly apply to misconduct by an employee or representative
4	Significant breaches (and suspected breach investigations that are ongoing) must be reported within 30 days
5	The required content of breach reports should be prescribed by ASIC and be lodged electronically
6	Criminal penalties should be increased for failure to report as and when required
7	A civil penalty should be introduced in addition to the criminal offence for failure to report as and when required
8	Encourage a cooperative approach where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity
9	Streamline the reporting requirements for responsible entities of managed investment schemes by replacing the requirements in section 601FC(1)(l) of the <i>Corporations Act</i> with an expanded requirement in section 912D.
10	Require annual publication of breach report data for licensees by ASIC
Chapter 2: Harmonisation and enhancement of search warrant powers	
Number	Description
11	ASIC-specific search warrant powers in various acts should be consolidated into the ASIC Act

12	ASIC Act search warrants should provide for search and seizure of 'evidential material'
13	ASIC Act search warrant powers should include ancillary powers that mirror the Crimes Act provisions
14	ASIC Act search warrants should only be issued when there is a reasonable suspicion of a contravention of an indictable offence
15	Material seized under ASIC Act search warrants should be available for use in criminal, civil and administrative proceedings for as long as is reasonable and practicable
16	Use of material seized under search warrants by private litigants should be subject to appropriate limits
<i>Chapter 3: ASIC's access to telecommunications intercept material</i>	
Number	Description
17	ASIC should be able to receive telecommunications intercept material to investigate and prosecute serious offences.
<i>Chapter 4: Industry codes in the financial sector</i>	
Number	Description
18	ASIC approval should be required for the content of and governance arrangements for relevant codes
19	Entities should be required to subscribe to the approved codes relevant to the activities in which they are engaged.
20	Approved codes should be binding on and enforceable against subscribers by contractual arrangements with a code monitoring body
21	An individual customer should be able to seek appropriate redress through the subscriber's internal and external dispute resolution arrangements for non-compliance with an applicable approved code
22	The code monitoring body, comprising of a mix of industry, consumer and expert members, should be required to monitor the adequacy of the code and industry compliance with it over time, and periodically report to ASIC on these matters.

Chapter 5: Strengthening ASIC's licencing powers	
Number	Description
23	ASIC should be able to refuse a licence application (or, for existing licensees, take licensing action) if it is not satisfied controllers are fit and proper
24	Empower ASIC with the ability to cancel a licence if the licensee fails to commence business within six months
25	ASIC should be able to refuse a licence application if it is false or misleading in a material particular.
26	Introduce an express obligation requiring applicants to confirm that there have been no material changes to information given in the application before the licence is granted
27	Align the assessment requirements for AFS licence applications with the enhanced credit licence assessment requirements
28	A statutory obligation should be introduced to notify change of control within 30 days of control passing, with penalties for failure to notify
29	Align consequences for making false or misleading statements in documents provided to ASIC in AFS and credit contexts
Chapter 6: ASIC's power to ban individuals in the financial sector	
Number	Description
30	Once an administrative banning power is triggered, ASIC should be able to ban a person from performing a specific function, or any function, in a financial services or credit business.
31	The grounds for exercising ASIC's power to ban individuals from performing roles in financial services and credit businesses should be expanded.
Chapter 7: Strengthening penalties for corporate and financial sector misconduct	
Number	Description
32	The maximum imprisonment penalties for criminal offences in ASIC-administered legislation should be increased as outlined in Table A

33	The maximum pecuniary penalties for criminal offences in the Corporations Act should generally be calculated by reference to the following formula: maximum term of imprisonment in months multiplied by 10 = penalty units for individuals, multiplied by a further 10 for corporations
34	The maximum penalty for a breach of section 184 should be increased to reflect the seriousness of the offence, to 10 years' imprisonment and/or a fine: for individuals the greater of 4,500 penalty units of three times the benefit gained (or loss avoided); and for corporations the greater of 45,000 penalty units, or three times the benefit gained (or loss avoided) or 10% annual turnover.
35	The Peters test should apply to all dishonesty offences under the Corporations Act
36	Imprisonment should be removed as a possible sanction for strict and absolute liability offences
37	An ordinary offence should be introduced to complement a number of strict and absolute liability offences as outlined in Table B
38	Maximum pecuniary penalties for strict and absolute liability offences currently set at 5, 10 or 15 penalty units should be increased to 20 penalty units for individuals, corresponding penalties for corporations should be increased to 200 penalty units
39	All strict and absolute liability offences should be subject to the penalty notice regime
40	Maximum civil penalty amounts in ASIC-administered legislation should be increased as follows: – For individuals: 2,500 penalty units (currently \$525,000); – For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (\$210 million)).
41	Disgorgement remedies should be available in civil penalty proceedings brought by ASIC under the Corporations, Credit and ASIC Acts
42	The Corporations Act should require courts to give priority to compensation
43	The civil penalty regime should be expanded to the provisions outlined in Table C
44	The provisions outlined in Table D should be made infringement notice provisions.

45	Infringement notices should be set at 12 penalty units for individuals and 60 penalty units for corporations for any new infringement notice provisions
<i>Chapter 8: ASIC's directions powers</i>	
Number	Description
46	ASIC should have the power to direct financial services or credit licensees in the conduct of their business where necessary to address or prevent risk to consumers.
47	The directions power should be triggered where ASIC has reason to suspect that a licensee has, is or will contravene AFS or credit licensing requirements (including relevant laws).
48	ASIC should be able to make an interim direction without a hearing, for a period of time, if the direction is to cease a type of activity and a delay in making a direction would be prejudicial to the public interest.
49	A licensee should have an opportunity to be heard before the direction is made, and the ability to review a direction at the Administrative Appeals Tribunal.
50	The requirement to comply with a direction should be an obligation of licensees, and there should be a civil penalty provision for non-compliance.

Principles guiding the ASIC Enforcement Review

In formulating its final positions, the Taskforce has been guided by the need to promote industry and community confidence in the regulatory framework and ensure that ASIC has pathways available to address issues appropriately as they arise. To achieve these aims, the Taskforce has adopted the following principles to guide the review.

These guiding principles should be considered together. In some circumstances, relevant guiding principles can have conflicting priorities, for example, where the Taskforce considered inserting a new regulatory pathway (the ability to disgorge profits, for example) the potential impost on industry needed to be measured against the benefits of the proposal. In these circumstances, the Taskforce applied relevant guiding principles and determined what it considers to be the most appropriate policy trade-offs between opposing principles.

ASIC's enforcement regime should be strengthened

In recent years, there have been widespread concerns about misconduct and consumer outcomes in the financial services sector. The Financial System Inquiry concluded that the current penalties in ASIC's legislation are unlikely to act as a credible deterrent against misconduct by large firms. The Senate Economic References Committee White Collar Crime report raised concerns that contraveners were profiting from their misconduct even after penalties were imposed.

These shortcomings have contributed to a decline in consumer confidence in the sector. The recommendations from those reviews led to the establishment of the Taskforce. Consistent with its terms of reference, strengthening ASIC's enforcement regime includes: addressing gaps or deficiencies to ensure more effective enforcement of the regulatory regime; fostering consumer confidence in the financial system; and enhancing ASIC's ability to prevent harm effectively.

ASIC's enforcement regime should be designed with checks and balances to ensure fair treatment and to safeguard against arbitrary exercise of powers

In considering how ASIC's enforcement regime may be strengthened, the focus should not be limited to desired regulatory outcomes. Due consideration should be given to protections afforded to the regulated population and how to best safeguard individual civil liberties and rights to ensure fair treatment by the regulator.

This includes setting appropriate checks and balances for the exercise of those powers. It also includes ensuring transparency of process, certainty of outcome and appropriate procedural fairness measures for those subject to ASIC's enforcement powers.

ASIC should have a strong and effective set of investigatory and information gathering powers

Investigatory and information gathering powers are essential to ASIC's work. They support ASIC's functions by enabling access to material information for ASIC's administrative and regulatory decision-making; ensuring proper protections for individuals providing information and in handling information obtained; and allowing ASIC to gather evidence that can be used in court proceedings.

The framework for investigatory and information gathering powers should be subject to appropriate checks and balances, as discussed above. Specifically, this includes determining the appropriate 'trigger' for powers, limiting access to information received, and providing clear procedures around the use of these powers.

The enforcement regime should provide ASIC with a comprehensive set of regulatory pathways to enable proportionate and tailored responses

Co-operation between ASIC and its regulated population is to be encouraged, but ASIC must also be able to take enforcement-oriented action where appropriate. The powers in ASIC's toolkit should therefore allow it to use lighter touch options (including options involving industry self-regulation) but at the other end of the spectrum, penalties should represent a credible deterrent and reflect community perceptions as to the seriousness of engaging in certain forms of misconduct. Further, ASIC should have a range of administrative powers appropriate to the efficient exercise of its functions.

ASIC-administered legislation should set obligations, burdens and sanctions consistently

Inconsistencies and arbitrary differences between and within ASIC-administered legislation are potentially unfair, inefficient and burdensome for the regulated population. In formulating its recommendations, the Taskforce has been guided by the need to achieve consistency, to ensure that to the extent possible, ASIC-administered legislation sets obligations, burdens and sanctions consistently.

ASIC's powers should be strengthened in a way that is justified and does not over-burden industry, or unduly impede innovation

To ensure ease of compliance for industry, regulatory regimes should be streamlined and avoid unnecessary overlap (or overregulation) wherever possible. Additional regulation should only be imposed where there is a demonstrated need (for example, where there is a regulatory gap or deficiency) and where the benefits exceed the potential impact on industry. This is important as excessive regulation could potentially stifle innovation.

The Taskforce considered the broader regulatory context (including other proposed reforms) in crafting its recommended reforms to ASIC's regulatory regime. Wherever possible, the Taskforce has preferred a simplified and streamlined approach to regulation that minimises regulatory cost.



Australian Government
The Treasury

Chapter 1 – Self-reporting of contraventions by financial services and credit licensees

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 1: Self-reporting of contraventions by financial services and credit licensees</i>	
Number	Description
1	The 'significance test' in section 912D of the <i>Corporations Act 2001</i> should be retained but clarified to ensure that the significance of breaches is determined objectively
2	Introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees under section 912D of the <i>Corporations Act 2001</i>
3	The obligation for licensees to report should expressly apply to misconduct by an employee or representative
4	Significant breaches (and suspected breach investigations that are ongoing) must be reported within 30 days
5	The required content of breach reports should be prescribed by ASIC and be lodged electronically
6	Criminal penalties should be increased for failure to report as and when required
7	A civil penalty should be introduced in addition to the criminal offence for failure to report as and when required
8	Encourage a cooperative approach where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity
9	Streamline the reporting requirements for responsible entities of managed investment schemes by replacing the requirements in section 601FC(1)(I) of the <i>Corporations Act</i> with an expanded requirement in section 912D.
10	Require annual publication of breach report data for licensees by ASIC

1. Self-reporting of contraventions by financial services and credit licensees

Overview

Self-reporting among AFS and credit licensees has come under intense scrutiny in the last decade. A series of parliamentary inquiries and media coverage relating to financial services-related misconduct have driven this scrutiny. Additionally, ASIC has publicly outlined concerns relating to aspects of the existing self-reporting regime.

Breaches of obligations set out in the Corporations Act span a broad spectrum of severity, from relatively minor contraventions such as one-off administrative failures to serious offences including fraud. Prior to 2003, AFS licensees were required to report all breaches to ASIC, regardless of severity. This requirement put a large regulatory burden on licensees in addition to an administrative burden on ASIC to process and appropriately action an influx of minor and insignificant reports. In 2003 a 'significance test' was introduced to provide a threshold for matters that necessitated self-reporting to ASIC.

The introduction of the 'significance test', while effective in reducing regulatory and administrative burdens, has given rise to ambiguity in terms of the threshold for the obligation to report as the test has a high degree of subjectivity. The test relies on an exercise of judgment by the licensee as to the significance of the breach. In determining significance, a licensee must consider, among other things, "the impact of the breach or likely breach on the licensee's ability to provide the financial services covered by the licence."¹ This subjective determination allows inconsistency in self-reporting.

Sound regulation of the financial services sector relies on timely detection of non-compliant behaviours. Early detection of misconduct, breaches of regulatory requirements and other important matters enable ASIC to:

- Monitor the extent and severity of non-compliance and commence surveillance and investigation where necessary;
- Take law enforcement and regulatory action where warranted, including administrative action to protect consumers of financial products and services; and
- Identify and respond to emerging risks and trends within the financial services industry.

Regulatory supervision is an effective way to detect non-compliant behaviour but where there are many individuals and entities subject to the regime, the detection of such behaviour is more difficult and can be significantly enhanced by effective mechanisms for self-reporting. The Corporations Act creates a self-reporting regime for the holders of an AFS licence requiring them to report certain breaches of their obligations to ASIC.² To comply with the mandatory obligation, licensees must put in place systems, policies and procedures to ensure that contraventions are identified and escalated appropriately within individual businesses subject to that Act.

Current obligation to self-report

AFS licence holders must comply with a set of general conduct obligations outlined in the Corporations Act.³ If an AFS licensee significantly contravenes, or is likely to significantly contravene

¹ *Corporations Act 2001*, s. 912D(1)(b)

² *Corporations Act 2001*, s. 912D

³ *Corporations Act 2001*, s. 912A and s. 912B

in future, one or more of the relevant obligations, the licensee has an obligation to report the matter to ASIC in writing.⁴ The report to ASIC must be made within 10 business days of the licensee “becoming aware of” the contravention or likely contravention.⁵ Failure to comply with this requirement is a criminal offence.⁶

The Corporations Act requires AFS licensees, when assessing the significance of a contravention, to consider:

- The number or frequency of similar previous breaches;
- The impact of the breach or likely breach on the AFS licensee’s ability to provide the financial services covered by the licence;
- The extent to which the breach or likely breach indicates that the AFS licensee’s arrangements to ensure compliance with those obligations is inadequate;
- The actual or potential financial loss to clients of the AFS licensee, or the AFS licensee itself, arising from the breach or likely breach; and
- Any other matters prescribed by regulations made for the purposes of section 912D(1)(b).⁷

There are additional factors that licensees may choose to take into account, but consideration of the above is paramount.

Concerns with the effectiveness of the existing AFS licensee self-reporting regime have been raised by ASIC and others in the course of a number of inquiries in recent years. Those concerns centre on:

- The subjectivity of the ‘significance test’ leading to inconsistent reporting of matters;
- The scope of application, with no equivalent reporting obligation on credit licensees and no specific obligation to report misconduct engaged in by employees and representatives of AFS licensees;
- Ambiguity as to when the time for reporting commences and delays in reporting; and
- The lack of flexibility in sanctioning failures to report and incentives to report.

Some submissions to the Taskforce also raised concerns about the auditor reporting obligations, in particular, inconsistency with the AFS licensee reporting obligation and duplication of reporting. After considering these issues the Taskforce decided not to recommend any changes to the auditor reporting requirements. The Taskforce considers that the existing requirements are appropriate and should operate alongside the AFS licensee reporting obligation given the role of an auditor.

Nature of the significance test

The key trigger for the obligation to self-report breaches is the significance of the breach. The significance threshold requires AFS licensees to make a qualitative assessment of any breach or likely breach with regard to the factors set out in the Corporations Act.⁸

The significance test transformed the previous objectively-based self-reporting obligation into a subjective one, with a number of factors intended to guide licensees in determining whether the obligation has been triggered. This is because significance is assessed from the perspective of the

⁴ *Corporations Act 2001*, s. 912D

⁵ *Corporations Act 2001*, s. 912D(1)(b)

⁶ *Corporations Act 2001*, s. 1311 and 1312 and item 264A of Schedule 3

⁷ *Corporations Act 2001*, s. 912D(1)(b)

⁸ *Corporations Act 2001*, s. 912(1)(b)

licensee . This subjectivity has the result that, although all AFS licensees have an obligation to report, the differing scale, nature and complexity of their respective businesses and balance sheets can mean that larger organisations need to report fewer breaches or less often - depending upon the precise interplay of each of the factors in the particular circumstances.

The subjectivity of the significance test is highlighted in *Regulatory Guide 78: Breach reporting by AFS licensees (RG78)*:

Whether a breach (or likely breach) is significant or not will depend on the individual circumstances of the breach. We consider that the nature, scale and complexity of your financial services business might also affect whether a particular breach is significant or not. You will need to decide whether a breach (or likely breach) is significant and thus reportable. When you are not sure whether a breach (or likely breach) is significant, we encourage you to report the breach.⁹

The subjectivity of the test has particular impact in borderline cases where it is necessary to determine whether a report to ASIC is necessary or not. In effect, in the absence of a clear or indisputable breach, licensees need to make a judgment whether a breach is significant or not, conscious of the factors stipulated in the statute. Licensees may sometimes adopt a view, rightly or wrongly, that:

- There is no impact of the breach on their ability to provide services;
- A given breach is an isolated incident or does not indicate that their compliance arrangements are inadequate; or
- The breach does not need to be reported because there are no losses to clients or the licensee's businesses or the losses are small or immaterial relative to capitalisation or balance sheet strength

These factors themselves are not necessarily objective either, since they involve judgments as to impact, adequacy of arrangements, and whether there is sufficient information or data to form views as to frequency and loss. In addition, only one factor focuses attention on the impact of the breach on consumers, in terms of actual or potential financial loss to clients. This is balanced against the other factors which focus on the significance of the breach to the AFS licensee's business. In aggregate, the test, including the statutory factors, therefore can tend to privilege licensee perceptions as to significance over external perspectives of significance.

The subjectivity of the test may be compounded by the fact that while some of the relevant licensee obligations in section 912A are objectively ascertainable, others are phrased in broad and subjective terms. Additionally, AFS licensees must make their own decisions about the weight to be given to each of the listed factors (and any other factors they consider relevant) in determining whether a breach or likely breach is significant, in the absence of a clear objective standard.

Another potential pitfall arises in respect of breaches that may involve detriment to consumers. Financial loss is not the only way in which an event can have an impact on consumers, but this is the only statutory factor which directs licensee attention towards consumers. For example, a failure to provide proper disclosure to a large number of clients may not be considered significant enough to report if it does not immediately involve financial loss. Nevertheless, a breach of this nature may be worth reporting to ASIC as it may impact trust and confidence and suggest a broader systemic failing. Erosion of trust and confidence in financial sector institutions can be seen as having a detrimental impact on consumers, even if it does not include direct financial loss.

⁹ *Regulatory Guide 78: Breach reporting by AFS licensees*, 78.12

Recommendation 1

The 'significance test' in section 912D of the *Corporations Act 2001* be retained but clarified to ensure that the significance of breaches is determined objectively.

The Taskforce recommends that the current 'significance test' for the obligation to report be retained but the Corporations Act should be amended to ensure that significance is determined by reference to an objective standard.

While this proposal was generally supported by industry questions were raised whether an objective test will incorporate a subjective element, with a number of stakeholders suggesting that the significance of a breach should be determined by reference to 'a reasonable person in the position of the licensee' or a compliance officer. The Taskforce considers that the test for determining whether a breach is significant and therefore reportable should, to the greatest extent possible, be set by reference to objectively determinable criteria.

A breach will be significant if there are sufficient facts or information to found an objectively reasonable belief, whether or not there is an actual belief, that it is significant having regard to the kind of factors set out in subsection 912D(1)(b) of the Corporations Act (subject to the matters deemed to be significant outlined below). A 'reasonable belief' will be formed if a reasonable person would expect the matter to be reported to the regulator.

To provide greater certainty for licensees and ensure that particular matters are always reported to the regulator, the new test should include a number of explicitly specified matters that are deemed to be significant. The nature of matters that should be deemed to be significant includes:

- Serious misconduct by an employee or authorised individual, including conduct that has resulted in or may result in the suspension, demotion, termination, resignation or referral to a law enforcement agency;
- Breaches that result in or have the potential to result in material loss to clients having regard to the amount invested and the circumstances of the client/s in question;
- In the case of a managed investment scheme, breaches that have or are likely to have a materially adverse effect on the interests of members of the scheme;
- Breaches of a financial services law that carry a penalty of imprisonment; or
- Breaches of financial services civil penalty provisions.

Additional matters should be able to be prescribed by regulation to enable a flexible response to risks as needed.

Any changes to the significance test should be supplemented by new, specific, regulatory guidance from ASIC that takes into account different businesses, products and distribution channels.

While as noted above there was general support for this proposal a number of submissions considered that the application of an objective test may not reduce ambiguity or lead to a change in the way that licensees assess breaches as there remain subjective elements in the significance criteria. Nevertheless, the Taskforce considers that, having regard to similar tests in other jurisdictions, this proposal in combination with the other recommendations will lead to greater consistency in reporting by licensees.

Scope of application

Currently, the *National Consumer Credit Protection Act 2009* (NCCP Act) does not impose a breach reporting obligation on credit licensees. Instead, the National Credit Act introduced a different

obligation, requiring credit licensees to lodge an annual Compliance Certificate with ASIC that nominally enables ASIC to broadly monitor compliance with general conduct obligations. When completing the Compliance Certificate, credit licensees are required to answer a series of questions, including whether they have adequate arrangements in place to meet their general compliance obligations. However, the Compliance Certificate regime is no substitute for the self-reporting obligation that AFS licensees are subject to because:

- The information in the certificate is high level, generalised information;
- ASIC is not able to ascertain the veracity of credit licensee responses in certificates without undertaking surveillance or issuing notices to obtain additional information; and
- There is no obligation to provide ASIC with information about breaches in a timely way, as certificates are only required annually.

ASIC currently receives information about possible significant failures to comply with the National Credit Act from the following sources:

- Self-reporting by a small number of credit licensees voluntarily;
- Competitor reports of misconduct from credit licensees about other credit licensees (particularly in relation to persons providing false information to support applications for credit by their clients); and
- Anonymised reports of possible systemic problems that are identified as a result of clients or customers activating external dispute resolution schemes.

Recommendation 2

Introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees under section 912D of the *Corporations Act 2001*.

The Taskforce recommends aligning the credit licensee reporting regime with the financial services licensee reporting regime so that both are subject to the same obligation and test for self-reporting. Expanding the obligation to report to credit licensees would allow ASIC to be informed of compliance issues in a more consistent and timely manner, as well as essential details around the nature of the breach, the adequacy of the credit licensee's response and whether any further regulatory action may be merited.

As credit licensees are currently expected to identify breaches and to maintain records of non-compliance, reporting compliance breaches to ASIC should not add significantly to the compliance obligations of credit licensees. While it might be said that, as some credit licensees are sole traders or one person companies, the compliance burden of self-reporting may increase, credit licensees are already required to have adequate compliance arrangements in place and to certify their compliance so this measure should not add to the existing costs.

While some of the relevant stakeholders suggested that imposing a breach reporting regime on credit licensees would place an onerous compliance and cost burden on them, most responses supported the harmonisation of breach reporting. The Taskforce considers that the particular characteristics of the credit industry and its participants should be taken into account in drafting the provision.

Recommendation 3

The obligation for licensees to report should expressly apply to misconduct by an employee or representative.

The Taskforce recommends that the obligation for licensees to report should expressly apply to misconduct by an employee or representative. Currently, the reporting obligation applies to breaches by an AFS licensee. However, Chapter 7 of the Corporations Act, in particular Part 7.7A, places important obligations on a representative (or provider of advice), rather than just the AFS licensee. While AFS licensees are in most circumstances liable for the conduct of employees and authorised representatives, there exists some ambiguity around when a breach by a representative is reportable. The decentralised nature of the authorised representative base in larger licensees may also present difficulties in ensuring timely identification and reporting of breaches.

The aim of this recommendation is to ensure that ASIC is notified of misconduct or other regulatory issues by representatives of licensees at the earliest opportunity. Extending the reporting obligation in this way would be consistent with the self-reporting regimes in a number of international jurisdictions, including the United Kingdom, Hong Kong and Singapore, which specifically require firms or companies to report misconduct engaged in by employees or representatives.

The Taskforce considers that this can be addressed by including serious misconduct by an employee or authorised individual in the list of misconduct that should be deemed to be reportable (see Recommendation 1).

Submissions to the Taskforce recognised that significant breaches or misconduct by employees or representatives may already be reported, but an express requirement would provide clarity. It was also noted that there would likely be an increase in breach reports relating to financial advice, including breaches of the duty of advisers to act in the best interests of clients. Broadly, respondents were supportive of the measure, and held that the licensee obligation to report misconduct by employees or representatives should be clearly and appropriately defined, with specific accompanying ASIC guidance describing potential breaches.

Timing and process

ASIC is concerned that uncertainty regarding the existing requirement to report within 10 business days after becoming aware of a breach or likely breach may delay reports. The potential for uncertainty arises from the fact that the commencement of the time period for reporting is dependent on subjective factors, including when the AFS licensee becomes aware of a breach and its significance as well as the robustness of internal reporting mechanisms. There also exists uncertainty whether the current 10 day reporting timeline commences from the licensee becoming aware of the breach or from the date on which the licensee forms the view that it is significant. The latter usually, though not always, may involve an internal investigation and in addition may give rise to a need to obtain legal advice as to significance and whether the reporting obligation is triggered or not.

Case study

Staff within an AFS licensee identified that some clients were being overcharged compared to the fees set out in the AFS licensee's Financial Services Guide. Staff within the AFS licensee investigated the issue, identified clients who were incorrectly charged and one year later engaged an external firm to provide independent advice on systems and controls. That firm advised that there were deficiencies in the controls in place to prevent such occurrences. Nine months later the risk rating of the issue was upgraded from low to medium risk. Another eight months passed before it was determined that it was a reportable issue and a breach report lodged with ASIC. Two and a half years had passed since the problem was originally identified.

From the perspective of licensees it is often difficult to gather all of the information needed to assess and report to ASIC within the current limit especially if fraud or deliberate concealment of information by the person responsible for the misconduct has occurred.

A separate issue relates to the content of breach reports. While there is a requirement to report breaches, there is no prescribed form in which to provide reports. Accordingly, the information contained in reports is determined by the AFS licensee and may not always be sufficient to enable ASIC to properly assess the breach. ASIC suggests Form FS80 (*Notification by an AFS licensee of a significant breach of a licensee's obligations*) on its website, but this is not compulsory and not uniformly used.

The varying quality and comprehensiveness of breach reports provided by AFS licensees means that ASIC is often not provided with enough information to assess and action a breach. This necessitates further inquiries by ASIC, which in turn increases the length of time taken to consider and deal with the breach report. Further, there is no obligation on AFS licensees to provide relevant supporting documentation accompanying the breach report.

Recommendation 4

Significant breaches (and suspected breach investigations that are ongoing) must be reported within 30 days.

The Taskforce recommends that there should be an objective element to the trigger for reporting and that reporting requirements should extend to circumstances where a breach is being investigated by the licensee but the investigation has not concluded within the prescribed time limit. In addition, the time frame should be extended so that licensees, in the first instance, have 30 days for conducting investigations and the initial assessment whether a matter is reportable. This should be achieved by providing that when a licensee becomes aware of conduct or has information that reasonably suggests that a breach has occurred, may have occurred or may occur in the foreseeable future, the licensee must as soon as practicable – but in any event within 30 calendar days – lodge a report with ASIC notifying that:

- A significant breach has occurred or may occur in the foreseeable future; or
- A significant breach may have occurred and is still under investigation, with an outline of the investigation being conducted by the licensee and the expected time frame to conclude the investigation. The licensee would be under a continuing obligation to submit a further report as soon as practicable if the investigation concludes that the breach has in fact occurred and is significant.

The extension of the reporting period from 10 to 30 days recognises and takes into account stakeholder submissions to the Taskforce that licensees generally require more than 10 days to conduct a sufficiently thorough investigation to determine whether a significant breach has occurred. This will also likely improve the quality of breach reports and so assist ASIC in the process of assessing such reports.

The 30 day reporting period should commence when the AFS licensee becomes aware of or has reason to suspect that a breach has occurred, may have occurred or may occur – rather than when the licensee determines that the relevant breach *has* occurred and *is* significant. This modifies the trigger for reporting so that it is based on an objective assessment of the information available to the licensee. There may also be instances where an AFS licensee could be deemed to be aware of the facts and circumstances that established the breach or where the licensee has received relevant information from various sources, such as a government agency, its auditor, and industry Ombudsman and/or a current or former employee. Should the licensee determine, during the period

of investigation that no significant breach has occurred, there would be no obligation to report to ASIC.

Initially, the Taskforce suggested that the current 10 business day timeframe should commence from when a licensee becomes aware or has reason to suspect that a significant breach has occurred, may have occurred or may occur. Responses to the position paper on this topic were varied. Numerous stakeholders did not support the extension to require reporting of suspected or potential breaches, with concerns that this would lead to over reporting and an increased burden on licensees. Others sought to clarify that the 10 day time frame would only commence once the licensee became aware of or had information reasonably suggesting that a breach had or may have occurred and had determined that it was significant. Others suggested that if the test was modified 10 business days may not be sufficient. The Taskforce considers that Recommendation 4 provides an objective element to the trigger for the reporting time frame, an expanded timeframe in which to report, and achieves greater certainty for licensees, with little or no additional regulatory burden.

Recommendation 5

The required content of breach reports should be prescribed by ASIC and be lodged electronically.

The Taskforce recommends that the required content of breach reports be prescribed by ASIC and lodged electronically. In a number of the reporting regimes, other than breach reporting, outlined in the Corporations Act, documents are required to be lodged with ASIC in a “prescribed form.” Such documents must conform to requirements as specified by ASIC.¹⁰ The Taskforce considers that the efficiency and usefulness of the reporting process would be enhanced if reports are required to:

- Be lodged with ASIC electronically in machine readable form to allow for some automated analysis of reports;
- Be lodged in a prescribed form; and
- Include information and supporting documents required by the form.

While specific information should be provided in the prescribed form there should also be sufficient flexibility to allow AFS licensees to supplement the information provided to ensure that ASIC receives all relevant information and contextual background. The requirement for electronic delivery would assist ASIC in processing the larger volumes of reports that is likely to result from the changes to the reporting regime as detailed. It would also assist ASIC in potentially deploying technology to automate some tasks relating to breach reporting, and may reduce regulatory burden by lessening the need for ASIC to issue notices for broad information.

Encouraging compliance

A failure to comply with the obligation to report is a criminal offence, with a maximum penalty of 50 penalty units or imprisonment for one year or both in the case of an individual, and a maximum penalty of 250 penalty units in the case of a body corporate.¹¹

¹⁰ *Corporations Act 2001*, Section 350

¹¹ See sections 1311(1A), 1312 and item 264A of Schedule 3 of the *Corporations Act 2001*. Currently a penalty unit is \$210, therefore the maximum penalties at present are \$10,500 for individuals and \$52,500 for a body corporate.

At present, there are no alternatives to criminal sanctions, which are in practice unsuitable in all but the most egregious cases of intentional failure to report when there is clear evidence of intent. In some instances, such evidence is unlikely to be available, or it may prove ambiguous. Further, prosecutions in these instances are likely to be complex as criminal standards of proof apply. Consequently, ASIC has only brought one prosecution for failure to report since the self-reporting regime was introduced. This suggests that the current regime is not conducive to pursuing action against non-compliant licensees. There is little utility in having a sanction that is rarely applied as this undermines any desired deterrent effect for non-compliance. The recommendations made in this report should have the effect of making the requirement easier to enforce by clarifying its operation.

Additionally, the level of the applicable fine is relatively low when compared to other statutory offences of a similar nature. ASIC is also limited by the scope of penalties available to it, and at present lacks lower impact penalties as part of its regulatory toolkit. This means that ASIC does not have the flexibility to pursue necessarily the most appropriate action depending on the severity and intent of breaches. There is room for enhancement of the penalty regime through expanding the enforcement options available to ASIC, as well as encouraging further collaboration between licensees and ASIC.

Recommendation 6

Criminal penalties should be increased for failure to report as and when required.

The Taskforce recommends that the monetary and custodial penalties for failure to report breaches in a timely fashion should be increased to reflect the importance of the obligation and community expectations. An increase to the maximum criminal penalty would make the offence an indictable rather than a summary offence, conveying the seriousness of a breach. The proposed increase is set out under recommendation 32.

While industry cooperation is an important feature of the self-reporting regime, the Taskforce considers that regulation should maintain a serious sanction to deter deliberate non-compliance with reporting obligations. The suite of recommendations relating to obligations to report aim to strike a balance between industry cooperation and ASIC's mandate to take appropriate and proportionate action in relation to identified breaches.

Stakeholder responses to this proposal were mixed, with several key players not supporting a criminal penalty for failure to report breaches. However, among these submissions and those that supported a criminal penalty regime there was agreement that such penalties should only apply in the most severe cases.

Recommendation 7

A civil penalty option be introduced in addition to the existing criminal offence for failure to report as and when required.

The Taskforce recommends that there be a civil penalty in addition to a criminal penalty for failure to report when required, or at all. This would give ASIC greater flexibility to pursue the most appropriate action depending on the severity and intent of the breach. At present, ASIC lacks a range of enforcement options, including lower impact penalties as part of its regulatory toolkit. Providing a range of enforcement options may become more important if the criminal penalty is increased, as proposed in Recommendation 6.

The introduction of a civil penalty may result in ASIC taking enforcement action in relation to breach reporting obligations more often, particularly because it could seek a civil penalty for any breach of section 912D of the Corporations Act when it pursues civil penalty proceedings. However civil

penalty proceedings can be complex and take time to resolve. Nonetheless, the Taskforce considers that the addition of a civil penalty option may increase the willingness of licensees to report to ASIC. The civil penalty regime, which is an important part of ASIC's regulatory toolkit, is dealt with in a later section of this report.

There was unanimous support for the introduction of a civil penalty regime among stakeholder submissions to the Taskforce, with responses acknowledging that this would enhance the flexibility of the penalty regime.

The Taskforce proposal to introduce a civil penalty and an infringement notice provision for a failure to report when required, are set out under recommendations 43 and 44.

Recommendation 8

Encourage a cooperative approach where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity.

The Taskforce recommends that a cooperative approach be encouraged where licensees report breaches, suspected or potential breaches or employee or representative misconduct at the earliest opportunity. While sanctions are a necessary and important feature of the self-reporting regime, the Taskforce also considers that there should be statutory provisions encouraging a collaborative approach between ASIC and AFS licensees, to encourage reporting of events and information to the regulator at the earliest opportunity.

This can be achieved through creating a formal provision expressly reinforcing ASIC's prerogative to choose whether to take action in respect of licensees when they self-report and certain additional requirements are satisfied. Particularly if a licensee is self-reporting suspected significant breaches of obligations, it should be given an opportunity to complete its investigations. If the licensee cooperates with ASIC and addresses the matter to ASIC's satisfaction, ASIC may choose, at its discretion, to take no administrative or civil action against the licensee. Circumstances conducive to such an outcome should include:

- The report to ASIC sets out a program to address the matter including completion of any further investigations and the manner in which the licensee will rectify or remediate the matter;
- The program includes regular time frames for the provision of additional information to ASIC;
- The program has clear time frames for implementation and completion;
- The program will resolve the matter to the satisfaction of ASIC; and
- The program is implemented to the satisfaction of ASIC.

This recommendation does not fetter ASIC's discretion to take action against licensees found to have breached their obligations in appropriate cases, particularly where there is systemic abuse and recidivism, so the object of general deterrence can be maintained. This recognises the submission of ASIC to the Taskforce, which, while supportive of a cooperative approach to reporting, argued that any formal provision to this effect should not prevent it from balancing the broad range of relevant factors in making a decision on what, if any, regulatory action to take.

Cooperation between licensees and ASIC already occurs in practice to some extent, but there will be benefits to industry and the regulator through making this express in the legislation, to promote a more co-operative approach between ASIC and its regulated population. Benefits could include:

- Ensuring ASIC’s limited resources can be focussed on more problematic or egregious matters; and
- Delivering quicker more certain outcomes for consumers (through remedial programs) than proceedings that could take years to resolve through a court.

Related matters

Recommendation 9

Streamline the reporting requirements for responsible entities of managed investment schemes by replacing the requirements in section 601FC(1)(l) of the Corporations Act with an expanded requirement in section 912D.

The Taskforce recommends that reporting requirements for responsible entities of managed investment schemes be streamlined by replacing the requirements in section 601FC(1)(l) of the Corporations Act with an expanded requirement in section 912D.

Section 601FC(1)(l) of the Corporations Act imposes an additional self-reporting obligation on responsible entities of managed investment schemes. Breaches of the Corporations Act that have had or are likely to have a materially adverse effect on the interests of members of the managed investment scheme must be reported by a responsible entity as soon as practicable after it becomes aware of the breach.

The trigger and time frame for reporting are different from those in section 912D of the Corporations Act. Generally, a breach that is required to be reported under section 601FC(1)(l) would, in most circumstances, also need to be reported under section 912D, although a breach that must be reported under s912D would not necessarily need to be reported under s601FC(1)(l).

This creates additional and unnecessary complexity and regulatory burden. The Taskforce recommends that the self-reporting obligation in section 601FC(1)(l) should be removed so that all breaches by responsible entities are self-reported under section 912D of the Corporations Act. This would streamline the self-reporting regime for responsible entities. To ensure there were no important matters that would no longer be reportable it would be appropriate to:

- Expand the types of conduct or breaches to be reported by responsible entities under section 912D to include significant or suspected significant breaches of the Corporations Act that relate to the scheme; and
- Incorporate the threshold for reporting in section 601FC(1)(l) (material adverse effect on the interests of members or consumers) in the list of breaches the legislation deems to be significant (see Recommendation 1).

Recommendation 10

Require annual publication of breach report data for licensees by ASIC.

The Taskforce recommends that ASIC should be required to report on breach report data for licensees annually. The Taskforce has noted Recommendation 9 in the House of Representatives Standing Committee on Economics 2016 *Review of the Four Major Banks: First Report* (the Coleman Report) regarding annual publishing of breach reporting and other data, including names of those “guilty of misconduct in the provision of financial services.” The Taskforce does not support the public naming of individuals based solely on beach reporting.

ASIC includes aggregate breach report data in its annual reports, including the number of breaches reported to ASIC. In addition, ASIC's annual reports also contain data on the number of criminal convictions, civil actions, amounts of fines or civil penalties imposed, and administrative actions such as banning of individuals in respect of misconduct in financial services. In respect of convictions and civil action as well as disqualifications, the names of culpable individuals are published by ASIC in various forms during the relevant year, including in media releases and ASIC's biannual enforcement reports. ASIC also reports on its current Wealth Management Project in its enforcement and annual reports, which includes information about the categories of gatekeeper against whom enforcement action was taken and highlight examples of conduct targeted during the relevant period.

The existing ASIC reporting framework should be supplemented, however, by publication of firm or license-level breach reporting data. This addresses the substance of the concerns identified in the Coleman Report regarding enhancing accountability and providing an incentive for improved behaviour, and provides a more appropriate balance between those considerations and the need for procedural fairness and to preserve the integrity of investigative processes.

Annual reporting at an industry or licensee level was supported in a number of submissions, although several submissions also opposed the publication of breach reporting data on the grounds that it would deter licensees from reporting breaches to ASIC. Several respondents to the Taskforce's position paper also submitted that there should be no "naming and shaming" of individual licensees or individuals. In the Taskforce's view this reporting should be confined to significant breaches and should be at the licensee level, but could extend to identifying the operational area of the licensee's organisation in which the breach occurred. The Taskforce considers that this may assist in enabling industry and consumers to identify areas where significant numbers of breaches are occurring and provide licensees with an incentive to improve their compliance outcomes in those areas. Reporting should be confined to licensees (not individuals) and the content of reporting should be considered after work by ASIC to determine what licensee-level disclosures would be most useful. This would include whether divided by industry or product, and whether limited to actual breach.



Chapter 2 – Harmonisation and enhancement of search warrant powers

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 2: Harmonisation and enhancement of search warrant powers</i>	
Number	Description
11	ASIC-specific search warrant powers in various acts should be consolidated into the ASIC Act
12	ASIC Act search warrants should provide for search and seizure of 'evidential material'
13	ASIC Act search warrant powers should include ancillary powers that mirror the Crimes Act provisions
14	ASIC Act search warrants should only be issued when there is a reasonable suspicion of a contravention of an indictable offence
15	Material seized under ASIC Act search warrants should be available for use in criminal, civil and administrative proceedings for as long as is reasonable and practicable
16	Use of material seized under search warrants by private litigants should be subject to appropriate limits

2. Harmonisation and enhancement of search warrant powers

Overview

Search warrants are one of the most effective investigative tools available to investigators to obtain and secure evidential material. They are widely used by a range of law enforcement agencies and regulatory authorities at the Commonwealth, State Territory levels.

Search warrants are executed without prior notice. This limits the opportunity for individuals subject to an investigation to destroy, alter or conceal evidence. By contrast, under some relevant legislation (but not the ASIC Act), ASIC is required, before applying for a search warrant, to first give the person concerned a 'Notice to Produce', effectively giving the investigated party notice of ASIC's interest.¹²

ASIC has legislative responsibility for enforcement of the Corporations Act, the ASIC Act, the NCCP Act, the *Superannuation Industry (Supervision) Act 1993* (SIS Act), the *Retirement Savings Accounts Act 1997* (RSA Act) and various other laws. Section 1(2)(g) of the ASIC Act provides:

In performing its functions and exercising its powers, ASIC must strive to ... take whatever action it can take, and is necessary, in order to enforce and give effect to the laws of the Commonwealth that confer functions and powers on it.

ASIC's core enforcement functions include, but are not limited to:

- Conducting investigations into suspected relevant contraventions of the law, which are variously enforceable by criminal prosecution, civil proceedings (including civil penalty proceedings) and/or administrative action;
- Commencing, and conducting or supporting the Commonwealth Director of Public Prosecutions (CDPP) to conduct, criminal prosecutions in respect of such contraventions;
- Commencing and conducting various types of civil proceedings in respect of such contraventions, such as proceedings for the imposition of civil penalties, proceedings to seek compensation for victims and interlocutory proceedings for injunctions in connection with investigations or proceedings being pursued by ASIC; and
- Taking various forms of administrative action in respect of such contraventions.

Current search warrant powers

For the purpose of carrying out its investigative functions ASIC is currently able to utilise specific search warrant powers contained in:

- Sections 35-57 of the ASIC Act;
- Sections 269-271 of the NCCP Act;
- Sections 271-273 of the SIS Act; and
- Sections 102-104 of the RSA Act

¹² NCCP Act, section 269(1); SIS Act, section 271(1); RSA Act, section 102(1).

These search warrant provisions all empower ASIC, for the purpose of exercising its investigative functions, to apply to a magistrate for a search warrant in respect of specific premises to search for and seize relevant 'books', a term which is broadly defined and encompasses computer devices.¹³

Additionally, ASIC can apply to a magistrate for a search warrant to be issued under section 3E of the Crimes Act for execution by the AFP, which can make seized material available to ASIC under s3ZQU of the Crimes Act. However, there are limitations on such material, as it can only be used by ASIC for the purpose of investigating and prosecuting criminal offences. It cannot be used for the purpose of investigating contraventions that are actionable by only civil or administrative proceedings and it is not admissible in any kinds of civil or administrative proceedings undertaken by ASIC.¹⁴

ASIC has identified problems with the search warrant powers available to it which limit their utility as an investigative tool in a number of circumstances. Those problems relate to:

- The inconsistencies between the specific search warrant powers contained in the ASIC Act, NCCP Act, SIS Act and RSA Act, especially in relation to the 'forewarning' requirement in the latter three Acts (but no longer in the ASIC Act);
- Warrants issued under the ASIC Act, NCCP Act, SIS Act and RSA Act authorise the search for and seizure of only specified "particular books," rather than the more generally described "evidential material" that can be seized pursuant to search warrants issued under the Crimes Act and Competition and Consumer Act;
- The lack of a range of ancillary provisions (including provisions relating to the search, seizure and copying of electronic material), such as those now contained in the Crimes Act, in the search warrant powers contained in the ASIC Act, NCCP Act, SIS Act and RSA Act; and
- ASIC's inability to use material, lawfully obtained pursuant to Crimes Act search warrants, for the purpose of investigating contraventions that can be addressed by only civil or administrative proceedings, or conducting any such proceedings, creates practical difficulties for ASIC and impacts on its ability to effectively collaborate with the AFP and other criminal law enforcement agencies

Consequentially, ASIC rarely exercises the search warrant powers in the ASIC Act, NCCP Act, SIS Act and RSA Act, generally favouring Crimes Act search warrants despite their limitations. Since January 2011, ASIC has obtained just over 200 warrants to search premises. Of those search warrants, two were obtained under the ASIC Act, with none obtained under the NCCP Act, SIS Act or RSA Act.

Nature of search warrants

The specific search warrant powers contained in the ASIC Act, NCCP Act, SIS Act and RSA Act are not supported by the range of provisions contained in the Crimes Act and the Competition and Consumer Act. As a result,

- There is no ability to apply for search warrants by telephone, facsimile or other electronic means in urgent cases;
- There are no clear powers relating to the use of electronic equipment at the premises (including to access data stored elsewhere) and copying or seizing data contained on electronic equipment;
- There is no power to take away electronic devices for further examination and/or processing;

¹³ See, for example, the definition of 'books' in section 5(1) of the ASIC Act, section 5(1) of the NCCP Act, section 10(1) of the SIS Act, section 16 of the RSA Act, each of which includes 'document'.

¹⁴ See, for example, *Williams v Keelty* (2001) 111 FCR 175; *ASIC v Rich* (2005) 220 ALR 324.

- With the exception of the ASIC Act, there is no clear power to require an occupier to provide reasonable assistance (such as opening locked storage cupboards, providing passwords, lighting, power or facilities) during the execution of a search warrant

Business practices have evolved in recent years to the point that core documentary evidence relevant to ASIC investigations, such as business and financial records, are now held predominantly, if not solely, in electronic form on computers and other electronic devices and not in paper form. Additionally, as methods of business communications have evolved from paper correspondence (such as letters and memoranda) through to electronic communications (such as emails and SMS texts) through to internet-based messaging and communication platforms (such as Snapchat, WeChat and WhatsApp) and social media platforms (such as Facebook), mobile phones and tablets have become repositories of communication records that may be important in ASIC investigations. Accordingly, there is a pressing need for ancillary powers expressly addressing the operation, of, copying, and seizure of data from computers and electronic equipment.

Recommendation 11

ASIC-specific search warrant powers in various acts should be consolidated into the ASIC Act.

The Taskforce recommends that ASIC-specific search warrant powers in various Acts should be consolidated into the ASIC Act. This would mean that search warrants obtained in investigations of contraventions of all legislation administered by ASIC, including investigations of suspected contraventions of the Corporations Act, ASIC Act, NCCP Act, SIS Act and RSA Act, would be centralised in the ASIC Act. General search warrant powers such as those in the Crimes Act would not be affected by this measure and could still be used by ASIC in appropriate circumstances. Search warrants under the enhanced ASIC Act provisions would continue to be issued to, and executed by, a member of the AFP or an ASIC officer accompanied by an AFP member.

In effect, this will remove the forewarning requirement from the NCCP Act, SIS Act and RSA Act, reducing the risk of the destruction, concealment and alteration of evidence by individuals under investigation by ASIC in relation to contraventions of those acts.

In addition, this will result in consistent search warrant powers across the legislation in respect of which ASIC has specific enforcement responsibility and enable consistency to be maintained. If amendments are considered necessary in the future, only one set of provisions will need to be amended. This may be particularly relevant given the other recommendations of the Taskforce relating to search warrant powers.

The Taskforce notes that the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) creates a standard framework for monitoring and investigation powers and includes provisions relating to the issue and execution of search warrants.¹⁵ The Regulatory Powers Act has effect where a Commonwealth act specifically triggers its provisions. Among other things, the Regulatory Powers Act provides a means for ensuring greater consistency in the monitoring and investigative powers exercised by regulatory agencies, thereby reducing the administrative burden on agencies and providing greater certainty for those who are the subject of investigations. The Regulatory Powers Act may provide another means by which to achieve the harmonisation of ASIC's search warrant powers although care would need to be taken to ensure that the provisions are equivalent to those in the Crimes Act.

¹⁵ See sections 32 and 18-22 of the Regulatory Powers Act. The Act also includes provisions relating to the conduct of investigations and enforcement provisions relating to civil penalties, infringement notices, enforceable undertakings and injunctions.

The Taskforce agrees with the Law Council’s submission that section 69 of the ASIC Act should extend to the proposed consolidation of search warrant powers into the ASIC Act. Section 69 of the ASIC Act preserves legal professional privilege. It specifies that lawyers are entitled to refuse to comply with a requirement under certain provisions of the ASIC Act to provide information or produce a book where to do so would involve disclosing, or the book contains, a privileged communication.

Recommendation 12

ASIC Act search warrants should provide for search and seizure of ‘evidential material.’

The Taskforce recommends removing the requirement for search warrants issued under the ASIC Act, NCCP Act, SIS Act and RSA Act to specify particular books that can be searched and seized under the warrant. This could be achieved by modelling the ASIC Act search warrant power on the search warrant powers in the Crimes Act and Competition and Consumer Act, such that:

- A warrant could be issued under the ASIC Act where there are reasonable grounds for suspecting that there is or will be “evidential material” at premises identified in the warrant; and
- Adopting the broader “kind of evidential material specified in the warrant” criterion for search and seizure under the warrant.

In the Crimes Act, evidential material means a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form.¹⁶ The definitions of a “thing relevant to” an indictable and a summary offence mean, amongst other things, that the material relating to the commission of Commonwealth offences and State offences that have a federal aspect or connection can be seized under a Crimes Act warrant.¹⁷

In the Competition and Consumer Act evidential material means a document or thing that may afford evidence relating to a contravention of that Act and contraventions of other acts in respect of which the ACCC performs an enforcement role. The broad definition of evidential material in the Competition and Consumer Act means that the ACCC can theoretically seek a search warrant in any investigation where there are reasonable grounds to suspect a contravention of the Competition and Consumer Act, whether or not those contraventions would give rise to criminal or civil consequences.

Recommendation 13

ASIC Act search warrant powers should include ancillary powers that mirror the Crimes Act provisions.

The Taskforce recommends that the new or expanded ASIC Act search warrant powers include additional provisions that mirror the provisions in Division 2 of Part IAA of the Crimes Act. Given that the Crimes Act has been most recently amended it provides the most up to date provisions, which have addressed issues associated with searching and seizing electronic equipment. This would:

- Enhance the search warrant powers in relation to the search, seizure and copying of electronic evidence to reflect contemporary business and communication practices in which information is stored and transmitted electronically rather than in paper form;

¹⁶ Section 3C of the Crimes Act

¹⁷ Section 3 of the Crimes Act

- Provide additional practical powers such as the ability to obtain search warrants from a magistrate by telephone and the ability to seize evidence of other corporate crime which is identified in the course of executing the warrant;
- Harmonise the ASIC Act, NCCP Act, SIS Act and RSA Act search warrant powers with the search warrant powers contained in other legislation (Crimes Act, Competition and Consumer Act) that are well understood by regulatory and law enforcement agencies and the Courts; and
- Increase the overall effectiveness of the search warrant powers available to ASIC and lead to consequential efficiencies in relation to ASIC’s investigations and enforcement proceedings.

It is not anticipated that this will lead to a substantial increase in the number of search warrants sought by ASIC. Search warrant operations are major logistical exercises that involve significant cost, planning, and coordination with the AFP. They also require considerable resources to be available, both from ASIC, the AFP, and, in certain circumstances, external computer forensic providers. Consequently, search warrants will only be appropriate in serious cases where there is a real risk of destruction or concealment of evidence.

Issuing warrants

Recommendation 14

ASIC Act search warrants should only be issued when there is a reasonable suspicion of a contravention of an indictable offence.

The Taskforce recommends that ASIC Act search warrants should only be issued when there is a reasonable suspicion of a contravention of an indictable offence. This would impose a threshold for the issue of an ASIC Act search warrant.

The Taskforce considers that the appropriate threshold for the issue of a search warrant under an enhanced ASIC Act search warrant power would be a reasonable suspicion of:

- An indictable offence against the Corporations Act, ASIC Act, National Credit Act, SIS Act and RSA Act; or
- An indictable offence that otherwise falls within ASIC’s general power of investigation under section 13(1) of the ASIC Act or section 247(1) of the National Credit Act.

Imposing this threshold would ensure that search warrants are only issued in investigations of serious offences and achieves an appropriate balance between the need for the regulator to have access to effective investigative tools as well as the rights of individuals.

Use of seized material

Section 37(5) of the ASIC Act permits ASIC to seize “particular books” for as long as a reason exists under the Act to retain it. ASIC may use or permit the use of seized books for the purposes of a proceeding, which is defined broadly and includes criminal, civil and administrative proceedings. In contrast, evidential material obtained pursuant to a Crimes Act search warrant can only be used by ASIC for the purpose of investigating and prosecuting criminal offences. It cannot be used for the purpose of investigating contraventions that are actionable by only civil or administrative proceedings and it is not admissible in any kinds of civil or administrative proceedings undertaken by ASIC. ASIC considers that restrictions on the permissible use of evidence obtained pursuant to Crimes Act search warrants create practical difficulties because:

- Most ASIC investigations will have actual or potential criminal, civil and administrative enforcement components;
- At the early stages of an investigation (which is when search warrants are typically executed) it will rarely be known which type or types of enforcement action will ultimately be available and most appropriate; and
- The receipt of evidential material obtained pursuant to Crimes Act search warrants (that can only be lawfully used for ‘criminal’ law enforcement purposes) can potentially taint non-criminal aspects of an ASIC investigation and/or invite costly and time-consuming legal challenges.

ASIC is required to protect information that is provided to it in confidence or that is protected information from unauthorised use or disclosure. However, there are a number of circumstances in which ASIC is permitted to or may be required to release information, which may include material seized under a search warrant. ASIC can disclose information to Australian and international governments and agencies to enable or assist them to perform their functions and exercise their powers. In addition, in the following circumstances, information may be provided to private litigants:

- ASIC may provide a transcript of an examination conducted by ASIC (which may refer to seized material) to a person’s lawyer if the person is commencing a proceeding to which the examination relates;
- ASIC may release books obtained under a compulsory notice or warrant to third parties for use by them in proceedings;
- ASIC may be served with a subpoena or summons requiring production of the material;
- ASIC may be required to respond to a notice for non-party discovery.¹⁸

In each of the above situations there may be safeguards that will prevent or limit ASIC’s ability to release the information. However the extent to which these safeguards apply will depend on the specific circumstances applying to the request. Although not very common, material seized under a search warrant may be released to private litigants for the purposes of separate legal proceedings.

Recommendation 15

Material seized under ASIC Act search warrants should be available for use in criminal, civil and administrative proceedings for as long as is reasonable and practicable.

The Taskforce recommends that ASIC should be able to use and permit the use of material seized under an ASIC Act search warrant for the purposes of criminal, civil and administrative proceedings for as long as is reasonable and practicable. If the other reforms proposed are adopted this would apply to material seized in investigations of suspected contraventions of the Corporations Act, ASIC Act, NCCP Act, SIS Act and RSA Act with a threshold for applying for a warrant of reasonable suspicion of an indictable offence.

The Taskforce recommends that limitations on the circumstances in which ASIC can hold or use seized material before it must be returned should be imposed. For example, the Competition and Consumer Act provides that items seized under a search warrant can be kept by the ACCC for up to 120 days, after which time reasonable steps must be taken to return the material unless proceedings have commenced and not been completed, or a magistrate has made an order that the inspector may retain the material for the ongoing purposes of investigation. Taskforce consultation on this matter received submissions proposing a range of approaches. It was noted that 120 days would be

¹⁸ *Information Sheet 181: Providing information and documents to private litigants and Regulatory Guide 103: Confidentiality and release of information*

insufficient as it is rare for criminal proceedings to have commenced within 120 days of a search warrant being executed.

Currently, ASIC can retain material seized under a search warrant “for as long as is necessary” pursuant to subsection 37(5) of the ASIC Act. The Taskforce recognises that criminal investigations and prosecutions brought by ASIC are generally complex and may take time to complete. Setting a time limit for the retention of stored material with an ability to apply for an extension of time is likely to lead to additional court proceedings, and will not necessarily ensure that investigations based on search warrant material are conducted efficiently. The Taskforce considers that ASIC’s retention of material seized under search warrant should be subject to a requirement that the retention is reasonable in the circumstances. Accordingly, the Taskforce considers that ASIC’s current ability to hold and use seized material “for as long as necessary” should be modified to enable ASIC to hold the material for as long as is reasonable and practicable in the circumstances.

Case study

In the case of Andrew Sigalla, former chairman of Sydney-based technology company TZ Ltd, there were almost four years between the commencement of an ASIC investigation and charges being laid, with seven years between the beginning of the investigation and the case going to trial. The investigation involved over 2,300 hours of forensic accounting analysis of more than 27 bank accounts to trace stolen funds. 24 charges were laid against Sigalla involving almost \$9 million of company funds. Sigalla received a 10 year prison sentence.

Recommendation 16

Use of material seized under search warrants by private litigants should be subject to appropriate limits.

The Taskforce considers it appropriate to provide additional protection to material seized under a search warrant that would limit the ability of private litigants to access that material, given:

- The invasive nature of search warrants;
- That they involve an exercise of state power by a law enforcement agency;
- The impacts on a person’s rights and dignity, including with respect to privacy and to avoid self-incrimination; and
- The enhanced ASIC Act search warrant power proposed in this paper will enable ASIC to search and seize a broader range of material, including data from electronic devices.

Public consultation sought views on whether private litigants should be able to access material seized by ASIC under a search warrant, recognising that there are a number of circumstances in which ASIC is permitted to or may be required to release information, which may include material seized under a search warrant, at the request of private litigants.

After considering a range of submissions on this issue, the Taskforce recommends that it would only be appropriate for private litigants to access material seized by ASIC under a search warrant where they have obtained an order from a Court, which may include a subpoena or other processes available under relevant court rules.



Chapter 3 – ASIC’s access to telecommunications intercept material

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 3: ASIC's access to telecommunications intercept material</i>	
Number	Description
17	ASIC should be able to receive telecommunications intercept material to investigate and prosecute serious offences.

3. ASIC's access to telecommunications intercept material

Overview

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) regulates access to and use of:

- Telecommunications interception – live stream of the content of communications carried over a telecommunications service, for example, real-time listening of telephone calls;
- Telecommunications data – including subscriber details and details of telecommunications such as call time and location but not actual content; and
- Stored communications – including text messages, voicemails and emails.

The TIA Act sets out a regime that enables agencies to access various forms of telecommunication information in prescribed circumstances and depending on the agency's status as an interception agency, criminal law enforcement agency or enforcement agency. The staggered levels of access with differing thresholds for access to communications are based on considerations of the relative intrusiveness of particular kinds of communications.

Designated 'interception' agencies¹⁹ can seek warrants (TI warrants) to intercept telecommunications for the purpose of investigating serious offences defined in section 5D of the TIA Act. These are all agencies whose exclusive area of operation is law enforcement.²⁰ ASIC is not an interception agency for the purposes of the TIA Act.

Interception agencies are subject to more comprehensive oversight and accountability frameworks than criminal law enforcement and regulatory agencies, such as ASIC. Interception agencies must apply to an eligible judge or nominated member of the Administrative Appeals Tribunal for a TI warrant.²¹ A TI warrant will only be granted where the applicant can demonstrate that it would likely assist with the investigation of a "serious offence," and satisfy a number of other statutory criteria, which include having regard to privacy concerns.²²

The information an interception agency receives under a TI warrant is subject to strict controls under the TIA Act.²³ However, interception agencies can generally use material obtained pursuant to TI warrants for the purpose of investigating and prosecuting a "prescribed offence," which includes a "serious offence" or other crimes punishable by imprisonment for a period of at least three years.²⁴

Interception agencies may also communicate information obtained under a TI warrant to another agency specified in the TIA Act (recipient agency) if the material appears (among other things) to relate to a matter that could be investigated by the recipient agency. In this case the recipient

¹⁹ Including the Australian Federal Police (AFP), Australian Commission for Law Enforcement Integrity and Australian Crime Commission, now called the Australian Criminal Intelligence Commission.

²⁰ In 2007, the Parliamentary Joint Committee on the Australian Crime Commission, in an inquiry into the future impact of serious and organised crime on Australian society, considered telecommunications interception to be an 'invasive power' and recommended that the 'potential gravity of the exercise of such powers should be properly restricted to those agencies whose exclusive area of operation is law enforcement.'

²¹ TIA Act, sections 5 and 39.

²² TIA Act, section 46.

²³ See in particular TIA Act, sections 63, 67, 68 and 74

²⁴ TIA Act, sections 67, 5 and 6L

agency may generally use the information to investigate and prosecute offences within its jurisdiction.²⁵

Current status of ASIC's access to telecommunications intercept material

ASIC is recognised as a criminal law enforcement agency under the TIA Act. This gives it powers enabling it to access telecommunications data if its disclosure is reasonably necessary for enforcement of criminal law, enforcement of a law imposing a pecuniary penalty or protection of public revenue. ASIC can also apply for warrants authorising access to stored communications for the purpose of investigating a serious contravention or other offences. Any subsequent use of telecommunications data or stored communications obtained by ASIC is strictly restricted by legislative and procedural safeguards.

ASIC however, is not an interception agency or recipient agency under the TIA Act, despite the fact that the definition of 'serious offence' in the TIA Act includes offences against provisions of the Corporations Act relating to insider trading,²⁶ market manipulation²⁷ and, financial services fraud,²⁸ as well as other fraud offences that are commonly investigated and prosecuted by ASIC.

As a result, ASIC cannot apply for TI warrants for the purpose of investigating defined serious offences within its statutory responsibility or receive intercepted material lawfully obtained by other agencies for the purpose of investigating such offences or other "relevant offences."²⁹

Where an interception agency uncovers material relating to serious Corporations Act offences or other serious corporate crime, it is currently prevented from sharing that material with ASIC, except for the specific purpose of that agency's own investigation. This means that ASIC's ability to conduct cooperative investigations with other interception agencies (such as the Australian Federal Police) is limited. As a result of these issues, in practice ASIC officers are seconded to the relevant interception agency to assist in the conduct of an investigation by that agency. This can create management and administrative difficulties and result in inefficiencies and delays, which can in turn prejudice the investigation.

Receiving telecommunications intercept material

Recommendation 17

ASIC should be able to receive telecommunications intercept material to investigate and prosecute serious offences.

The Taskforce considers that reform of telecommunications interception powers would:

- Reflect ASIC's current status as a criminal law enforcement agency that has primary responsibility for investigating criminal offences that are already expressly defined as "serious offences" in the TIA Act and are difficult to prove;
- Enhance ASIC's ability to successfully investigate and prosecute serious offences and thereby achieve its legislative objectives;

²⁵ TIA Act, section 68.

²⁶ Corporations Act, s1043A.

²⁷ Corporations Act, ss1041A — 1041D

²⁸ Corporations Act, ss1041E — 1041G

²⁹ TIA Act, section 5E and section 116

- Allow ASIC and other agencies, in particular the AFP, to conduct effective cooperative or parallel investigations and share evidence relating to serious criminal wrongdoing that may fall within each agency’s principal remit (for example, foreign bribery); and
- Avoid the circumstance in which an interception agency is in possession of evidence of serious corporate offences but unable to share that information with ASIC.

In advancing this recommendation the Taskforce recognises that telecommunication intercept powers intrude on the privacy of individuals. Accordingly, any legislative expansion of the powers needs to be proportionate to the seriousness of the misconduct sought to be addressed and ensure that there are adequate safeguards to protect against unjustified intrusion into personal privacy.

The Taskforce recommends that ASIC should be able to receive telecommunications lawfully intercepted under a TI warrant for the purposes of investigating and prosecuting offences, within its jurisdiction, that are defined under the TIA Act as “serious offences,” including serious Corporations Act offences. While there may be a number of ways to enable ASIC to receive and use telecommunications lawfully obtained by other agencies, the Taskforce specifically recommends that ASIC should be defined as a “recipient agency” under section 68 of the TIA Act.

The recommendation would not expand the range of offences for which TI warrants could be sought under the TIA Act, the range of evidence that could be obtained pursuant to a TI warrant or broaden the admissibility of material obtained under a TI warrant. It will only permit ASIC to receive and use information that has already been lawfully intercepted by other interception agencies where that information is or may be relevant to a serious offence that ASIC may investigate. In addition, the existing robust safeguards contained in the TIA Act would remain intact. When in receipt of material from an interception agency ASIC would be subject to the same strict limitations, restrictions, reporting and record-keeping requirements that currently apply.

Public consultation on this proposal drew mixed responses, with calls for both stronger powers for ASIC as well as maintaining ASIC’s current limited capabilities. The Taskforce considers that the recommendation above achieves an appropriate balance between necessary powers to investigate and prosecute “serious offences”, and respect for the privacy of individuals.



Chapter 4 – Industry codes in the financial sector

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 4: Industry codes in the financial sector</i>	
Number	Description
18	ASIC approval should be required for the content of and governance arrangements for relevant codes
19	Entities should be required to subscribe to the approved codes relevant to the activities in which they are engaged.
20	Approved codes should be binding on and enforceable against subscribers by contractual arrangements with a code monitoring body
21	An individual customer should be able to seek appropriate redress through the subscriber's internal and external dispute resolution arrangements for non-compliance with an applicable approved code
22	The code monitoring body, comprising a mix of industry, consumer and expert members, should be required to monitor the adequacy of the code and industry compliance with it over time, and periodically report to ASIC on these matters.

4. Industry codes in the financial sector

Overview

Industry codes – often described as ‘codes of practice’ or ‘codes of conduct’ – are intended to improve confidence in the relevant industry and to provide a set of best practice guidelines to which participants should adhere. The Australian financial sector at present has a system of codes to which most participants in key industries subscribe. Despite this, the current codes regime is widely considered insufficient, lacking regulatory oversight and limiting consumer confidence in the sector. The impact of recent poor practice has resulted in the Australian financial sector coming under intense public and regulatory scrutiny and impaired consumer confidence in the sector. A robust and enforceable code regime subject to ASIC oversight would likely increase public trust in the financial sector and improve both practice as well as dispute resolution mechanisms.

At present, ASIC approval of relevant codes is optional and seldom sought. ASIC has the power under the Corporations Act to approve codes, though it is not required to do so and only issues approvals on application. To gain ASIC approval, the industry code must conform to the guidelines contained in *Regulatory Guide 183: Approval of financial service sector codes of conduct* (RG183).

ASIC can achieve greater regulatory oversight through a co-regulatory model by exercising its power to approve codes. Under such a co-regulatory model codes would remain industry-led and not mandated by legislation, but would require ASIC approval and be subject to monitoring. Under this model, industry participants would be required to subscribe to an ASIC approved code, and in the event of non-compliance with the code, an individual customer would be entitled to seek appropriate redress through the participant’s internal and external dispute resolution arrangements.

Confidence in the financial sector will likely be increased through evidence that industry participants are governed by binding and enforceable codes of practice. Such codes would ensure that breaches are properly acted upon and that consumer complaints are handled through appropriate mechanisms. The Taskforce considers that the proposed code regime should, where possible, align with the proposed jurisdiction of the new Australian Financial Complaints Authority (AFCA), which will operate the dispute resolution system that consumers can access.

The content of codes would remain a matter for industry to determine (subject to it being sufficient to obtain ASIC’s approval). The Taskforce anticipates that ASIC would ultimately determine which activities or sectors would be appropriate for the application of the co-regulatory approach to industry codes, and also recognises that there should ideally be a single approved code covering an activity, rather than a proliferation of alternative codes (but acknowledges that in some sectors more than one code may be appropriate, having regard to the structure of the industry). The proposed model does not preclude the adoption of other, voluntary codes in relation to financial sector activities not specified by ASIC.

The Taskforce considers that the proposed co-regulatory model would substantially strengthen the existing code regime while preserving the participatory role for industry.

Current status of industry codes

The Government’s approach to codes to date has been to provide flexibility to industry participants. It has sought to foster an environment in which industry works cooperatively with the regulator and consumer associations to determine best practice.

Currently, there are 11 codes in the financial services industry, with the Financial Planning Association Professional Ongoing Fees Code the only one with formal ASIC approval. The codes are:

- Code of Banking Practice, an initiative of the Australian Bankers' Association;
- Customer Owned Banking Code of Practice (developed by Abacus, now the Customer Owned Banking Association);
- Financial Planning Association of Australia's Code of Professional Practice;
- General Insurance Code of Practice;
- ePayments Code (formerly the Electronic Funds Transfer Code of Conduct);
- National Insurance Brokers Association's Insurance Brokers Code of Practice;
- Mortgage and Finance Association of Australia's Code of Practice;
- Finance Brokers Association of Australia's Code of Conduct;
- Australian Collectors and Debt Buyers Association Code of Practice;
- Financial Services Council's Life Insurance Code of Practice; and
- Financial Planning Association Professional Ongoing Fees Code.

These codes contain guidelines specific to the industries they govern, prescribing rules for dispute resolution and sanctions for breaches. These rules are intended to supplement regulation in areas which require flexibility, as well as the ability to respond to changing expectations and circumstances. Codes are an effective source of dispute resolution and also have potential to improve industry practices.

Case study

The Financial Conduct Authority (FCA) is the conduct regulator for financial services firms and financial markets in the United Kingdom, and is the prudential regulator for a portion of those firms. The FCA has the power to issue statements of principle and code of practice with respect to the conduct expected of approved persons. They are able to take disciplinary action against those that have failed to comply with codes of practice; however, enforceability does not extend to private actions for breaches of the code.

Approval of codes

One of the primary challenges of the code of conduct regime at present is that codes are not required to be approved by ASIC. The result is that there is no external compulsion on those formulating industry codes to include a minimum set of consumer protections or minimum standards on enforceability. ASIC's power to approve codes exists under the Corporations Act, extending to codes that "relate to any aspect of the activities of" AFS licensees and their authorised representatives, and "issuers of financial products."³⁰ At present, to meet the ASIC threshold, a code should satisfy the following criteria:

- The rules contained in the code must be binding on (and enforceable against) subscribers through contractual arrangements;
- The code must be developed and reviewed in a transparent manner, which involves consulting with relevant stakeholders including consumer representatives; and
- The code must have effective administration and compliance mechanisms.³¹

ASIC approval of codes is currently not a legislative requirement and none of the major codes have been approved by ASIC. This means there are still no regulated minimum standards which the provisions of codes must meet.

³⁰ *Corporations Act*, Section 1101A.

³¹ RG183.20 (*Regulatory Guide 183: Approval of financial service sector codes of conduct*)

Recommendation 18

ASIC approval should be required for the content of and governance arrangements for relevant codes.

The requirements governing approval of industry codes by ASIC are largely covered by RG183. However, it may prove necessary for ASIC to review and update that document to capture the full spectrum of requirements of the proposed co-regulatory model. Specifically, the Taskforce recommends that ASIC approval include the following requirements:

- Each code would set out clear service standards that a consumer or small business customer can expect in dealings with the subscriber, and these should be more than mere restatements of existing obligations at law;
- Codes should be formulated by industry and formalised through appropriate structures, such as an incorporated code body with a board made up of an appropriate mix of industry representatives, consumer representatives and independent experts; and
- Codes should include robust enforcement provisions, on the basis that compliance with the code by subscribers is expected rather than optional or aspirational.

The Taskforce recognises that if an industry is required by ASIC to have its code approved this may involve costs as well as time for negotiations with ASIC. Additionally, ASIC's enhanced role under the new model may require additional resourcing.

Submissions to the Taskforce's positions paper on this were mixed. Many submissions argued that particular industries or codes should or should not be subject to the requirement for an ASIC approved code. The Taskforce accepts that not all industries are likely to be appropriate for the operation of this regime. The requirements may only be appropriate for sufficiently mature industries where the industry sector, or a significant proportion of it, has the necessary capacity and commitment to implement and manage a code that meets the approval standards. The Taskforce recognises that imposing a mandatory requirement on individual licensees to subscribe to an ASIC approved code will not overcome the lack of capacity in an industry sector to develop one. However, the Taskforce believes that the process of identifying appropriate industries and activities for the application of the requirement must be done on a case by case basis, taking into account the environment in any sector at the time. This is why the Taskforce considers that ASIC should have discretion to determine the activities and industry sectors in which it is appropriate for the requirement to operate. This could be supplemented by appropriate guidelines in the implementing legislation.

The Taskforce considers that ASIC should, in considering the potential application of the new regime, prioritise assessment of retail banking, retail life insurance, the provision of insurance and associated services through superannuation or other group arrangements, retail general insurance, and insurance brokerage. As noted in the Taskforce's position paper, the ePayments code differs from other codes in the financial services sector in some respects, including that it is ASIC-administered. ASIC submitted that, as a result of these differences, the ePayments code should be dealt with separately and potentially given legislative effect (e.g. through a legislative rule-making power). The Taskforce notes that this is a matter the Government may wish to consider, but that the regime recommended in this Chapter should remain open for application to the ePayments code.

The Taskforce raised a question around competition considerations in its positions paper and some submissions touched on this. The key issue is that certain conduct associated with forming and subscribing to codes may potentially impact competition and so may also enliven provisions of Part IV of the Competition and Consumer Act 2010. The position paper flagged that consideration may need to be given to whether these matters should be expressly taken to be authorised as an exception to Part IV of the *Competition and Consumer Act 2010*. The Taskforce takes no final view on this but notes that consideration should be given, in implementing this recommendation, to the

question whether the process for obtaining approval can be streamlined in a way that addresses any concerns over the effect of codes that the Australian Competition and Consumer Commission may have in any individual case.

Subscribing to codes

One of the major challenges of the current industry code of conduct regime is that the benefits of industry codes are not available to significant numbers of consumers because not all players in relevant industry subsectors are code subscribers. Even in some of the key financial subsectors, there is significant underrepresentation. For example, of the 33 Australian owned banks, 10 are signatories to the Banking Code of Practice and 14 are signatories to the Customer Owned Banking Code of Practice. Consumer confidence is lessened when some industry participants choose not to become signatories to their relevant code.

For a code to be enforceable, subscribers must first agree to be bound by the terms of the code. There are two main types of arrangements for contractual enforceability. In the first and most common, there is a contractual agreement to abide by the code between subscribers and the relevant body with the power to administer and enforce the code. The second is where code subscribers incorporate their agreement in individual contracts with consumers.

Recommendation 19

Entities should be required to subscribe to the approved codes relevant to the activities in which they are engaged.

The Taskforce recommends that, entities engaging in activities covered by an approved code should be required to subscribe to that code. This could be achieved by a condition on their Australian Financial Services Licence or some similar mechanism. Some submissions noted that not all entities participate in industries hold AFSs. An example is superannuation trustees. The Taskforce accepts this but notes it is the reason why “or other similar mechanism” was mentioned in its positions paper. Subscription to a code could, for example, be tied to the provision of certain products or services.

ASIC submitted, and the Taskforce accepts, that the power to activate this requirement should, to the extent possible, be unfettered. ASIC’s power to impose the requirement in licence conditions on new and existing licensees (or through any other mechanism adopted by the legislature), should be modifiable by ASIC and should have a legislative, not administrative character. Further, the Taskforce acknowledges that in some circumstances, it may be necessary for ASIC to impose the requirement to subscribe to more than one code, for example where licensed entities conduct activities in multiple subsectors.

It is the Taskforce’s view that ASIC should have some flexibility in the timing for implementation of any such requirement. This position enables the regulator to ensure that firms are signatories to their appropriate codes, without an unnecessary increase in compliance costs. There are key subsectors where gaps in coverage or ambiguities around enforcement of codes have been identified. The Taskforce considers that these subsectors should be prioritised in the application of the proposed requirement.

Recommendation 20

Approved codes should be binding on and enforceable against subscribers by contractual arrangements with a code monitoring body.

In addition to codes becoming binding and enforceable against subscribers, the Taskforce recommends that where ASIC considers it appropriate there could also be a requirement that the provisions of the code be incorporated into agreements with the customers. Some industry codes already have this requirement, such as the Banking Code. Ultimately this will be a matter for ASIC in setting out the standards of enforceability it requires before it will approve the relevant code, and it will need to take account of the practicality of making code provisions contractually enforceable in any given sector.

Codes should expressly provide that a subscriber's failure to comply with the code is to be taken into account in resolving disputes with individual customers through the subscriber's IDR and by AFCA, on the basis that compliance with the code by subscribers is expected rather than optional or aspirational.

Code compliance

Recommendation 21

An individual customer should be able to seek appropriate redress through the subscriber's internal and external dispute resolution arrangements for non-compliance with an applicable approved code.

The Taskforce recommends that in the event of non-compliance with an approved code, an individual customer would be entitled to seek appropriate redress through the participant's internal and external dispute resolution arrangements.

External dispute resolutions are a key mechanism of code compliance. For example, at present consumers can bring complaints to the Financial Ombudsman Service (FOS) where they are not satisfied with the outcome after complaining to the relevant provider. Additionally, code compliance committees may also refer disputes to the FOS in certain circumstances. This is likely to continue to be the case under AFCA.

Recommendation 22

The code monitoring body, comprising a mix of industry, consumer and expert members, should be required to monitor the adequacy of the code and industry compliance with it over time, and periodically report to ASIC on these matters.

The Taskforce recommends that the code monitoring body be responsible for monitoring the adequacy of the code as well as industry compliance with it. Each subscriber would be required to monitor its ongoing compliance with the code and report periodically to the code body. The ability to monitor compliance is a key component of an effective industry code.

Should the code body consider there to be evidence of systematic non-compliance, the code body could require the subscriber to take steps to improve its compliance practices. The code body could also itself escalate concerns to ASIC for further investigation, for example where a subscriber is non-compliant with the requirements of section 912A of the Corporations Act.

The code monitoring body, consisting of an appropriate mix of industry representatives, consumer representatives and independent experts should also keep the code content under review on an ongoing basis and adapt it to changing market conditions.



Chapter 5 – Strengthening ASIC’s licencing powers

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 5: Strengthening ASIC's licencing powers</i>	
Number	Description
23	ASIC should be able to refuse a licence application (or, for existing licensees, take licensing action) if it is not satisfied controllers are fit and proper
24	Empower ASIC with the ability to cancel a licence if the licensee fails to commence business within six months
25	ASIC should be able to refuse a licence application if it is false or misleading in a material particular.
26	Introduce an express obligation requiring applicants to confirm that there have been no material changes to information given in the application before the licence is granted
27	Align the assessment requirements for AFS licence applications with the enhanced credit licence assessment requirements
28	A statutory obligation should be introduced to notify change of control within 30 days of control passing, with penalties for failure to notify
29	Align consequences for making false or misleading statements in documents provided to ASIC in AFS and credit contexts

5. Strengthening ASIC's licencing powers

Overview

Part 7.6 of the Corporations Act governs licensing of financial services providers. A person who carries on a financial services business in Australia must hold an AFS licence, subject to certain exemptions.³² Those exemptions include where a person provides a financial service as representative of an AFS licensee whose licence covers the provision of the service.³³

Applications for AFS licences are made to, assessed by and granted by ASIC. ASIC must grant an application for an AFS licence if the applicant and application meet the requirements of section 913B of the Corporations Act. Section 913B of the Act also provides that ASIC must not grant such a licence unless those requirements are met. ASIC may refuse to grant an application for an AFS licence after offering the applicant an opportunity to appear or be represented at a private hearing and make submissions.³⁴

ASIC is required under section 913B of the Corporations Act to consider a range of factors when deciding whether to grant a licence, including making an assessment of the applicant's competence and confirming that there is no reason to believe the applicant is likely to contravene its licence obligations and financial services laws.

To grant an application for an AFS licence, ASIC must be satisfied, among other things, that there is no reason to believe that:

- If the applicant is an individual, the applicant is not of good fame or character; or
- If the applicant is a body corporate, any of the applicant's responsible officers (meaning an officer who would perform duties in connection with the holding of the licence) are not of good fame or character; or
- If the applicant is a partnership or the trustees of a trust, any of the partners or trustees who would perform duties in connection with the holding of the licence are not of good fame or character.

ASIC may suspend or cancel a licence if it is no longer satisfied of these matters.

ASIC is also responsible for granting credit licences. The Credit Act governs the licensing of persons who engage in credit activities. A person must not engage in a credit activity unless the person holds an Australian credit licence, or engages in the activity as a credit representative or as an employee or director of a credit licensee or related body corporate.³⁵ To grant an application for a credit licence, ASIC must, amongst other things, have no reason to believe that the applicant is not a fit and proper person to engage in credit activities. For that purpose, ASIC must consider a number of matters, including:

- Whether a banning order has ever been made against the applicant under the Credit Act or the Corporations Act;
- If the applicant is a body corporate, whether ASIC has reason to believe that any of the directors, secretaries or senior managers of the body corporate who would perform duties in relation to the credit activities to be authorised by the licence is not a fit and proper person to engage in credit activities;

³² Corporations Act s. 911A

³³ Corporations Act s.911A(2)(a)

³⁴ Corporations Act s.913B(5)

³⁵ Credit Act s.29

- If the applicant is a partnership or the trustees of a trust, whether ASIC has reason to believe that any of the partners or trustees who would perform duties in relation to the credit activities to be authorised by the licence is not a fit and proper person to engage in credit activities.

ASIC may also suspend or cancel a licence if ASIC has reason to believe that the licensee is not a fit and proper person to engage in credit activities.

Current licencing powers

ASIC has, over a number of years, made submissions seeking to strengthen its licensing powers. A number of AFS licensing reforms were most recently implemented in the *Corporations Amendment (Future of Financial Advice) Act 2012*. Subsequently, ASIC made further submissions about other licencing related reforms to the FSI, including providing greater clarity and discretion to refuse a licence and requiring reassessment of a licence on any change in control.

The FSI final report acknowledged ASIC’s submissions and recommended that ASIC be provided with stronger regulatory tools.³⁶ The Government’s response stated that it would develop legislative amendments to strengthen ASIC’s enforcement tools in relation to the financial services and credit licencing regimes. These included enabling ASIC to:

- Approve changes of licensee control;
- Consider a broader range of factors in determining whether an applicant satisfies the “fit and proper” test to be granted a licence; and
- Impose conditions on firms to address concerns about internal systems relating to serious or systemic conduct (including external reviews).³⁷

Granting licences

There is no express requirement for ASIC to assess whether a controller is of good fame or character, or is fit and proper to be a controller of an applicant seeking a licence.³⁸ When assessing a licence application, at present ASIC must consider and be satisfied that:

- The responsible officers (directors or secretaries who perform duties in connection with holding the licence) of AFS licence applicants are of good fame and character; and
- The directors, secretaries and senior managers of credit licence applicants are fit and proper to engage in credit activities.³⁹

As a result there is no obligation for an applicant to make specific disclosure about the past history, conduct or character of controllers and ASIC receives no up-front information about these matters. ASIC does, however, require new applicants to identify any controller on application forms. ASIC then undertakes database searches to ascertain any prior conduct known to ASIC about individuals. If so, this conduct is taken into account in determining whether ASIC believes the applicant will be able to comply with its obligations as a licensee.

Section 915B(1)(a) of the Corporations Act enables ASIC to immediately suspend or cancel an AFS licence where a licensee ceases to carry on a financial services business. ASIC can also immediately

³⁶ Recommendation 29, Final Report of the Financial System Inquiry, December 2014.

³⁷ Improving Australia’s financial system – Government response to the Financial System Inquiry, October 2015. P.24

³⁸ Control of a licensee is defined in Corporations Regulation 7.6.04(2)(b) and the National Consumer Credit Protection Regulation 9(11).

³⁹ Corporations Act s.913A(3) and definition of a responsible officer in s.9, and Credit Act s.37(2)(h)

suspend or cancel a licence where a credit licensee has not commenced, or has ceased to carry on a credit business under section 54(1)(b) of the Credit Act. The lack of a power to suspend or cancel an AFS licence if a licensee fails to commence carrying on the business of providing financial services provides entities with an opportunity to ‘warehouse’ a licence. This can have the effect of commoditising the licence by making it attractive for holders to obtain and subsequently sell the licensee. This also impacts ASIC’s resources, which are expended to assess an application for which there may be no present intention to commence operations. While the Credit Act enables ASIC to immediately suspend or cancel a credit licence if the licensee does not commence operations (as well as if it has ceased carrying on the business), there is a lack of certainty as to when a licensee should have commenced business. Greater certainty would benefit licensees and ASIC.

Recommendation 23

ASIC should be able to refuse a licence application (or, for existing licensees, take licencing action) if it is not satisfied controllers are fit and proper.

The Taskforce recommends that ASIC should be able to refuse a licence application if it is not satisfied that the controllers of the applicant are fit and proper and to take licensing action if it is no longer satisfied of this, including on a change of control. To achieve this, it will be necessary to:

- Enable ASIC to refuse to grant a licence (after offering a hearing) if it is not satisfied that the controllers of the applicant are fit and proper to control an AFS or credit licensee⁴⁰;
- Following a change in control, require licensees to provide ASIC with information to enable ASIC to assess whether the new controllers are fit and proper to control the licensee and confirm that the licensee continues to be competent to provide the relevant services and comply with its licence obligations; and
- Enable ASIC to suspend or cancel a licence (after offering a hearing) if it is no longer satisfied that the controllers of a licensee are fit and proper to control an AFS or credit licensee.

The Taskforce considers that ASIC should be able to refuse to grant a licence after offering a hearing if it is not satisfied that the controllers of the applicant are fit and proper to control an AFS or credit licensee. The legislation should:

- Expressly require ASIC to assess whether the controllers of a licence applicant are fit and proper persons to control an AFS or credit licensee; and
- Enable ASIC to refuse to grant the licence applied for if it is not satisfied of the fitness and propriety of the applicant’s controllers.⁴¹

The Taskforce considers that the requirement for ASIC to assess the fitness and propriety of controllers should not require the applicant to establish that its controllers are fit and proper. Rather, the assessment that applies to responsible officers (for AFS licence applicants) and directors and senior managers (for credit licence applicants) should apply to controllers. That is, before granting a licence ASIC would have to assess and have no reason to believe that a controller is not a fit and proper person to control a licensee. The licence applicant would need to provide ASIC with sufficient information about its controllers, including relating to their prior conduct, to enable ASIC to properly make this assessment. The concept of who is a controller goes beyond merely the holding company of the licensee as the definition of control includes consideration of the practical

⁴⁰ In accordance with Recommendation 6 the applicable test for AFS licence applications will be whether the relevant person is ‘fit and proper’ as applies in credit licence applications rather than the current test ‘of good fame and character.’

⁴¹ Corporations Act s. 913B(1) and (5)

influence a person can exert and any practice or behaviour affecting the licensee's operating policies.

Therefore, in assessing controllers, ASIC would assess the suitability of the individual or groups of individuals acting together who actually exercise control of a licensee. After offering a hearing, ASIC could refuse to grant the licence applied for if it was not satisfied that the controllers of the applicant were fit and proper to control a licensee.⁴² The legislation should expressly state that the assessment of whether controllers, responsible managers, directors or senior managers are fit and proper to hold that role within a licensee will consider, among other things, whether those individuals have previously held such a role in a licensee that has not complied with a determination of an approved external dispute resolution body.

The majority of stakeholder responses on this matter supported the proposal at hand, assessing that it would not result in an exorbitant increase in the regulatory burden on licensees. Several respondents commented that the definition of 'fit and proper' needs to be unambiguous and clearly outlined by ASIC in relation to the proposed change.

Recommendation 24

Empower ASIC with the ability to cancel a licence if the licensee fails to commence business within six months.

The Taskforce recommends that ASIC should be able to immediately cancel an AFS licence and credit licence if the licensee:

- has not commenced to engage in a financial services or credit business within six months of being granted a licence to do so; or
- has ceased to carry on a financial services or credit business.

Licensees should be given the ability to seek an extension of time from ASIC where a licensee is unable to commence its business within the six month timeframe. The extension should be sought before the expiry of the initial six month period. This will address both the issue of 'warehousing' AFS licences and provide certainty for AFS and credit licensees as to when ASIC's power to cancel a licence for failure to commence engaging in business will arise.

Recommendation 25

ASIC should be able to refuse a licence application if it is false or misleading in a material particular.

The Taskforce recommends that there should be a specific ground for ASIC to refuse an AFS or credit licence application if it is false or misleading in a material particular. This may occur as a result of a false or misleading statement made or omission of information from the application. Currently, there is no express power to refuse a licence application in these circumstances. At present ASIC must rely on the general test, under which the false or misleading statement may provide a basis for ASIC to have reason to believe that the applicant is likely to contravene its licence obligations.⁴³ Licence applicants may seek to argue that the relevant conduct was inadvertent, not serious or that the circumstances leading to the making of the statement have been remediated and therefore the conduct does not impact on the applicant's ability to comply with its licence obligations.

Once ASIC is satisfied that the information or document is false or misleading in a material particular it may refuse to grant the licence, after offering the applicant the opportunity to attend a hearing

⁴² Corporations Act s. 913B(1) and (5)

⁴³ Corporations Act s.913B(1)(b)

and make submissions. Stakeholder responses to this proposal were supportive of allowing ASIC the ability to refuse licenses based on materially false or misleading statements in applications.

Recommendation 26

Introduce an express obligation requiring applicants to confirm that there have been no material changes to information given in the application before the licence is granted.

The Taskforce recommends that applicants seeking an AFS or credit licence or to vary an existing licence should have an express obligation to confirm, before the licence or variation is granted, that there have been no material changes in the applicant’s circumstances that would render statements or information in the application to be false or materially misleading. This should include express requirements to specify that there have been no changes to the way the applicant will meet its financial requirements, and the applicant’s eligibility and expectation of obtaining professional indemnity insurance. The confirmation could be provided at the end of the assessment period after the applicant has been provided with a draft of the licence that ASIC proposes to grant. The granting of the licence would be subject to provision of the applicant’s confirmation as to the currency and accuracy of the information in the application (and any other matters required by ASIC in the relevant circumstances).

This will ensure that ASIC’s decision to grant a licence or licence variation is based on up to date information about the circumstances of the applicant, particularly with respect to the arrangements on which the applicant relies to satisfy ASIC that it can comply with its obligations as a licensee.

Recommendation 27

Align the assessment requirements for AFS licence applications with the enhanced credit licence assessment requirements.

The Taskforce recommends that the assessment requirements for AFS and credit licence applications should be as similar as possible. The Taskforce considers that there are no policy reasons for treating them differently and that licence applicants in similar circumstances should be subject to the same assessment criteria and requirements. To the extent practicable, the requirements should be universal for both types of licence applicants.

To achieve this, the AFS licence assessment criteria in the Corporations Act should be updated and made consistent with the equivalent and enhanced provisions adopted in the Credit Act in 2010. This will require amendments to the Corporations Act as follows:

	Corporations Act – AFS licence applications	Credit Act – Credit licence applications	Proposed amendments to s913B of the Corporations Act
1.	ASIC looks at the: <ul style="list-style-type: none"> • natural person applicant; • responsible officers of a body corporate applicant; • natural person partners of partnership applicants; and • natural person trustees of trust applicants.⁴⁴ 	ASIC looks at the: <ul style="list-style-type: none"> • natural person applicant; • directors, secretaries and senior managers of a body corporate applicant; • natural person partners of partnership applicants; and • natural person trustees of trust applicants.⁴⁵ 	Amend subsection 913B(3)(a)(i) from “responsible officer” to “director or secretary and senior manager” of body corporate applicants.

⁴⁴ Corporations Act ss.913B(2) and (3).

2.	ASIC has regard to whether the above persons are of “good fame or character”. ⁴⁶	ASIC has regard to whether the above persons are “fit and proper” to engage in credit activities. ⁴⁷	Change the test of “good fame or character” to the “fit and proper” test.
If Recommendation 1 is adopted the above will be extended to ‘controllers’ for AFS and credit licence applications.			
3.	Where ASIC has reason to believe that individuals associated with the AFS licence applicant are not of good fame and character it must also consider whether the applicant’s ability to provide financial services will nevertheless not be significantly impaired. ⁴⁸	No requirement to consider whether the applicant’s ability to engage in credit activities would nevertheless not be significantly impaired after forming a reasonable belief that individuals are not fit and proper to engage in credit activities.	Remove the requirement to consider whether an AFS licence applicant’s ability to provide financial services would nevertheless not be significantly impaired after forming a reasonable belief that individuals are not of good fame and character (or fit and proper if the test is amended).
4.	ASIC has no express power to request an audit report. There is a ‘catch-all’ power to request any additional information in relation to matters that can be taken into account in deciding whether to grant the licence. ⁴⁹	ASIC can expressly request an audit report as well as any additional information in relation to any matters that ASIC may have regard to in deciding whether to grant the licence. ⁵⁰	Include an express power for ASIC to require an audit report as well as any additional information in relation to any matters that ASIC may have regard to in deciding whether to grant the licence.
5.	No deemed withdrawal mechanism for failure to comply with ASIC’s request for additional information.	Deemed withdrawal where the applicant does not lodge the additional information requested by ASIC, including an audit report. ⁵¹	Include a deemed withdrawal where there is a failure to provide additional information requested by ASIC.

As stated above, the legislation should expressly state that the fit and proper assessment will consider, among other things, whether individuals have previously held a role in a licensee that has not complied with a determination of an approved external dispute resolution scheme body, and the role in the business the person proposes to take, particularly if they will not perform duties in connection with holding the licence.

Control obligations

The Taskforce considers that following a change in control, licensees should provide ASIC with information to enable ASIC to assess whether the new controllers are fit and proper to control the licensee and the licensee continues to be competent to provide the relevant services and comply with its licence obligations.

At present, licensees are required by a statutory licence condition to notify ASIC within 10 business days of the licensee becoming aware of a change in control.⁵² However, this is the only express obligation relating to controllers of a licensee. When complying with the notification obligation licensees are not required to provide information about the prior history or conduct of the new controllers or the implications for the ongoing conduct of the licensee’s business.

⁴⁵ Credit Act ss.37(1)(g) and (h).

⁴⁶ Corporations Act ss.913B(2) and (3).

⁴⁷ Credit Act s.37(1)(c).

⁴⁸ Corporations Act ss.913B(3)(a) and (b).

⁴⁹ Corporations Act s.913B(1)(ca).

⁵⁰ Credit Act s.37(4).

⁵¹ Credit Act s.38(5).

⁵² Corporations Regulation 7.6.04(1)(i) and the National Consumer Credit Protection Regulation 9(10).

The Government's response to the final report of the *Financial Services Inquiry* stated that it would develop legislative amendments to strengthen ASIC's enforcement tools in relation to the financial services and credit licensing regimes, including enabling it to "approve changes of licensee control."

While there is potential for significant changes to occur within a licensee upon a change of control that may affect the operations, policies, procedures and competency of the licensee, licensees continue to be subject to the general obligations imposed on AFS licensees by section 912A of the Corporations Act and credit licensees by section 47 of the Credit Act. The general understanding is that the majority of licensees will ensure that they continue to do this.

Case study

In a recent surveillance of 55 licensees in the Australian retail over-the-counter derivatives industry, ASIC found that over 60% had gone through some material change of control but 85% of those had failed to notify ASIC. Many of these licensees were smaller foreign-owned or foreign-controlled businesses which demonstrated either a lack of awareness or understanding of their Australian regulatory obligations, or reluctance to invest resources in meeting compliance obligations for the Australian businesses. It also became evident in that surveillance that many of these AFS licensees were outsourcing key aspects of their financial service to third parties. Often these third parties were based overseas, and subject to little or no regulatory oversight in the jurisdiction in which they operated.

Recommendation 28

A statutory obligation should be introduced to notify change of control within 30 days of control passing, with penalties for failure to notify.

The Taskforce recommends that a statutory obligation requiring licensees to notify ASIC of changes of control within 30 business days of the change of control taking effect as well as penalties for failure to notify should be introduced. This would replace the existing statutory licence condition that requires notification within 10 business days of the licensee becoming aware of the change. Given the impact that a change of licensee control can have it is important that ASIC is provided with timely notifications about changes of controllers of licensees. The 30 day time frame is consistent with the required timeframe for notifying ASIC of new or ceasing financial advisers or representatives.

Requiring notification to ASIC within 30 business days of the change of control taking effect will provide certainty as to when the 30 day timeframe commences. In addition, licensees will be required to have in place systems and procedures to ensure that they can comply with the notification requirement within the 30 day timeframe.

Imposing penalties will deter deliberate non-compliance with the notification obligation and enable ASIC to take specific action to respond to a failure to notify. Following receipt of submissions the Taskforce considers that a failure to notify of a change of control within the required time frame should be a strict liability offence with penalty notice consequences (consistent with Recommendation 39). ASIC should also retain the ability to take licensing action for a breach of the obligation to notify of a change in control where the circumstances warrant such action.

Recommendation 29

Align consequences for making false or misleading statements in documents provided to ASIC in AFS and credit contexts.

Relevant matters

The Taskforce recommends that the consequences for making false or misleading statements in documents provided to ASIC in the AFS and credit contexts should be the same. This should apply with respect to statements made in licence applications, licence variation applications and any other document lodged with ASIC. The AFS and credit licensing regimes impose similar standards of conduct on those wishing to offer licensed services and similar consequences for breaching those obligations. The process for applying for an AFS and credit licence are also similar.

This will require amendments to the Corporations Act so that there is no specific provision that applies with respect to false or misleading statements made in AFS licence applications and/or to ensure that:

- Recklessness as to whether a statement is false or misleading or contains a material omission is prohibited;
- A person making a statement or authorising the making of a statement is required to take reasonable steps to ensure that a document submitted to ASIC does not contain a false or misleading statement or a material omission which renders a document materially misleading;
- Authorising a statement in an AFS licence application that is false or misleading or contains a material omission is prohibited.

In addition, the Taskforce considers that the penalties for misleading ASIC in AFS licence applications should be consistent with the penalties that apply for misleading ASIC in any other circumstance and are aligned with those that currently apply with respect to false or misleading statements in the Credit Act. To achieve this, it will be necessary to increase the applicable criminal penalty and introduce similar civil penalty consequences to those that apply in section 225 of the Credit Act.



Chapter 6 – ASIC’s power to ban senior individuals in the financial sector

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 6: ASIC's power to ban individuals in the financial sector</i>	
Number	Description
30	Once an administrative banning power is triggered, ASIC should be able to ban a person from performing a specific function, or any function, in a financial services or credit business.
31	The grounds for exercising ASIC's power to ban individuals from performing roles in financial services and credit businesses should be expanded.

6. ASIC's power to ban individuals in the financial sector

Overview

Public confidence in the integrity of individuals who work in the financial sector is essential. This is particularly so for individuals who occupy senior positions within financial institutions. To foster this confidence, it is important that financial sector regulators have appropriate powers to remove individuals who have acted contrary to the public interest and prevent their continued involvement in the sector.

Both the FSI and the earlier Senate report on the *Performance of the Australian Securities Investments Commission* recognised shortcomings in ASIC's existing banning powers. The FSI noted that:

*Currently, ASIC can prevent a person from providing financial services, but cannot prevent them from managing a financial firm. Nor can ASIC remove individuals involved in managing a firm that may have a culture of non-compliance.*⁵³

As identified by the FSI there are two key problems with ASIC's powers at present. The first relates to the scope of banning orders. ASIC's powers are limited to banning a person from providing financial services or engaging in credit activities.

In the financial services context, the effect of a banning order is that a person is prohibited from providing financial services. However, this does not prevent a person from having another role in a business that provides financial services, for example as a director, officer, compliance manager or owner, unless they are providing the services themselves.

This means that a person can be banned from providing financial services, but still hold a senior position or management role in a financial services business. In that capacity they may be responsible for the provision of financial services by others in the business and for the policies and procedures of the business. In some circumstances, the person's ongoing responsibility for the provision of financial services may pose a risk to consumers given their previous conduct. The same issues arise with respect to the scope of banning orders that prevent a person from engaging in credit activities.

The Taskforce considers that this issue can be addressed by expanding the scope of banning orders, so that ASIC can ban a person from:

- Performing a specific function in a financial services or credit business, including being a senior manager, or a controller of a financial services or credit business; and/or
- Performing any function in a financial services or credit business.

The second problem identified relates to the threshold currently in place for ASIC to make a banning order. ASIC is empowered to make a banning order in a range of circumstances involving poor conduct in the provision of financial services or engaging in credit activities. However, the existing provisions do not necessarily cover a director or senior manager of a financial services or credit business who is demonstrated to be unfit to fulfil their role.

⁵³ *Financial System Inquiry, Final Report, p.218*

Current status of ASIC's banning powers

ASIC's existing banning powers are governed by two regimes: the Corporations Act and the Credit Act. Relevantly, under the Corporations Act, ASIC may ban a person from providing financial services if:

- The person has not complied with the general obligations imposed on financial services licensees under section 912A;
- ASIC has reason to believe that the person is likely to contravene these obligations;
- ASIC has reason to believe that the person is not of good fame or character;
- ASIC has reason to believe that the person is not adequately trained, or is not competent to provide a financial service or financial services;
- The person has not complied with a financial services law⁵⁴;
- ASIC has reason to believe that the person is likely to contravene financial services law;
- The person has been involved in the contravention of a financial services law by another person; or
- ASIC has reason to believe that the person is likely to become involved in the contravention of a financial services law by another person.⁵⁵

A banning order may prohibit a person from providing any financial services or specified financial services in specified circumstances or capacities, permanently or for a specified period of time.⁵⁶

ASIC may only make a banning order against a person after giving the person an opportunity to appear, or be represented, at a hearing before ASIC, and to make submissions to ASIC on the matter.⁵⁷ Application may be made to the Administrative Appeals Tribunal (AAT) for a review of a decision by ASIC to ban a person from providing financial services.

A person who engages in conduct that breaches a banning order is guilty of an offence, the maximum penalty for which is a fine of 25 penalty units (currently \$5,250) or six months' imprisonment, or both⁵⁸.

ASIC provides detailed guidance on the exercise of its power to ban a person from providing financial services in *Regulatory Guide 98: Licensing: Administrative action against financial services providers* (RG98).

Under the Credit Act, ASIC may make a banning order against a person in certain circumstances that include where:

- The person has contravened any credit legislation, or been involved in the contravention of a provision of any credit legislation by another person;
- ASIC has reason to believe that the person is likely to contravene any credit legislation or be involved in the contravention of a provision of any credit legislation by another person;
- ASIC has reason to believe that the person is not a fit and proper person to engage in credit activities.⁵⁹

⁵⁴ Defined in section 761A of the Corporations Act.

⁵⁵ Corporations Act section 920A(1)(b), (ba), (d), (da), (e), (f), (g) and (h) of the Corporations Act. The circumstances also include where ASIC suspends or cancels an AFS license held by the person, or the person becomes an insolvent under administration or is convicted of fraud.

⁵⁶ Corporations Act section 920A(1) and 920B. If ASIC has reason to believe that the person is not of good fame or character, ASIC may only make a permanent banning order: section 920B(2).

⁵⁷ Corporations Act section 920A(2). This requirement does not apply insofar as ASIC's grounds for making the order include that the person's AFS licence was suspended or cancelled under section 915B – which does not require a hearing – or that the person has been convicted of serious fraud.

⁵⁸ The Taskforce is recommending an increase to this penalty as part of its review of criminal penalties.

The banning order may prohibit a person from engaging in any credit activities or specified credit activities in particular circumstances or capacities permanently or for a specified period.⁶⁰ Provisions similar to those under the Corporations Act apply, including representation at a private hearing before ASIC.

A person who engages in conduct that breaches a banning order may be liable to a maximum civil penalty of 2,000 penalty units (currently \$420,000), or guilty of a criminal offence with a maximum fine of 100 penalty units (currently \$21,000) or two years' imprisonment, or both.⁶¹

ASIC provides detailed guidance on the exercise of its power to ban a person from engaging in credit activities in *Regulatory Guide 218: Licensing: Administrative action against persons engaging in credit activities* (RG218).

Expanding the scope of banning powers

Currently, a person who is banned from providing financial services can own, hold a senior position within, and be involved in the management of a financial services business despite the banning. As discussed above, this may not always be appropriate. For example, where the banned person supervises others who are providing financial services and/or the banned person is responsible for policies and procedures relating to the licensee's provision of financial services.

Recommendation 30

Once an administrative banning power is triggered, ASIC should be able to ban a person from performing a specific function, or any function, in a financial services or credit business.

The Taskforce recommends that ASIC should have the power to ban a person from:

- Performing a specific function in a financial services or credit business, including managing a financial services or credit business. This would also cover the existing ability to ban from providing financial services or engaging in credit activity; and
- Performing any function in a financial services or credit business.

There was unanimous support in stakeholder submissions for expanding the scope of ASIC's banning powers and applying this to individuals who perform roles in credit businesses in addition to financial services businesses.

This new power to ban a person from engaging in specific functions or any function would only be triggered when the power to make a banning order under section 920A of the Corporations Act or s80 of the Credit Act is activated. This type of approach has been adopted in a number of international jurisdictions. The Monetary Authority of Singapore has powers enabling it to prohibit a person from taking part, directly or indirectly, in the management of, acting as a director of or becoming a substantial shareholder in the holder of a capital markets licence. Similar powers are exercised by the Ontario Securities Commission in Canada.

The advantage of this approach is that the banning order can specify functions from 'control of a licensee' to 'management' of a financial services or credit business based on the circumstances that

⁵⁹ Credit Act section 80(1)(d), (e) and (f). The circumstances also include where ASIC suspends or cancels a credit licence held by the person, or the person becomes insolvent (otherwise than as the trustee of a trust) or is convicted of fraud.

⁶⁰ Credit Act sections 80(1) and 81.

⁶¹ The Taskforce is recommending increases to these penalties as part of its review of criminal penalties and its review of civil penalties.

activated the power to make the banning order. It also means that other kinds of management roles (such as compliance officers) can be captured.

To allow flexibility for ASIC, the Taskforce recommends that the power to ban should be cast so that ASIC can ban a person from fulfilling specified positions, such as senior manager or manager, or in justifiable cases, to ban a person from any involvement in a financial services business.

Concerns were raised during the public consultation that banning should only apply to influential roles, with mixed views on whether individuals should be banned from risk, compliance and audit roles. Recognising that the discretion to make a banning order must be exercised for protective purposes the Taskforce considers the banning power should cover roles all levels of a business as potential harm to consumers can occur at any level. Further, risk, compliance and audit roles serve an important secondary protective function in financial services and credit businesses. ASIC should have discretion to exclude a banned person from taking these positions. At the same time, the Taskforce recognises the importance of procedural fairness in administrative decision making and that the legislation provide appropriate measures as well as the right of a banned person to seek a review of ASIC's decision in the AAT. Based on these considerations, the Taskforce has retained its original position.

Revising the banning threshold

At present, ASIC does not have an express power to administratively ban senior office holders and managers in circumstances where they did not provide financial services (and were not involved in contraventions of relevant financial services laws) but were managing or overseeing the conduct of a financial services business that exhibits systemic non-compliance with financial services laws or other regulatory requirements. This issue also applies to both the financial services licensing and credit licensing regimes.

Recommendation 31

The grounds for exercising ASIC's power to ban individuals from performing roles in financial services and credit businesses should be expanded.

The Taskforce recommends that the banning power be enlivened where ASIC has reason to believe that the person is not:

- Fit and proper to provide a financial service or financial services, or to perform the role of officer or senior manager in a financial services business⁶²; and/or
- Adequately trained, or is not competent, to provide a financial service or financial services, or to perform the role of officer or senior manager in a financial services business.

In the credit context, the existing powers to ban where ASIC has reason to believe that a person is not fit and proper, adequately trained or competent would be extended to those who perform the role of officer or senior manager in a credit business.

The grounds for ASIC's power to ban should also include circumstances where a person has more than once been an officer, partner or trustee of a financial services or credit licensee that was:

- The subject of a report by AFCA regarding a failure to comply with a determination of that authority⁶³; or

⁶² The Taskforce recommends that this test replace the 'good fame or character' test in section 920A.

- A corporation where in the course of being wound up a liquidator lodged a report under subsection 533(1) of the Corporations Act about the corporation's inability to pay its debts (phoenixing-related activity).

The scope of the expanded banning powers (in so far as they relate to senior roles) would be limited by the current definitions of 'officer' and 'senior manager' in the Corporations Act.⁶⁴ Retaining the existing definitions of 'officer' and 'senior manager' was largely supported by stakeholder submissions.

These definitions include persons who occupy specified roles (such as directors and secretaries) and who perform particular functions within a corporation, including persons who:

- Make, or participate in making, decisions that affect the whole, or a substantial part, of the business of the institution;
- Have the capacity to affect significantly the institution's financial standing; or
- Are shadow officers – in accordance with whose instructions the officers are accustomed to act.

Introducing grounds, as detailed above, for banning based on reports of non-compliance with determinations of AFCA would reflect the importance of complying with determinations of the new authority. The Taskforce recommends that phoenixing-related activity be included as a basis for banning, and that this be cast in similar terms to the disqualification of a person from managing corporations currently in section 206F of the Corporations Act. As per this disqualification power, the period of banning would be capped at a maximum five-year period. This was considered by stakeholders to be appropriate and proportionate when banning a person on this basis. The five-year cap should only apply to the phoenixing grounds for banning. Where ASIC's banning power is enlivened on the basis of multiple grounds, including the phoenixing grounds, the 5 year cap will not prevent a longer period of banning being imposed on the basis of concerns relating to the other grounds. Almost all responses to the public consultation agreed that phoenixing activities were appropriate grounds for enlivening the banning power.

The Taskforce also considered and sought submissions on whether grounds for administrative banning by ASIC should be expanded to include where a person has breached their duty under sections 180, 181, 182 or 183 of the Corporations Act. This would align the consequences for breaching these duties with those imposed on officers and employees of responsible entities of managed investment schemes in Chapter 5C of the Corporations Act, which form part of financial services laws and therefore can trigger the banning order power.⁶⁵ Stakeholder views on this proposal were mixed, with most considering it unnecessary or believing that it raised procedural fairness issues.

Ultimately, the Taskforce decided that expansion of the banning power to ban from performing particular roles in financial services companies, as well as giving ASIC power to ban where a person is not fit and proper, or adequately trained and competent, would give ASIC the flexibility needed to deal with most cases. At the same time, in appropriate cases ASIC may still apply to the court seeking orders to disqualify a manager of a financial services business from managing corporations and restrain them from carrying on a financial services business. Given these considerations, the Taskforce chose not to proceed with the proposal that breaching sections 180, 181, 182 or 183 of the Corporations Act be grounds for administrative banning by ASIC, rather than a court.

⁶³ The Final Report of the Review of the financial system external dispute resolution and complaints framework contemplates that the Australian Financial Complaints Authority will be required to make reports of non-compliance.

⁶⁴ Section 9, *Corporations Act 2001* (Cth)

⁶⁵ Section 601FD, *Corporations Act 2001* (Cth)

As previously discussed, these additional grounds, as with other grounds in section 920A of the Corporations Act, would be subject to procedural fairness and administrative review. Individuals will have the opportunity to be heard before ASIC makes a banning order and ASIC's decision is subject to merits review.

The Taskforce considers that these recommendations will enhance the financial services and credit regimes and address the shortcomings that have been raised. In its submission ASIC argued that new duties or expectations should be created in a manner similar to those detailed in the Banking Executive Accountability Regime (BEAR) reforms.⁶⁶ ASIC suggested that:

- There should be new obligations requiring individuals in financial services and credit businesses to take reasonable steps within their role as a manager to achieve compliance in the activities they manage with potential banning for serious failures to meet that duty; and
- A requirement that very large entities map key responsibilities.

In addition, a number of consumer organisations submitted in response to the BEAR consultation paper⁶⁷ that there was a need for improvements to the accountability regime that better links executive remuneration and any penalties to widespread consumer harm. These organisations noted that it is proposed that the BEAR will apply to ADIs and conduct of a systemic or prudential nature. It will not apply to non-ADI businesses, including insurers, or necessarily to conduct matters (non-prudential) where consumer or shareholder interests may be at risk.⁶⁸

Taking these issues into account the Taskforce maintains its view that it is not necessary to impose new duties or expectations of a kind proposed by the BEAR across the financial sector. It considers that ASIC's banning powers will be adequately enhanced through the recommendations in this chapter. This is consistent with the Taskforce's view that new powers should be introduced only where there is a demonstrated need for them.

⁶⁶ These reforms are aimed at enhancing the responsibility and accountability of Authorised Deposit-taking Institutions and their directors and senior executives. The BEAR (among other things) proposes to enable the Australian Prudential Regulation Authority to administratively disqualify a person from being a senior manager, director or auditor where they have not met new expectations created by the BEAR.

⁶⁷ The BEAR Consultation Paper was released in July 2017. In September 2017 stakeholder views were sought on the exposure draft of the Treasury Laws Amendment (Banking Executive Accountability and Related Measures) Bill 2017 (see <https://treasury.gov.au/consultation/c2017-t222462/>).

⁶⁸ The equivalent regime in the United Kingdom will be extended to cover insurers and non-prudentially regulated firms and gives powers to the Prudential Regulation Authority and the Financial Conduct Authority. These differences were also recognised by the Senate Inquiry into the BEAR Bill.



Chapter 7 – Strengthening penalties for corporate and financial sector misconduct

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 7: Strengthening penalties for corporate and financial sector misconduct</i>	
Number	Description
32	The maximum imprisonment penalties for criminal offences in ASIC-administered legislation should be increased as outlined in Table A
33	The maximum pecuniary penalties for criminal offences in the Corporations Act should generally be calculated by reference to the following formula: maximum term of imprisonment in months multiplied by 10 = penalty units for individuals, multiplied by a further 10 for corporations
34	The maximum penalty for a breach of section 184 should be increased to reflect the seriousness of the offence, to 10 years' imprisonment and/or a fine: for individuals the greater of 4,500 penalty units of three times the benefit gained (or loss avoided); and for corporations the greater of 45,000 penalty units, or three times the benefit gained (or loss avoided) or 10% annual turnover.
35	The Peters test should apply to all dishonesty offences under the Corporations Act
36	Imprisonment should be removed as a possible sanction for strict and absolute liability offences
37	An ordinary offence should be introduced to complement a number of strict and absolute liability offences as outlined in Table B
38	Maximum pecuniary penalties for strict and absolute liability offences currently set at 5, 10 or 15 penalty units should be increased to 20 penalty units for individuals, corresponding penalties for corporations should be increased to 200 penalty units
39	All strict and absolute liability offences should be subject to the penalty notice regime
40	Maximum civil penalty amounts in ASIC-administered legislation should be increased as follows: – For individuals: 2,500 penalty units (currently \$525,000); – For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (\$210 million)).
41	Disgorgement remedies should be available in civil penalty proceedings brought by ASIC under the Corporations, Credit and ASIC Acts
42	The Corporations Act should require courts to give priority to compensation

43	The civil penalty regime should be expanded to the provisions outlined in Table C
44	The provisions outlined in Table D should be made infringement notice provisions.
45	Infringement notices should be set at 12 penalty units for individuals and 60 penalty units for corporations for any new infringement notice provisions

7. Strengthening penalties for corporate and financial sector misconduct

Overview

The issues examined by the Taskforce in relation to penalties can be separated into two broad categories. These are, on the one hand, quantum of penalties, and on the other, what might be called penalties ‘pathways’. The term ‘quantum’ of penalties is meant to capture both fines and other pecuniary penalties, as well as terms of imprisonment. The term ‘pathways’ refers to the scope of provisions determined by the legislature to attract criminal or civil penalties or some form of administrative sanction.

The ASIC-administered legislation contains a wide variety of criminal offences and civil contraventions. Criminal offences carry a broad range of consequences both in terms of potential fines and, for more serious offences, terms of imprisonment. Civil penalties usually are determined by reference to a flat cap on maximum amounts that can be imposed. For example, currently under the Corporations Act the maximum amount for individuals is \$200 000, and for corporations, \$1 million. ASIC may also deal with certain matters administratively, such as by use of penalty or infringement notices, which allow a recipient to pay an amount in response to an alleged contravention to avoid formal proceedings being brought against them.

As noted in the Taskforce Positions Paper no. 7, concerns have emerged in a number of fora that the penalties in the legislation administered by ASIC, and penalties imposed in the courts, may not be substantial enough to represent a credible deterrent or meet community expectations as to the seriousness of misconduct in these sectors. For example, the FSI concluded that the maximum penalties in financial sector laws were unlikely to deter misconduct by large firms and recommended substantially increasing civil and criminal penalties.

In response to those concerns, and to its assessment of their merit, the Taskforce consulted on a range of potential increases in quantum of penalties.

ASIC has also argued for a significant increase in the ‘pathways’ for penalties and administrative action in response to contraventions, and accordingly the Taskforce consulted on possible expansion of the suite of provisions that attract civil penalties, criminal offences, penalty notices, and infringement notices.

The Taskforce received 31 submissions in response to Positions Paper 7. There was strong support for many of the Taskforce positions consulted on. However, some submissions opposed proposals to increase the quantum of penalties (both civil and criminal), and to the proposals to expand the range of contraventions that attract penalty or infringement notices. These and other significant matters raised are addressed in detail below. The Taskforce recommendations include adjustments to the original positions consulted on as a result of submissions received.

In particular, the Taskforce recommendation on civil penalty amounts has been adjusted and is now as follows:

Maximum civil penalty amounts in all ASIC-administered Acts should be:

- For individuals: 2,500 penalty units (currently \$525,000); and
- For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units).

This is a simpler and more consistent result than that consulted on, which had a lower penalty unit amount for corporations for contraventions of the Corporations Act or Credit Act. However, the Taskforce has, in its recommendation, also capped the total possible maximum amount for corporations based on 10% of annual turnover at not more than 1 million penalty units. These adjustments achieve greater symmetry with the BEAR, as well as comparable competition and consumer provisions.

Based on this approach, the civil penalty amount for corporations requires consideration by the courts of three potential options for determining the relevant maximum penalty in any given case. The applicable maximum penalty would be the greatest of those three amounts. The court then would have the usual discretion to impose a penalty *up to* that amount.

The Taskforce has carefully considered submissions around the extent to which there should be additions to the classes of provisions that attract penalty or infringement notices. For the reasons set out in this chapter, The Taskforce has maintained its positions and recommended expansion of these classes, but has reduced the extent of that expansion in line with the principles outlined.

The Taskforce has made recommendations broadly in line with other positions outlined in the Positions Paper, outlining its response to significant issues raised, below. In Positions Paper 7, the Taskforce set out principles that guided its deliberations on these issues. A revised version of those principles is set out in Appendix A to this chapter.

Quantum of penalties: Criminal

The Corporations Act, ASIC Act and Credit Act and the National Credit Code (Credit Code) provide criminal penalty provisions that ASIC has responsibility for investigating and enforcing. These Acts and various parts of them have emerged disparately over time, giving rise to inconsistencies in the penalty regime of each. For example, in 2010, the Federal Parliament increased penalties for insider trading, market manipulation offences and dishonest conduct in the provision of financial products and services in the Corporations Act. The maximum term of imprisonment was doubled from five to 10 years and maximum fines were increased to the greater of 4,500 penalty units (currently \$945,000), or three times the value of the benefits obtained for individuals, and for corporations the greater of 45,000 penalty units (currently \$9.45 million), three times the value of the benefits obtained, or potentially 10% of annual turnover in the preceding 12 months. These now represent the highest maximum penalties currently applicable for contraventions of the Corporations Act.

In contrast, despite their comparable seriousness, the maximum penalties for a number of other offences under the Corporations Act that involve dishonesty in relation to conduct as a director, officer or employee of a corporation, remain at a maximum of five years' imprisonment and/or 2,000 penalty units (currently \$420,000).⁶⁹

For any given offence, the statutory maximum penalty restricts the court's sentencing discretion because it marks the *absolute limit* of any sentence that may be imposed and is reserved for instances of the offence that are so grave that they warrant the imposition of the ultimate prescribed penalty for that offence. Where the offence is not so grave the judge must consider the facts of the particular offence and where they lie on the spectrum of misconduct.

⁶⁹ For example Corporations Act subsection 184, 601FD, 601FE, 601UAA and 601UAB

Broadly, the highest maximum prison terms for white collar and corporate offences in Australia are generally comparable with those in other jurisdictions, with the exception of the maximum term of imprisonment in the United States, which is 20 years.⁷⁰ Additionally, it should be noted that some of the corporate offences in Australia differ substantially from comparable offences in other jurisdictions. For example, in addressing breaches of directors' and officers' duties, Australia is unique in having specific statutory duties.

Recommendation 32

The maximum imprisonment penalties for criminal offences in ASIC-administered legislation should be increased as outlined in Table A.

Particular categories of offences where the Taskforce has identified the potential to increase penalties are defective disclosures, false or misleading statements to customers, failure to comply with corporate obligations, unlicensed conduct, failure to comply with financial services licensee obligations, client money obligations, credit code obligations, failure to comply with ASIC requirements and making false or misleading statements to ASIC.

The next part of this chapter will discuss some of the Taskforce's recommended increases to criminal penalties, without addressing each and every increase recommended. A complete list of increases in imprisonment penalties is provided in Table A.

The Law Council of Australia raised concerns with increasing penalties for offences that "do not necessarily involve dishonesty." The Australian Institute of Company Directors also raised similar concerns. While the Taskforce has discussed the importance of strengthening criminal penalties for offences with an element of dishonesty, this does not mean offences can only be serious where dishonesty is a requirement. Offences that can be constituted by other fault elements – intention, recklessness, and criminal negligence can cause significant harm and may warrant criminal punishment (as expressly acknowledged under the Criminal Code). The degree of 'dishonesty' or other measures of culpability are obviously matters that will be considered by the courts in exercising their sentencing discretion.

Defective disclosure and false or misleading statements to consumers

Chapter 7 of the Corporations Act sets out a number of disclosure requirements for licensees and financial services providers, including requirements to give consumers specific documents and offences relating to the provision of defective disclosure documents. Disclosure documents are generally defective if they contain misleading or deceptive statements or omit material information including information required by the Act to be included in the document.⁷¹

The offences of failing to provide disclosure documents when required have maximum penalties of a fine of 50 penalty units (for strict liability offences) where a fault element such as intention is not required to be established) and 100 penalty units (or 500 penalty units for a body corporate) and/or two years' imprisonment for an ordinary offence. Knowingly providing defective disclosure carries a maximum penalty of 200 penalty units (1,000 penalty units for a body corporate) and/or five years' imprisonment.

⁷⁰ In the United Kingdom and Hong Kong, the maximum prison terms for similar offences are ten years. In Ontario, Canada, the maximum prison term is 14 years, and in the United States it is twenty years.

⁷¹ See sections 952B(1), which defines 'defective' with respect to the Financial Services Guides and statement of advice, and section 1021B(1) with respect to Product Disclosure Statements

These disclosure requirements are fundamental obligations designed to protect consumers. Knowingly providing defective documents to consumers is comparable with the obligations under section 1041E. Similar breaches should carry the same penalty as section 1041E.

The Taskforce recommends that the prison terms for offences of failing to give a required disclosure document be increased to five years. Further, under subsection 952L(2), an authorised representative must comply with a licensee direction under subsection 952L(1). Contravention of this obligation currently carries a maximum penalty of 100 penalty units and/or two years' imprisonment. The maximum penalty should be increased to five years' imprisonment and 600 penalty units for individuals, to correspond with the recommended increase to subsection 952L(1).

In its submission AFMA notes that disclosures under section 1041E are distinct from those under sections 952D, 952F, 952L and 1021D as section 1041E disclosures "cover a wide range of statements that are voluntarily made" rather than disclosures required by statute. On that basis, AFMA submits that these disclosure provisions are "far easier to breach" than section 1041E. Other stakeholders also raised concerns with increasing the penalties for disclosure-related offences. The Taskforce acknowledges that these provisions are not entirely analogous to section 1041E. Nonetheless they relate to necessary disclosures that allow consumers to make informed decisions and cover knowing and dishonest misconduct by a specific class of licensed professionals that should be subject to a higher standard of conduct.

SPECIFIC RECOMMENDATION 32.1

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsections 952D(1); 952D(2); 952F(2); 952F(3); 952F(4); 952L(1); 1021D(1); 1021D(2)	5 years' imprisonment and/or 200 penalty units (individuals) 1,000 penalty units (corporations)	General formula does not apply 10 years' imprisonment and/or 4,500 penalty units or x3 benefits (individuals) 45,000 penalty units or x3 benefits or 10% annual turnover (corporations)
Subsection 952C(3); 952L(2) and 1021C(3)	2 years' imprisonment and/or 100 penalty units (individuals) 500 penalty units (corporations)	5 years' imprisonment and/or 600 penalty units (individuals) 6,000 penalty units (corporations)

Chapter 6D provides that a person should only make an offer of securities or distribute an application form for an offer of securities after a disclosure document for the offer has been lodged with ASIC, except in some very specific circumstances. The sale of securities without a prospectus or other disclosure document can have the result that substantial funds are raised illegally from investors to their detriment and for the benefit of those involved in the fundraising. Investors can also be adversely affected by misstatements and omissions in disclosure documents.

On the basis of the seriousness of these offences, the Taskforce recommends that the maximum criminal penalty be increased as outlined below.

The recommended penalty increase is intended to act as a substantial deterrent to those who intentionally seek to avoid their disclosure obligations and those who cause harm to investors.

SPECIFIC RECOMMENDATION 32.2

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsection 727(1); 728(3)	5 years' imprisonment and/or 200 penalty units (individuals) 1,000 penalty units (corporations)	General formula does not apply 10 years' imprisonment and/or 4,500 penalty units or x3 benefits (individuals) 45,000 penalty units or x3 benefits or 10% annual turnover (corporations)

Failure to comply with corporate obligation

A number of offences (including section 184) under the Corporations Act involve dishonesty in relation to conduct as a director, officer or employee of a corporation. Given these offences also relate to employees and officers using their position to improperly gain a benefit, or to cause detriment to others, the Taskforce considers it appropriate to increase the criminal penalty for these offences to match the recommended increase to section 184, as outlined below.

SPECIFIC RECOMMENDATION 33.3

Relevant provision	Current maximum penalty	Recommended maximum penalty
Section 596AB	10 years' imprisonment and/or 1,000 penalty units (individuals) 5,000 penalty units (corporations)	General formula does not apply 10 years' imprisonment and/or 4,500 penalty units or x3 benefits (individuals) 45,000 penalty units or x3 benefits or 10% annual turnover (corporations)
Subsections 601FE(4)	601FD(4); 5 years' imprisonment and/or 2,000 penalty units (individuals) 10,000 penalty units (corporations)	As above
Subsections 601UAB(1)	601UAA(1); 5 years' imprisonment and/or 300 penalty units (individuals) 1,500 penalty units (corporations)	As above

Section 206A(1) prevents any person who is disqualified from managing corporations from then participating in management responsibilities. Disqualification from managing corporations is an

important protection against individuals who have demonstrated themselves unfit to perform a management role.

The current penalty is not sufficient to meet community expectations about misconduct of this kind, which has the capacity to undermine the protective purpose served by disqualification. The recommended increase to the maximum imprisonment penalty is intended to ensure consistency with offences of equivalent seriousness.

SPECIFIC RECOMMENDATION 33.4

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsection 206A(1)	1 year imprisonment and/or 50 penalty units (individuals)	5 years' imprisonment and/or 600 penalty units (individuals)
	250 penalty units (corporations)	6,000 penalty units (corporations)

Unlicensed conduct

In Australia, financial services and credit providers must be licensed by ASIC. Carrying on a financial services business without a licence is an offence under section 911A. Section 920C establishes an offence where a person who has been banned from providing financial services engages in conduct in breach of a banning order. A ban from providing financial services is an important protection against individuals who have demonstrated themselves unfit to provide these services. The conduct is comparable to carrying on a financial services business without a licence, with the aggravating factor that the person has already been banned from providing financial services.

Similar to the proposal to increase the penalty for section 206A above, the offending conduct can undermine the protective purpose served by banning. The proposed increase to the maximum imprisonment penalty for these offences is intended to ensure consistency with offences of equivalent seriousness. Stakeholder submissions from the Association of Financial Advisers and Lecturer Andrew Serpell were broadly supportive of increases to penalties for unlicensed conduct given the risk of significant consumer harm.

SPECIFIC RECOMMENDATION 33.5

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsection 911A(1)	2 years' imprisonment and/or 200 penalty units (individuals)	5 years' imprisonment and/or 600 penalty units (individuals)
	1,000 penalty units (corporations)	6,000 penalty units (corporations)
Subsection 920C(2)	6 months' imprisonment and/or 25 penalty units (individuals)	5 years' imprisonment and/or 600 penalty units (individuals)
	125 penalty units (corporations)	6,000 penalty units (corporations)

Failure to comply with financial services licensee obligations

Breaches of financial services laws can result in significant consumer detriment. Protecting the integrity of Australia's financial and insurance sector is crucial to the well-being of Australia's economy. Despite this, research indicates that on the whole, courts apply imprisonment terms relating to contraventions of the Corporations Act cautiously and conservatively.

Breaching financial services licensee obligations has the potential to do significant harm to an individual and undermines the integrity of the broader financial services profession. The maximum penalty should be raised to meet with community expectations for such misconduct.

SPECIFIC RECOMMENDATION 33.6

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsections 991E(1) and (3)	6 months' imprisonment and/or 25 penalty units (individuals)	1 year imprisonment and/or 120 penalty units (individuals)
	125 penalty units (corporations)	1,200 penalty units (corporations)

Licensees also have certain obligations to assist ASIC or authorised persons in the performance of the corporate regulator's functions. Compliance with such obligations is fundamental to the licensing regime and failure to comply should carry a significant penalty higher than those currently allowed. In particular, a licensee's obligation under section 912C to comply with a direction from the regulator to provide a statement containing specified information is fundamental to the licensing regime, and a contravention should attract a substantial pecuniary penalty.

SPECIFIC RECOMMENDATION 33.7

Relevant provision	Current maximum penalty	Proposed maximum penalty
Subsection 912C(3)	6 months' imprisonment and/or 25 penalty units (individuals)	2 years imprisonment and/or 240 penalty units (individuals)
	125 penalty units (corporations)	2,400 penalty units (corporations)

Licensees have various obligations to notify ASIC about breaches of their obligations and about participants in the market. The licensee's obligation to report breaches is fundamental to the licensing regime. For example, the obligation to notify ASIC of any breach of conditions on approval under subsection 851D(8) carries a penalty of 100 penalty units for individuals. While the current maximum imprisonment penalty of two years is appropriate, the criminal pecuniary penalty should be increased to reflect the seriousness of such misconduct. Recommendation 33, outlined below, would increase the pecuniary penalty for such instances.

A financial services licensee is obliged to keep financial records which correctly record and explain the transactions and the financial position of the licensee's financial services business under

subsection 988A(1). Failure to comply with these requirements is an offence punishable by a fine of 200 penalty units or five years' imprisonment for an individual.

The obligation to keep proper financial records is fundamental to financial reporting requirements. The Taskforce is not proposing to increase the maximum imprisonment penalty for this offence but considers the pecuniary penalty too low, and that it may be treated as a cost of business. Recommendation 33, outlined below, would increase the pecuniary penalty for individuals.

Defective disclosure to ASIC

ASIC investigates a wide variety of serious corporate, markets and financial services related offences. Some of these offences may be notoriously difficult to investigate and prosecute. Investigations can be very complex, as many corporate offences are committed in-house, within corporate and business structures, under a veil complexity or hidden within a vast body of legitimate trading or commercial activity. It is often difficult to obtain information and evidence from relevant parties, particularly where they may themselves be implicated, have close ties to a suspect or corporate entity or persons with commercial interests and reputations to protect.

As with many of Australia's various crime commissions, ASIC often relies on its compulsory examination powers to personally examine individual persons, many of whom are not otherwise cooperative, to obtain prompt, direct, truthful and unfiltered information and evidence. The provision of false or misleading information to ASIC, in the course of a compulsory examination or investigation, can significantly impede the course of justice.

The maximum penalty that currently applies to the provision of false or misleading information to ASIC under subsection 64(1) of the ASIC Act and subsection 291(1) of the Credit Act is two years' imprisonment and/or a fine of 100 penalty units. The Taskforce recommends that this penalty be raised to ensure consistency with equivalent offences in other legislation, such as those for providing false or misleading information to entities such as the Australian Criminal Intelligence Commission and Royal Commissions that are comparable to ASIC. The Taskforce notes AFMA's submission that similar penalties for Commonwealth Tribunals differ greatly to the penalties recommended by the Taskforce. However, the Taskforce considers that ASIC's investigatory role is more akin to that of the Australian Criminal Intelligence Commission and Royal Commissions as opposed to a body such as the Administrative Appeals Tribunal.

SPECIFIC RECOMMENDATION 33.8

Relevant provision	Current maximum penalty	Recommended maximum penalty
Subsections 64(1) ASIC Act and 291(1) Credit Act	2 years' imprisonment and/or 100 penalty units (individuals)	5 years' imprisonment and/or 600 penalty units (individuals)
	500 penalty units (corporations)	6,000 penalty units (corporations)

Increases to maximum criminal pecuniary penalties

The Taskforce considers that penalties should be increased for some of the offences in the categories discussed above. In respect of imprisonment, recommended new maximum terms for offences identified are set out in Table A.

In respect of fines, the Taskforce recommends that, in addition to increasing maximum amounts, the regime should be simplified and made more consistent by determining maximums by reference to a formula based on the maximum term of imprisonment for the relevant offence. This approach is already adopted as standard in the *Crimes Act 1914*⁷² (Crimes Act), but only applies where no other intention appears. The practice of prescribing particular amounts for particular offences thus overrides the Crimes Act in many instances.

The Crimes Act provides for the maximum fine for individuals to be calculated by months of imprisonment x 5 = maximum penalty units.

For corporations, a further multiple of five is applied to the formula for individuals. This is consistent with the Attorney-General's Department's *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (AGD guide) which contemplates a pecuniary penalty for individuals that is five times the number of months of imprisonment.

Recommendation 33

The maximum pecuniary penalties for criminal offences in the Corporations Act should generally be calculated by reference to the following formula:

**Maximum term of imprisonment in months X 10 = penalty units for individuals;
multiplied by a further 10 for corporations**

The Taskforce recommends that pecuniary penalties for individuals should be calculated by taking the number of months of imprisonment and multiplying by ten. Pecuniary penalties for corporations should be ten times the pecuniary penalty for individuals. While these multiples are higher than those in the Crimes Act, the Taskforce notes that the AGD guide contemplates that this may be appropriate for corporate offences.

There are other examples of this. For instance, under Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2017, some of the proposed offences for a corporation go beyond the five times multiplier on the individual offence. The Explanatory Memorandum to the Bill justifies the higher corporate penalty by stating 'corporations involved are likely to be well-resourced, and therefore a higher maximum penalty is required to ensure that the provision acts as an effective deterrent and punishment'. On this basis, the provision is consistent with the AGD Guide which specifies that each offence should have a maximum penalty that is adequate to deter and punish a worst case offence⁷³. For similar reasons, the Taskforce considers the 10 times ratio for corporations appropriate.

In their submission, Anderson, Hedges and Walsh noted that increasing penalties for corporations of all sizes could have a significant impact on SMEs, "imposing penalties on corporations that run SMEs poses a significant risk of incentivising illegal phoenix activity aimed at avoiding payment by the corporations of the penalties." The Taskforce notes that the recommended increases are to the

⁷² Section 4B

⁷³ Paragraph 151, Explanatory Memorandum, Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2017.

maximum penalty and that courts are likely to take into consideration the size of the entity in determining an appropriate penalty.

The formula does not have the effect of substituting a pecuniary penalty for imprisonment. Rather it maintains the court's discretion to apply an imprisonment penalty or a pecuniary penalty or both for individuals. The formula simply determines the maximum fine amount.

The Taskforce recommends that there should be an exception to the application of the formula for the most serious offences in the legislation – generally those offences that carry a maximum term of imprisonment of 10 years, such as corporate fraud. These offences should carry a bespoke pecuniary penalty as outlined in this report.

There are two other circumstances where the new formula will not be appropriate. First, in respect of offences that do not have an imprisonment option. Second, some offences calculate pecuniary penalties by reference to the number of days for which the offence continues. For example, subsection 904G(5) of the Corporations Act provides for a pecuniary penalty of '100 penalty units for each day, or part of a day, in respect of which the offence is committed and does not include an imprisonment option. Pecuniary penalties cast this way will not be affected by the recommended formula. However, some of these penalties may nonetheless be increased through other positions adopted by the Taskforce, such as the proposal to raise the maximum pecuniary penalties for strict liability offences to 20 penalty units.

Corporate fraud offences

Corporate fraud, in ASIC's context, refers to serious misconduct engaged in by directors, other company officers, and in some cases employees, that gives rise to criminal liability. Perpetrators exploit their position to derive a benefit for themselves or someone else.

The Corporations Act contains a number of provisions relating to fraudulent conduct. The offence under section 184 has the most general application. Subsection 184(1) imposes criminal liability where a director or officer of a corporation acts recklessly or with intentional dishonesty and fails to fulfil his or her duties to the corporation. Subsections 184(2) and 184(3) apply where a director, officer or employee uses their position or information dishonestly (or recklessly) with the intention to gain an advantage for themselves or someone else or to cause a detriment to the corporation.

ASIC is responsible for conducting investigations into suspected contraventions of the Corporations Act. ASIC also has the power to investigate breaches of corporate offences under the crimes legislation of the States and Territories. In determining which offences to prosecute, ASIC considers the likely penalty arising out the prosecution. As a result, ASIC regularly investigates whether misconduct amounts to a contravention of a State or Territory-based offence as well as, or instead of, offences under the Corporations Act. Prosecuting a combination of Commonwealth and State or Territory-based offences raises difficulties due to legal differences between jurisdictions, and, on conviction, differences in statutory penalties and sentencing practices. In some instances the prosecution may not be permitted to run a single trial involving both Commonwealth and State charges despite the commonality of the evidence supporting the offences. Conducting multiple trials has a significant impact on the alleged offender and is costly for them, courts, the CDPP and ASIC.

The most common maximum penalty for these State-based offences is up to ten years' imprisonment.⁷⁴ However, the penalty for contravening section 184 is only up to five years' imprisonment and/or a fine of up to 2,000 penalty units (currently \$420,000).⁷⁵

⁷⁴ For example, s192E of the *Crimes Act 1900* (NSW), s139 of the *Criminal Law Consolidation Act 1935* (SA) and s326 of the *Criminal Code* (ACT). However, in Western Australia, the ten year maximum is only applied to fraud

Recommendation 34

The maximum penalty for a breach of section 184 should be increased to reflect the seriousness of the offence, to 10 years' imprisonment and/or a fine: for individuals the greater of 4,500 penalty units of three times the benefit gained (or loss avoided); and for corporations the greater of 45,000 penalty units, or three times the benefit gained (or loss avoided) or 10% annual turnover.

To address these issues, the Taskforce recommends an increase to the maximum penalty for a breach of section 184 to 10 years' imprisonment and/or a fine: for individuals the greater of 4,500 penalty units of three times the benefit gained (or loss avoided); and for corporations the greater of 45,000 penalty units, or three times the benefit gained (or loss avoided) or 10% annual turnover.

Increasing the penalty under section 184 would align the penalty with comparable State and Territory-based offences. Further, it would realign the penalty with the maximum penalties for dishonest conduct in the financial services context and "cheating" in a markets context. These penalties are of comparable seriousness and were increased in 2010, while the penalty for section 184 has remained unchanged since 2001.

The recommendation would also increase ASIC's ability to prosecute corporate offences under Commonwealth laws, ensuring that ASIC can consistently access investigative powers in the prosecution of corporate fraud offences.

Additionally, ASIC has raised concerns that the wording in subsections 184(2) and (3) raises ambiguity around whether misconduct that *benefits the corporation* would amount to an offence. Minor amendments may be necessary to clarify that a person commits an offence if they use their position dishonestly to gain an advantage even where it is to the benefit of the corporation.

The Taskforce notes submissions overwhelmingly supported increasing penalties for s 184 contraventions as proposed by the positions paper.

Dishonesty test

Currently, there is no consistent definition of dishonesty in Commonwealth law. The Criminal Code contains definitions of dishonest that reflect the *Ghosh* definition, which is a two-tiered test that includes both an objective and subjective element.⁷⁵ It requires proof that the defendant's conduct was dishonest according to the standards of ordinary people, and also that the defendant knew the conduct was dishonest. A similar definition applies in section 1041G of the Corporations Act.

The High Court has confirmed the *Peters v R* objective definition as the preferred common law standard for dishonesty in Australia. The Peters test applies an objective definition of "dishonest

contrary to s409 of the *Criminal Code* (WA) in cases in which the person deceived is not less than 60 years old – otherwise the maximum is seven years. South Australia also has an "aggravated offence" provision in relation to victims known by the offender to be over 60 years of age that elevates the maximum penalty for deception to 15 years imprisonment. In Queensland, fraud contrary to section 408C is subject to a standard maximum penalty of five years' imprisonment; however this is elevated to 14 years in specified circumstances – including where the offender is a director or officer of the victim corporation – and to 20 years if the "yield" to the offender or detriment caused is more than \$100,000.

⁷⁵ From 1 July 2017, the *Crimes Amendment (Penalty Unit) Act 2017* increased the value of the penalty unit for Commonwealth offences from is \$210 (from \$180) with indexation to occur every three years following this date.

⁷⁶ *R v Ghosh* [1982] 2 All ER 689.

according to the standards of ordinary, decent people.”⁷⁷ This definition has been held to apply to some provisions of the Corporations Act, for example sections 588G and 184.

Recommendation 35

The Peters test should apply to all dishonesty offences under the Corporations Act.

In addition to amending the section 184 penalty, the Taskforce recommends that the Corporations Act should include a single definition of dishonesty that reflects current common law. This would ensure consistency and certainty when prosecuting offences relating to dishonesty.

Given the Peters test has been approved by the High Court as the preferred test for dishonesty, the Taskforce, and majority of stakeholders, considered that this would be the appropriate test to apply across all dishonesty-related offences in the Corporations Act. While this would not resolve the inconsistency between the Criminal Code and Corporations Act, it would provide consistency within the Corporations Act.

Strict and absolute liability offences

A central protection underpinning criminal penalties is the proof of a fault or mental element of the offence. This is because the law recognises that individuals and corporations should generally not be subject to pecuniary penalties or imprisonment for unintended or unforeseen consequences of their conduct. However, a number of corporate law offences may be prosecuted even in the absence of a mental element or *mens rea*. These are commonly referred to as strict liability offences.

Strict liability offences remove the fault element that would otherwise attach to a physical element of an offence. For such an offence to be made out, the regulator must prove that the individual or corporation engaged in the physical elements of the offence. The Attorney-General’s Department Guide provides that application of strict and absolute liability all fault elements of an offence should only be considered appropriate where:

- The offence is not punishable by imprisonment and is punishable by a fine of up to 60 penalty units for an individual (300 penalty units for a body corporate);
- The punishment of offences not involving fault is likely to significantly enhance the effectiveness of the enforcement regime in deterring offences; or
- There are legitimate grounds for penalising persons lacking ‘fault’, for example, because they will be placed on notice to guard against the possibility of any contravention.⁷⁸

There are approximately 375 strict and absolute liability offences in the Corporations Act. These offences are found in a number of areas including the composition of corporate entities and licensing, the provision of information both to the general public and the regulator, compliance with ASIC and court/tribunal directions, directors’ duties and remuneration, corporate governance, including audit requirements, and the holding of monies on behalf of others. The vast majority of strict and absolute liability penalties in the Corporations Act range from five to 60 penalty units for individuals (currently \$1,050 to \$12,600) and 25 to 25 penalty units for corporate bodies (currently \$5,250 to \$63,000).

In enacting strict liability offences, Parliament recognises that the act of contravening these offences is sufficient to warrant a pecuniary penalty. There is value in having strict liability offences in

⁷⁷ *Peters v R* [1998] 192 CLR 493.

⁷⁸ *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, Attorney-General’s Department, p.23.

corporate regulation because it allows ASIC to enforce breaches of lower level offences in a more straightforward way, without the need to prove a fault element. In particular, ASIC regulates areas that people choose to enter, including company directors, superannuation trustees and financial advisers. It is expected that individuals in these roles should not only refrain from consciously doing wrong, but also take active steps to fulfil certain statutory obligations. A sophisticated regulatory regime like the corporate law requires certain positive obligations to be placed upon participants.

Recommendation 36

Imprisonment should be removed as a possible sanction for strict and absolute liability offences.

Currently, a number of Corporations Act strict and absolute liability offences also allow for a maximum term of imprisonment either in conjunction with, or in substitution for, the pecuniary penalty. For example, under section 205G, if a director fails to notify the relevant market operator of shareholdings, they may be subject to a pecuniary penalty of 10 penalty units and/or three months imprisonment.

The Taskforce recommends that imprisonment should be removed as a possible sanction for the contravention of strict and absolute liability offences under the Corporations Act. The Taskforce considers there is no demonstrable evidence that the possibility of imprisonment for these offences increases deterrence and the enforcement of these offences. The Taskforce also considers that individuals should not be imprisoned for inadvertent breaches of the law or offences where there is no mental element, consistent with the AGD Guide.

ASIC did not agree with Recommendation 36 in its submission, arguing that removal of imprisonment would undermine deterrence and:

“This is not to say that ASIC seeks custodial sentences against those who have breached strict and absolute liability provisions lightly. However, in particular cases where it is warranted, we will seek such remedies against wrongdoers. Custodial sentences are most often not appropriate in an isolated case, however, their presence and limited use, forms an important part of ASIC’s regulatory toolkit.”

The Taskforce considers, however, that where an offence warrants a custodial sentence, ASIC should be compelled to pursue that outcome via an offence provision that includes the usual protections and proof requirements applicable under the criminal justice regime. The Taskforce also notes that, under other recommendations in this report, ASIC would have a broader range of options to deal with such matters.

Recommendation 37

An ordinary offence should be introduced to complement a number of strict and absolute liability offences as outlined in Table B.

For example, the Taskforce recommends the introduction of a number of ordinary offences based on current strict and absolute liability offences. These new offences recognise that some current strict liability offences should be treated as a criminal offence if a fault element is present, and should be punishable by a fine and/or imprisonment term. It also allows for a greater scale of penalty where a contravention is committed deliberately and with intent.

Some provisions of the Corporations Act currently create both a strict liability offence and an ordinary offence for the same conduct. The Taskforce is of the view that the creation of a strict and

absolute liability offence and an ordinary offence for the same conduct allows a tailored and flexible response to the conduct, depending on the circumstances in which the offence is committed.

The above proposed classes of offences include sanctions for offences which are significantly higher than existing penalties, to reflect that the contravention is a deliberate breach of corporate law and therefore a higher level of culpability. In all these cases, it is the Taskforce's view that the current strict liability penalty does not adequately reflect the importance of these obligations in maintaining consumer confidence and the integrity of the financial industry. The new ordinary offence addresses serious cases of wilful or reckless non-compliance with the selected obligations. Absent an ordinary offence, individuals and companies found to be in contravention of these provisions may only be subject to a lower level fine. A list of the proposed offences is at Table B.

Recommendation 38

Maximum pecuniary penalties for strict and absolute liability offences currently set at 5, 10 or 15 penalty units should be increased to 20 penalty units for individuals, corresponding penalties for corporations should be increased to 200 penalty units.

The Taskforce recommends that all strict and absolute liability offences under the Corporations Act with a current maximum penalty of 5, 10 or 15 penalty units be increased to 20 penalty units for individuals. For these offences, the maximum penalty for corporations will also increase to 200 penalty units. For all other strict or absolute liability offences under the Corporations Act, the maximum pecuniary penalty for individuals will remain unchanged, with the current pecuniary penalty doubling for corporations. This is consistent with the new formula for calculating criminal pecuniary penalties as outlined in Recommendation 33.

Currently, there are a number of strict and absolute liability offences with pecuniary penalties below 20 penalty units (individuals) and 200 penalty units (corporations). The Taskforce is of the view that the maximum pecuniary penalty for these offences is too low and does not represent an adequate level of deterrence to would-be offenders. Pecuniary penalties for these contraventions need to be high enough so that they are not paid by the guilty and innocent alike as a cost of doing business. If penalties are always paid by offenders this may also have the unintended consequence of negatively affecting the stigma of the underlying offence. The recommended increase to these offences is also offset by the recommended removal of imprisonment as a possible sanction. The Taskforce recognises the importance of court discretion to set the appropriate penalty based on a statutory maximum. Accordingly, the Taskforce does not recommend setting a minimum amount for any penalties.

The weight of pecuniary penalties must be balanced against the fact that the offence can be established without a fault element. Penalties need to be set at a level where there is a deterrence factor for the guilty party without being punitive. In addition, if penalties are too low, the cost for ASIC to prosecute possible contraventions will outweigh the penalty itself.

A consequential change is also proposed for criminal pecuniary penalties for non-strict liability offences. To reflect the additional seriousness of these offences above strict liability offences, it is proposed that the maximum pecuniary penalties be increased to 30 penalty units for individuals and 300 penalty units for corporations.

Recommendation 39

All strict and absolute liability offences should be subject to the penalty notice regime.

As part of its enforcement toolkit, ASIC currently has the ability to issue penalty notices. However, this does not currently extend to all strict liability offences under the Corporations Act. The Taskforce recommends that the penalty notice regime should be available to ASIC for all strict and absolute liability offences under the Corporations Act.

Under section 1313 of the Corporations Act, ASIC currently has the ability to serve penalty notices on individuals and corporations for certain lower level breaches, for example failure to lodge documents within a prescribed time or notification of change to officeholders. A penalty notice must be in a prescribed form and set out details required by the Act including particulars of the relevant offence and the prescribed penalty. If the penalty notice is complied with, including payment of the prescribed penalty, no further action will be taken against the person and the payment is not considered an admission of liability for any purpose.

The Taskforce recommends that ASIC be given the power to issue penalty notices for half the maximum pecuniary penalty (subject to the prior recommendations) of the strict liability offence. Having removed the imprisonment component of the penalty for strict liability offences, an effective enforcement toolkit should allow ASIC to issue penalty notices to deal with these lower level breaches. This recommendation does not alter ASIC's ability to pursue contravention of the underlying offence and higher penalties. The Taskforce acknowledges that stakeholders in the consultation process were concerned that the proposed 50% of the maximum rate is high and is outside of the suggested 20% rate under the AGD Guide. A 20% rate is undesirable as recipients of penalty notices may simply pay them as a cost of compliance and would not reflect the administrative cost of issuing these notices. For example, a 20% rate for a 20 penalty unit offence would result in a penalty notice of 4 penalty units, which is lower than the current default penalty.

This recommendation will require amendments to penalties specified for strict liability offences in Schedule 3 of the Corporations Act and section 1311(5), which specifies a default penalty of five penalty units where no penalty is specified. Offences referred to in subsection 1311(5) are strict liability offences by reason of subsection 1311(6). Some minor amendments may also need to be made to align administrative aspects of the penalty notice regime with the infringement notice regimes.

Quantum: Civil penalties

Civil penalties were introduced for Corporations Law contraventions in 1993, recognising that a range of penalties should be available to the regulator to best address the individual circumstances of difference cases, and that criminal liability should apply only where conduct is genuinely criminal. Since that time, the use of civil penalties in legislation has become much more prevalent, and their nature perhaps less well-defined.

The maximum civil penalties in the Corporations Act have not increased since 1993, when the penalty for an individual was set at \$200,000 (and \$1 million for corporations since 2004). Apart from any other considerations, the value of these maximum penalties has eroded substantially due to the effects of inflation (these being set as fixed dollar amounts rather than penalty units). In addition, maximum civil penalties set in legislation for comparable conduct differ across the ASIC Act, the Credit Act and the *Competition and Consumer Act (2010)* (Competition and Consumer Act) and are higher than those set in the Corporations Act.

Recommendation 40

Maximum civil penalty amounts in ASIC-administered legislation should be increased as follows:

- For individuals: 2,500 penalty units (currently \$525,000);
- For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (\$210 million)).

The Taskforce sought, in Positions Paper 7, submissions on preliminary positions that maximum civil penalties in ASIC-administered Acts should be substantially increased, to ensure that ASIC can seek and courts are empowered to impose penalties that reflect community perceptions of the seriousness of engaging in corporate, financial market and financial services misconduct and are broadly consistent with the regimes of overseas counterparts and other domestic regulators.

The positions put by the Taskforce were:

- Penalties should be aligned with the maximum civil penalties for contravention of the consumer protection provisions in the ASIC Act with the increases to financial penalties proposed for the Australian Consumer Law, with equivalent penalties set by reference to penalty units as follows:
 - For individuals: 2,500 penalty units (currently \$525,000);
 - For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct.
- Additionally, the maximum civil penalties in the Corporations Act and Credit Act should be increased as follows:
 - For individuals: 2,500 penalty units (\$525,000);
 - For corporations: the greater of 12,500 penalty units (currently \$2.625 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct.

Many stakeholders commented on the above proposals in submissions. The key issues and the Taskforce's responses are set out below.

Maximum amounts for corporations

Many submitters argued that the "10% of annual turnover" figure should be available as an alternative only where the figure of three times profit gained or loss avoided could not be calculated. Submitters correctly pointed out that this is the case for proposed penalties under the Australian Consumer Law. AFMA argued, for example:

"The proposal would confer inordinate discretion or give inadequate guidance to judges imposing penalties. Consider, for example, a situation in which a wrong resulted in a benefit of \$1 million and the wrongdoer had annual turnover of \$500 million. By what objective standard is a judge to determine whether the maximum sanction should be \$3 million or \$50 million? And what if there were two wrongdoers in substantially the same position, one with annual turnover of \$500 million and the other with turnover of \$550 million. Why should the maximum sanction for one be \$50 million dollars and for the other \$55 million? And what if the conduct of the party with the lower turnover is objectively worse – how is the judge to

weigh that party's greater culpability against the other party's greater turnover? And what of the situation in which a party's turnover in the past is not a reflection of its capacity to pay in the present? These are not questions that should be left unanswered unless and until they are tested through the incremental process of the common law."

AFMA further argued that "Scaling penalties to the ability of the offender to pay similarly risks undermining notions of equality before the law and a rational and fair system of criminal justice."

The Taskforce does not accept these points. The financial capacity of a company is a relevant matter in setting civil penalties is an established principle. In *Australian Competition and Consumer Commission v Visa Inc* [2015] FCA 1020 (4 September 2015), Wigney J, in discussing "a checklist of matters that are usually relevant to the exercise of determining an appropriate pecuniary penalty" said:

*"Lest it be thought that there has been some departure from custom here, the list of potentially relevant matters includes the following: the size and financial position of the contravening company..."*⁷⁹

Further, in *Trade Practices Commission v. Stihl Chain Saws (Aust) Pty Ltd* (1978) ATPR 40-091, Smithers J. said:

*"The penalty should constitute a real punishment proportionate to the deliberation with which the defendant contravened the provisions of the Act. It should be sufficiently high to have a deterrent quality, and it should be kept in mind that the Act operates in a commercial environment where deterrence of those minded to contravene its provisions is not likely to be achieved by penalties which are not realistic."*⁸⁰

AFMA asserts that judges will have difficulty in assessing the legislative intent as to penalty because there could be a large discrepancy between figures such as three times benefit gained and 10% of turnover, especially for companies with higher turnovers. The Law Council of Australia made a similar point. The Taskforce does not however, find this point convincing. In the example from the AFMA submission outlined above, courts will have a benchmark by reference to the amount of benefit gained (ie three times 1 million), but will know also that they have a broad discretion to impose a penalty much higher than this if that is what the 'price of compliance' demands in all the circumstances including the commercial reality of a relevant company's financial capacity. Noting also that courts will use a wide range of other criteria to assess an appropriate penalty amount (as they must always do in the context of regimes like most of those for civil penalties in Australia), in which maximum penalties are set by reference to a flat amount rather than a bespoke maximum for each contravention, or a sliding or tiered scale.

The Taskforce has, however, come to the view that there should be an upper limit on the 10% turnover figure. The maximum amount announced for the BEAR is 1 million penalty units. For symmetry across legislation relating to the financial sector, and to avoid maximum penalties based on turnover from becoming too excessive, the Taskforce believes this cap should be adopted for its proposed regime.

ASIC submitted that, for civil penalties in the Corporations, ASIC and Credit Acts, maximum civil penalties for corporations should be the greater of 50,000 penalty units (currently \$10.5m) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct. This submission is consistent with the Taskforce proposal for (broad) alignment of ASIC Act provisions with the proposed new Australian Consumer Law penalties. However, it differs from the Taskforce position on maximum penalties for corporations under the

⁷⁹ At para 82.

⁸⁰ At 17,896

Corporations Act – 12 500 penalty units (\$2.625 million), or three times benefit or 10% annual turnover. Other submissions, including that of the Financial Planning Association of Australia, and the Financial Rights Legal Centre, questioned the basis for a difference in the maximum penalty unit amount for Corporations Act offences.

After further considering this matter, and noting that the proposed maximum penalty under the BEAR (for entities with assets less than \$10 billion) is also 50 000 penalty units, the Taskforce believes that setting the maximum penalty at that amount across the range of ASIC administered legislation would bring about a greater degree of alignment and participate in the setting of that amount as a broad benchmark in the corporate and financial sectors.

Maximum amounts for individuals

Most submissions supported the proposed increase in maximum penalties for individuals, across ASIC-administered legislation, to 2500 penalty units (\$525 000). An exception was ASIC, which submitted that:

“for individuals, the greater of 5,000 penalty units (currently \$1.05m), or three times the value of benefits obtained or losses avoided.”

The Taskforce has considered this view but does not accept it. A maximum penalty of 2500 penalty units aligns with other comparable legislation. In addition, none of the comparable legislation has the added ‘three times benefit obtained or loss avoided’ criterion for civil penalties for individuals. The Taskforce notes that individuals, in addition to exposure to potential disgorgement orders (under Taskforce proposals), are also potentially exposed to other sanctions such as disqualification, a significant consequence in itself.

After accounting for the matters raised above, the final recommendation of the Taskforce on these issues is that penalties be increased as outlined in the box below.

Box 1: Recommended civil penalty maximum amounts

Maximum civil penalty amounts in all ASIC-administered Acts should be:

- For individuals: 2,500 penalty units (currently \$525,000);
- For corporations: the greater of 50,000 penalty units (currently \$10.5 million) or three times the value of benefits obtained or losses avoided or 10% of annual turnover in the 12 months preceding the contravening conduct (but not more than 1 million penalty units (\$210 million)).

Disgorgement in civil penalty proceedings

At present there is no clear mechanism for ASIC to seek disgorgement of financial benefits in civil penalty proceedings. Disgorgement is a vehicle for preventing unjust enrichment and involves the removal of financial benefit (such as profits illegally obtained or losses voided) that arises from wrongdoing. Disgorgement orders reduce the likelihood that wrongdoers can treat penalties as a cost of doing business.

In a criminal context, the AFP and CDDP are empowered to bring civil proceedings under the *Proceeds of Crime Act 2002* (Cth) to recover the proceeds or benefits arising from alleged criminal offences, even in the absence of a criminal conviction.⁸¹ However, they would be unlikely to bring such proceedings in the absence of a criminal investigation and the prospect of a criminal conviction.

⁸¹ The *Proceeds of Crime Act*'s civil regime is directed to confiscating unlawfully acquired property independently from the prosecution process. The civil stream provides for the forfeiture of property on the basis of a court being satisfied to the civil standard that the person has committed a serious offence.

Orders made under the Proceeds of Crime Act require forfeited money to be paid into a ‘confiscated assets account’ and cannot be restrained for the benefit of the victims.

There is no similar process provided for civil penalty proceedings issued under the Corporations Act, ASIC Act or Credit Act. These Acts currently provide for the making of compensation orders in civil penalty proceedings and the court to make any order that it sees fit under section 1101B of the Corporations Act. However, these avenues do not provide a basis for disgorging financial benefits from wrongdoers.

It should be noted that the aim of a compensation order is different from disgorgement. A compensation order involves identifying the party who has suffered loss or damage and returning the quantified loss or damage to the injured party. In cases brought by ASIC, particularly in market misconduct matters, the parties suffering loss may not be easily identified while the financial benefit resulting from the misconduct can be quantified.

Under section 1101B of the Corporations Act, if there is a breach of a provision in Chapter 7 of the Corporations Act, the court may make any order it considers fit, provided that the order does “not unfairly prejudice any person.” While section 1101B provides a non-exhaustive list of orders that a court may make, it neither includes nor expressly prohibits an order for payment of profits. As a result a court could, theoretically, make such an order; however, there is no precedent for such an order being made.

Recommendation 41

Disgorgement remedies should be available in civil penalty proceedings brought by ASIC under the Corporations, Credit and ASIC Acts.

The Taskforce recommends that disgorgement remedies should be available in civil proceedings brought by ASIC under the Corporations, Credit and ASIC Acts. This would enable ASIC to seek orders requiring payment of an amount representing any profit gained or loss avoided by the person as a result of engaging in a contravention of a civil penalty provision. This recommendation recognises that it may not be appropriate for a defendant to retain a profit or benefit derived from contravening the law, particularly where the financial benefit can be quantified. This may be the case whether or not a person may also be liable to a pecuniary penalty order.

As in the case of disqualification orders, it may be expected that the court would take into account any disgorgement remedy sought or granted when exercising its discretion whether to make a pecuniary penalty order and in determining the amount of any penalty ordered to be paid.

The Taskforce considers that the legislation should include a general disgorgement remedy that may be ordered on the application of ASIC. The court should retain the discretion to determine whether any payment is appropriate and how it should be applied given the circumstances. Where there are parallel proceedings for compensation it may be appropriate to make the funds available to satisfy compensation orders. Otherwise it may be appropriate for the funds to be paid to consolidated revenue.

While the majority of respondents supported availability of disgorgement remedies in ASIC initiated civil penalty proceedings, a collection of respondents disagreed with the proposal. For example, Nyman Gibson Miralis Defence Lawyers and Advisors expressed concerns that while a defendant may be fined, any additional proceedings initiated by ASIC in a court of equity for disgorgement may punish the defendant twice. While there may be a procedural question regarding whether such proceedings are heard together or separately, the Taskforce does not agree that the offender is exposed to double punishment. An offender is always likely to be exposed to private action for recovery of ill-gotten gains from a contravention.

Correspondingly, AFMA recognises there may be difficulties in reconciling profits with alleged misconduct and, therefore, disgorgement proceedings having limited utility in such matters. Furthermore, AFMA notes financial institutions may compute their profits using varying accounting standards which may result in prejudicial and inconsistent application of the measure. No doubt these are matters that a court can take account of on any proceedings for disgorgement.

Priority for compensation

As above stated, under the ASIC and Credit Acts courts must give preference to making an order for compensation if a person has insufficient financial resources to pay a pecuniary penalty (or fine) and compensation. There is no equivalent provision in the Corporations Act.

Recommendation 42

The Corporations Act should require courts to give priority to compensation.

The Taskforce recommends that the Corporations Act should expressly require courts to give preference to making a compensation order where a defendant does not have sufficient financial resources to pay both a pecuniary penalty order and a compensation order. This will ensure that priority is always given to compensating victims who suffer loss or damage as a result of misconduct, which is consistent with the provisions in the ASIC Act and the Credit Act and appropriate given the increases to maximum civil penalties as proposed above. Submissions to Positions Paper 7 conclusively approved the suggested position. However, AFMA suggests any prioritisation mechanism not risk double jeopardy for the defendant, i.e. an offender initially having to pay compensation and, subsequently, a fine by regulator.

Pathways: Civil penalties

As outlined in Positions Paper 7, the Taskforce considered that civil penalties should be available for an increased range of contraventions of ASIC-administered legislation. Submissions on this were varied. ASIC's submission argues for a broad range of provisions to be opened to civil penalty proceedings. ASIC's justification for this, broadly expressed, is as follows:

“The availability of a civil penalty is a significant addition to ASIC’s enforcement capability, as part of a broad spectrum of potential enforcement responses, which also include negotiated outcomes or infringement notices for less serious contraventions and administrative action, such as licence cancellation, disqualification or banning, and criminal prosecution for the most serious misconduct.

As such, in ASIC’s submission civil penalties should be available across a broad range of contraventions of the legislation it administers. This would facilitate a more calibrated and proportionate response to the specific circumstances of the contravening conduct in each case.”

Against this, some stakeholders argued that civil penalties should not be extended beyond the existing list of eligible contraventions. An example is the submission of the Law Council of Australia:

“The list of civil penalty provisions in section 1317E was determined by Parliament after proper consultation and detailed consideration as to whether the particular provisions should be civil penalty provisions. In the Committee’s view, Parliament should be slow to add to this list (with the attendant consequences of making a provision a civil penalty provision) without clear evidence that it is necessary to meet the policy objectives of the relevant provision.

General statements that it might be useful for ASIC to have an additional set of remedies for certain provisions are not evidence of the policy need for the change.”

The Taskforce maintains the view that civil penalties should be available for a broader range of contraventions. However, the Taskforce agrees that careful consideration should be given to which provisions can appropriately be opened to civil penalties and which should not be included. This has not been an easy task. Nevertheless, the Taskforce has drawn on the history and purpose of civil penalties in coming to a conclusion and recommending that the provisions in Table C be made subject to civil penalties.

Civil penalties were first introduced in the financial sector as an additional penalty option for breaches of director’s obligations under the Corporations Act. Their introduction was essentially for the purpose of addressing conduct that is sufficiently serious to warrant the imposition of a sanction but is not truly criminal in nature. It was seen as necessary to provide a sanction to respond appropriately to misconduct that did not merit the ‘moral and social censure and stigma that attaches to conduct regarded as criminal’.⁸² As stated in the ALRC Principled Regulation report:

“Civil penalties provide a means for the state to enforce breaches of laws without going as far as declaring all lawbreakers ‘criminals.’⁸³

The ALRC considered that ‘there was value in maintaining provisions in legislation which allow for a choice of criminal or civil proceedings for the same conduct. Such flexibility is an important feature of regulation and allows a regulator the ability to tailor appropriate penalties to breaches’ and recognised that this can benefit the regulator and the regulated. At the same time the ALRC considered that the legislation should be drafted in a manner that clearly states the elements of each offence especially where different mental elements govern the criminal offence and civil penalty contravention.⁸⁴

As noted in the Positions Paper, the Taskforce considers that a civil penalty should not be available for contraventions where one of the elements of the offence is dishonesty. Conduct of this nature is truly criminal in character and warrants a criminal sanction. There are good reasons underpinning this principle. For example, providing for civil penalties for offences that are criminal in character may be inconsistent with articles 14 and 15 of the International Covenant on Civil and Political Rights (ICCPR), unless they provide for criminal process protections (see Parliamentary Joint Committee on Human Rights, Guidance Note 2: Offence provisions, civil penalties and human rights December 2014). See also “Traditional Rights and Freedoms—Encroachments by Commonwealth Laws” ALRC report 129:

“A person may be denied their criminal process rights where a regulatory provision is framed as a civil penalty, when it should—given the nature and severity of the penalty—instead have been framed as a criminal offence.”

The framework for the prosecution of criminal offences includes processes and protections to preserve civil rights and liberties. Regulatory regimes should be formulated so that criminal conduct is prosecuted within this framework – ie as a criminal offence – ensuring that criminal process rights are attached. This is not to say that there are no classes of misconduct in respect of which it may be appropriate to provide for both criminal and civil remedies, according to the degree of culpability. Contravening conduct may potentially span the spectrum that includes both criminal and non-criminal characterisation. For example, a contravention by a director involving similar physical elements may on the one hand be properly characterised as criminal if accompanied by fault elements such as intention, recklessness or dishonesty, but still be characterised as conduct

⁸² ALRC Principled Regulation report at [3.110]. See also the discussion at [2.10]-[2.11].

⁸³ Ibid at [3.46].

⁸⁴ ALRC Principled Regulation report at [11.5] and [11.65] – [11.67].

warranting a civil penalty in the absence of those elements. The question is whether, in the latter case, contravention of the provision, though not criminal, has the potential to be of such significance as to require a substantial sanction to promote compliance.

Recommendation 43

The civil penalty regime should be expanded to the provisions outlined in Table C.

The Taskforce recommends civil penalties for contraventions where there is a regulatory gap, and where a civil penalty would appropriately address that gap. The Taskforce, in deciding on its final recommendation, has sought to include contraventions that are serious enough to warrant pecuniary sanction and put a ‘price on non-compliance’, but has sought to exclude contraventions which, in its view, are properly characterised as criminal (noting that this is not always a straightforward matter).

The list of provisions that the Taskforce considers appropriate to make civil penalty provisions, based on the principles outlined above, are set out in Table B.

Licensee obligations

The Taskforce consulted on a preliminary position that licensee obligations (section 792A and 912A of the Corporations Act) should be made civil penalty provisions, subject to excepting some of their broader provisions such as the requirement to ‘comply with financial services laws’.

This was subject to the qualification that it may not be appropriate to make every obligation a civil penalty provision as the consequences of attaching a civil penalty to some obligations may be undesirable. For example, attaching a civil penalty to the obligation of AFS licensees to comply with financial services laws may cause duplication between the general obligation and specific provisions to which a civil penalty also attaches.¹²⁸ Further, in this example, a contravention of any financial services law by a licensee would potentially attract civil penalty liability, not just those laws to which it has been determined a civil penalty should attach.” The obligation to comply with licence conditions could be objectionable for similar reasons.

The Taskforce considers this position to be appropriate and has recommended that licensee obligations become civil penalty provisions with the exceptions outlined in the preceding paragraph.

Section 180

Positions Paper 7 queried whether a breach of section 180 of the Corporations Act (directors’ and officers’ duty of care and diligence) should continue to give rise to a civil penalty given it creates a contravention for negligent conduct. Stakeholders were divided on this issue. The AICD suggested a right to compensatory remedies would be more appropriate for such misconduct given it captures conduct spanning mere negligence as well as gross negligence. However, Anderson, Hedges and Welsh argue that public enforcement of section 180 is “a critical function in maintaining good standards of corporate governance”. Relevantly, disqualification is available as a remedy in cases of contravention thus providing ASIC with a method to enforce standards of conduct for directors and officers.

The Taskforce notes some stakeholder concerns around the proportionality of a civil penalty for mere negligence. However, as section 180(1) captures a range of negligent conduct, including what courts have referred to as gross negligence, and has the objective of ensuring directors and other officers exercise reasonable care and diligence it considers the section has an important governance role. In addition, allowing ASIC to enforce contraventions of s 180(1):

- means that ASIC has the discretion to bring proceedings where private litigation would not be brought (for example, the director does not have the assets to pay any compensation) but ASIC, in fulfilment of its objectives set out in the ASIC Act, is of the opinion that litigation should be brought; and
- enables courts to impose penalties (a management banning order and a pecuniary penalty) which would not be available when a contravention of s 180(1) is enforced through private litigation, where the court believes these penalties are justified.

On that basis, the Taskforce makes no recommendation to remove the civil penalty for contraventions of section 180.

Pathways: Infringement Notices

In Positions Paper 7, the Taskforce sought feedback on its preliminary position to expand the set of provisions which are subject to the issue of infringement notices. As noted in the paper, infringement notices are “an administrative device to dispose of a matter that involves a criminal or non-criminal breach.”⁸⁵ They are an allegation of a contravention of the law, payment of which causes the regulator to not pursue the alleged contravention any further. Payment of the notice also is not taken as an admission of guilt by the alleged offender. However, if the infringement notice is not complied with, ASIC remains entitled to bring other proceedings, civil or criminal, against the offending party.

Infringement notices, in one form or another, have been used for decades in Australia in relation to high volume, low-level, often quasi-criminal matters such as traffic offences. Their use has increased markedly in recent years at both the State and Federal level.⁸⁶

In federal regulation, an infringement notice may be used as an alternative to criminal or civil penalty proceedings. The ALRC Principled Regulation report recommended that infringement notices should apply in the case of criminal penalty schemes, only to ‘minor offences of strict or absolute liability’⁸⁷ and in the case of civil penalty schemes, only to ‘minor contraventions in which no proof of a fault element or state of mind is required’.⁸⁸

The use of infringement notices has, however, extended beyond what appears to have been contemplated in the ALRC Principled Regulation report. In 2004 ASIC acquired power to issue infringement notices not only for minor offences but for alleged breaches of continuous disclosure provisions with a penalty of up to \$100,000. Since then the regime has expanded further and infringement notices are currently available in relation to the following areas of the corporate law:

- certain unconscionable conduct and consumer protection provisions of the ASIC Act;
- strict liability offences and certain civil penalty provisions under the Credit Act; and
- breaches of the Market Integrity Rules, Derivative Transaction Rules and Derivative Trade Repository Rules.

⁸⁵ ALRC Principled Regulation report, n 2, p. 78

⁸⁶ Rees A, ‘*Infringement notices and federal regulation: wolves in sheep’s clothing?*’ (2014) 42 Australian Business Law Review 276.

⁸⁷ ALRC Principled Regulation report, n 2, Rec 12-1.

⁸⁸ *Ibid.*, n 2, Rec 12-2.

Under the Credit Act, there are over 100 civil penalty provisions and almost half of those provisions are currently subject to the applicable infringement notice regime. Infringement notice regimes are also available for significant offences under other Acts such as the Competition and Consumer Act. The types of contraventions for which infringement notices may be issued under these Acts do not always sit easily within the principles earlier enunciated by the ALRC.

ASIC has made relatively frequent use of the infringement notice powers in relation to alleged contraventions of significant (ie non-minor) provisions.⁸⁹ ASIC has used infringement notices for breaches of continuous disclosure obligations 37 times since their introduction, issuing approximately 3 per year on average. The number of infringement notices issued to a party at one time ranged from 1 to 3. The penalty amounts have ranged from \$33,000 to \$300,000 (by way of three notices in relation to 3 contraventions). ASIC has issued infringement notices under the ASIC Act for breaches of consumer protection provisions, 64 times since their introduction, issuing approximately 13 per year on average. The penalty amounts have ranged from \$2,040 to \$42,000. The number of infringement notices issued to a party at one time ranged from 1 to 4. Under the National Credit Act, ASIC has issued infringement notices, approximately 38 per year. The penalty amounts have ranged from \$5,500 to \$1.35M in total. The number of infringement notices issued to a party at one time ranged from 1 to 58.⁹⁰

Recommendation 44

The provisions outlined in Table D should be made infringement notice provisions.

As noted in Positions Paper 7, the use of infringement notices in the corporate law has been previously criticised by stakeholders, including the ALRC and the Law Council of Australia. The ALRC Principled Regulation report criticised the then CLERP 9 proposal for an infringement notice regime for contraventions of continuous disclosure provisions as they involved subjective judgments as to the materiality of information and so are contraventions involving a ‘state of mind’ element.⁹¹ The ALRC also raised concerns with the size of the penalties that could be levied under infringement notices. The Law Council of Australia has previously stated:

“Infringement notices in the area of white-collar crime have been a contentious issue. We as a body have always opposed the use of infringement notices. We believe it is lazy regulation. It does not involve a finding of culpability. It does not provide guidance to the community as to what conduct should be proscribed or not. We note that the ALRC does not support infringement notices in areas such as this, and we would continue our opposition to infringement notices and our opposition to a broadening of the application of infringement notices in the corporations’ context.”⁹²

In its submission to the Taskforce’s Positions Paper 7, the Law Council reiterated its opposition to expansion of the infringement notice regime:

“...infringement notices are suitable for relatively minor offences of the strict or absolute liability type and where a high volume of contraventions may be expected and/or it is easy to assess guilt/innocence. Civil penalty provisions, by their very nature, are inherently not of

⁸⁹ See in relation to Market Integrity Rules, for example, Reegan Grayson Morison and Ian Ramsay “Enforcement of ASIC’s market integrity rules: An empirical study”, *Australian Journal of Corporate Law*, Vol. 30, No. 1, pp. 10-33, 2015.

⁹⁰ Figures as at December 2016 (data supplied to the Taskforce by ASIC)

⁹¹ ALRC Principled Regulation report.

⁹² Page 71 Senate Standing Committee on Economics ‘*Lifting the fear and suppressing the greed – penalties for white-collar crime and corporate and financial misconduct in Australia*’ March 2017.

this type and we do not support ASIC's view that the provisions listed in Annexure D are suitable for infringement notices.”

The AICD opposed any expansion of the infringement notice regime on similar grounds:

“The AICD agrees with the positions stated previously by the Law Council of Australia and the ALRC. The imposition of infringement notices is a form of lazy regulation, and undermines the credibility and transparency of regulatory action. ASIC should be sufficiently resourced and equipped to pursue these contraventions through the Courts. The Courts have a critical role to play in the proper functioning of the corporate regulatory system.”

The Financial Services Council also raised concerns in its submission to the Taskforce:

“In our view, there should be appropriate controls and accountability on the use of infringement notice and penalty notice powers, particularly given the lower standard of proof and reputational consequences for licensees (and that the matters alleged in an infringement notice or penalty notice are not required to be proved in a court).”

The ALRC also noted some disadvantages, some of which have been echoed in submissions to the Taskforce:

“Disadvantages previously noted by the ALRC include the lack of court scrutiny; the risk that innocent people will pay the amount specified in the infringement notice to avoid ‘the expense of contesting proceedings’; the possibility of discriminatory enforcement against vulnerable members of the community; and the possibility of ‘net-widening’ that is, automatic issue of an infringement notice in circumstances which would otherwise have been dealt with by a caution or warning.” (par. 12.10)

The Taskforce is, however, mindful of the fact that infringement notices, properly utilised, can have benefits for regulators, the regulated and the public. In its principled regulation report, the ALRC, citing the NSW Law Reform Commission, noted:

“Infringement notices can prevent minor cases reaching court and save time and money both for the offender and the criminal justice system. The avoidance of a conviction results in reduced stigma. The system can be automated, is highly efficient and raises significant revenue. The penalty payable is considerably less than the maximum available were the matter to be dealt with in court.” (par. 12.9)

Against this background, the challenge for the Taskforce has been in establishing appropriate parameters around which contraventions are appropriate and which are not, for the application of the infringement notice regime.

For criminal offences, the question for the Taskforce was more straightforward, as it agrees with the ALRC principle that infringement notices or like schemes should generally apply only to strict and absolute liability offences. This is reflected in the Taskforce’s recommendation (above) that such offences be subject to the existing ‘penalty notice’ regime under section 1313 of the Corporations Act.

In relation to civil penalty provisions, the Taskforce has found the question considerably more difficult. While the Taskforce does not accept the proposition that civil penalty provisions are inherently unsuitable for application of the infringement notice regime, it does believe that their application should be subject to limitations, broadly in line with ALRC and AGD endorsed principles but having regard to the fact that the legislature has in the past considered it appropriate to depart from those principles to some extent by applying infringement notice regimes to a broader set of provisions.

With these considerations in mind the Taskforce has compiled a list of provisions, narrower than that consulted on, which it recommends be made infringement notice provisions. The Taskforce has

avoided including provisions that would necessarily involve complex adjudications of fact. Not all the provisions included can be described as ‘minor’ but the Taskforce’s intention, in including more significant provisions, is that ASIC would choose to issue infringement notices only in respect of contraventions toward the minor end of the scale of severity. This result should be encouraged by adoption of the Taskforce recommendation that penalty amounts be limited to 12 penalty units for individuals and 60 penalty units for corporations. Due to this limitation, ASIC can be expected to reserve the use of the regime for minor contraventions, leaving them to pursue civil penalties for more significant contraventions.

All provisions recommended for inclusion as infringement notice provisions are listed in Table D.

Recommendation 45

Infringement notices should be set at 12 penalty units for individuals and 60 penalty units for corporations for any new infringement notice provisions.

The Taskforce recommends that infringement notice amounts should generally be set at the prescribed maximums in the AGD guide: 12 penalty units for individuals and 60 penalty units for corporations. Any existing infringement notice provisions, including those amounts that are above the AGD guide (that is, continuous disclosure, Credit legislation) will remain unchanged.

The AGD guide provides that infringement notices may be employed for relatively minor offences where a high volume of contraventions is expected, a penalty must be imposed immediately to be effective, and/or it is easy to make an assessment of guilt or innocence.⁹³ It further notes that infringement notice schemes should not require proof of fault and so are more suitable for strict or absolute liability offences.⁹⁴ Further the guidelines state that the “amount payable under an infringement notice scheme should not exceed 12 penalty units for a natural person or 60 penalty units for a body corporate.”

The penalties available under most existing infringement notice provisions under ASIC-administered legislation are 12 penalty units for individuals (currently \$2,520), 60 penalty units for corporations (currently \$12,600) or a specified proportion of the maximum penalty that could be levied by a Court. One exception is the continuous disclosure regime, where infringement notice penalties are graduated, being \$33,000, \$66,000 or \$100,000, depending on whether the entity is a Tier 1, 2 or 3 entity in terms of market capitalisation and whether it is the entity's first contravention.

Under the Credit Act and Regulations, infringement notice penalties imposed for civil penalty provisions must not exceed one-fortieth of the maximum penalty that a court could impose, and must not exceed one-fifth of the maximum penalty that a court could impose for strict liability criminal offences. As the maximum civil penalty under the Credit Act is generally 2,000 penalty units, the individual infringement notice amount is 50 penalty units and for corporations, 250 penalty units. For consistency, this ratio will apply to any new infringement notice provisions under the Credit Act.

⁹³ AGD Guide, at [6.2.1].

⁹⁴ AGD Guide, at [6.2.1].

In consultations, a number of stakeholders (NCPA, CHERPA) supported an alternative ‘default proportion approach’, the current Credit Act model for determining the quantum of INs. It appears some stakeholders may have misunderstood the effect of this approach, if the recommendations to increase the maximum criminal and civil pecuniary penalties proceed. For example, a one-fortieth ratio for an individual civil contravention will be 62.5 penalty units under the new maximum of 2,500 penalty units. This is significantly higher than the proposed 12 penalty units and the Taskforce considers this amount would be inappropriate for an administrative action by ASIC. The Taskforce maintains the view that 12 and 60 penalty units is the appropriate measure.

Peer Disciplinary Review Panels

In Positions Paper 7, the Taskforce sought views from interested stakeholders on establishing a peer review panel for financial services and credit sectors in a manner similar to the Markets Disciplinary Panel. The Taskforce notes that ASIC has since established the Financial Services and Credit Panel (FSCP) to assist ASIC with making administrative decisions relating to financial services and credit activities. The Taskforce notes that further consideration may be given to expanding the administrative functions of the FSCP in future but makes no recommendation at this time.

Table A: list of recommended increases to imprisonment penalties

Relevant criminal offence	Current criminal penalty	Recommended criminal penalty
Corporations Act 2001		
<i>Part 2D.1 – Duties and powers</i>		
184(1)	5 years	10 years
184(2)	5 years	10 years
184(3)	5 years	10 years
<i>Part 2D.6 – Disqualification from managing corporations</i>		
206A(1)	1 year	5 years
<i>Chapter 2M – Financial reports and audit</i>		
344(2)	5 years	10 years
<i>Part 5C.2 – Responsible entity of registered scheme</i>		
601FD(4)	5 years	10 years
601FE(4)	5 years	10 years
<i>Part 5D.4 – Duties of officers and employees of licensed trustee companies</i>		
601UAA(1)	5 years	10 years
601UAB(1)	5 years	10 years
<i>Chapter 6B – Rights and liabilities in relation to Chapter 6 and 6A matters</i>		
670A(3)	1 year	5 years
<i>Chapter 6D – Fundraising</i>		
708AA(10)	6 months	2 years
708A(9)	6 months	2 years
727(1)	5 years	10 years
728(3)	5 years	10 years
<i>Chapter 7 – Financial services and markets</i>		
<i>Part 7.2 – Licensing of financial markets</i>		
792D(1)	6 months	2 years
<i>Part 7.3 – Licensing of clearing and settlement facilities</i>		
821C(1)	6 months	2 years
821C(3)	6 months	2 years
821D	6 months	2 years
821E(2)	50pu	2 years

Relevant criminal offence	Current criminal penalty	Recommended criminal penalty
Part 7.5 – Compensation regimes for financial markets		
892K	2 years	5 years
Part 7.5A – Regulation of derivative transactions and derivative trade repositories		
905A	500pu	2 years
907A	500pu	2 years
Part 7.6 – Licensing of providers of financial services		
911A(1)	2 years	5 years
911B(1)	2 years	5 years
911C	1 year	2 years
912C(3)	6 months	2 years
912D(1B)	1 year	2 years
912E(1)	6 months	2 years
Part 7.6 – Licensing of providers of financial services		
920C	6 months	5 years
Part 7.7 – Financial services disclosure		
952C(3)	2 years	5 years
952D(1)	5 years	10 years
952D(2)	5 years	10 years
952F(2)	5 years	10 years
952F(3)	5 years	10 years
952F(4)	5 years	10 years
952L(1)	5 years	10 years
952L(2)	2 years	5 years
Part 7.8 – Other provisions relating to conduct		
982D	6 months	2 years
991B(2)	6 months	1 year
991E(1)	6 months	1 year
991E(3)	6 months	1 year
993B(3)	5 years	10 years
993C(3)	2 years	5 years
Part 7.9 – Financial product disclosure – issue, sale and purchase		
Part 7.9 Division 2 – Product disclosure statements		
1012DAA(10)	6 months	2 years

Relevant criminal offence	Current criminal penalty	Recommended criminal penalty
1012DA(9)	6 months	2 years
Part 7.9 Division 3 – Other obligations of the issuer		
1017E(3)	2 years	5 years
1017E(4)	2 years	5 years
1017G(1)	2 years	5 years
Part 7.9 Division 7 - Enforcement		
1021C(3)	2 years	5 years
1021D(1)	5 years	10 years
1021D(2)	5 years	10 years
1021J(2)	2 years	5 years
1021J(3)	2 years	5 years
Part 7.12 – Miscellaneous		
1101E	1 year	2 years
1101F(1A)	1 year	2 years
1101F(1)	1 year	2 years
Part 9.3 - Books		
1307(1)	2 years	5 years
1307(2)	2 years	5 years
Part 9.4 - Offences		
1308(4)	5/25pu	2 years
1308(8)	5/25pu	5 years
1310	5 penalty units	2 years
Australian Securities and Investments Commission Act 2001		
Part 3 – Investigations and information gathering		
ASICA 64(1)	2 years	5 years
ASICA 64(2)	3 months	2 years
ASICA 65(2)	6 months	1 year
ASICA 66(1)	1 year	2 years
National Consumer Credit Protection Act 2009		
Chapter 2 – Licensing of persons who engage in credit activities		
Part 2.4 Banning or disqualification of persons from engaging in credit activities		
NCCP 82(2)	2 years	5 years
Chapter 3 Responsible Lending - Part 3.6A Miscellaneous Rules		

Relevant criminal offence	Current criminal penalty	Recommended criminal penalty
NCCP 160D(2)	2 years	5 years
Chapter 6 Compliance and Enforcement		
NCCP 291(1)	2 years	5 years

Proposed maximum penalty ⁹⁵ (individual/corporations)
3 months' imprisonment 30 penalty units / 300 penalty units
6 months' imprisonment 60 penalty units / 600 penalty units
1 year imprisonment 120 penalty units / 1,200 penalty units
2 years' imprisonment 240 penalty units / 2,400 penalty units
5 years' imprisonment 600 penalty units / 6,000 penalty units
General formula does not apply, as discussed above 10 years' imprisonment 4,500 penalty units or x3 benefits / 45,000 penalty units or x3 benefits or 10% annual turnover

⁹⁵ There will be exceptions to this general rule for setting criminal pecuniary penalties.

Table B: Complete list of new ordinary offences

Section	Current criminal penalty	New ordinary offence
<i>Part 2D.5 – Public information about directors and secretaries</i>		
205G(1) (strict liability)	10pu and/or 3 months 50pu	240pu and/or 2 years 2400pu
205G(3) (strict liability)	10pu and/or 3 months 50pu	240pu and/or 2 years 2400pu
205G(4) (strict liability)	10pu and/or 3 months 50pu	240pu and/or 2 years 2400pu
<i>Part 6.1 – Prohibited acquisitions of relevant interests in voting shares</i>		
606(1) (absolute liability)	25pu and/or 6 months 125pu	600pu and/or 5 years 6000pu
606(2) (absolute liability)	25pu and/or 6 months 125pu	600pu and/or 5 years 6000pu
606(4) (absolute liability)	25pu and/or 6 months 125pu	600pu and/or 5 years 6000pu
<i>Chapter 6C – Information about ownership of listed companies and managed investment schemes</i>		
671B(1) (strict liability)	25pu and/or 6 months 125pu	240pu and/or 2 years 2400pu
<i>Chapter 2M – Financial reports and audit</i>		
286 (strict liability)	25pu and/or 6 months 125pu	240pu and/or 2 years 2400pu
307A (strict liability)	50pu 250pu	240pu and/or 2 years 2400pu
<i>Part 7.8 – Other provisions relating to conduct</i>		
989CA(strict liability)	50pu 250pu	240pu and/or 2 years 2400pu

Table C: Complete list of new civil penalty provisions

Corporations Act
601ED(5)
670A
727
728
791A
792B
820A
821B
853F(2)
904C(1)
905A
911A
911B
912D
920C(2)
922M
941A
941B
946A
952E
952H
981B
981C
993D (3)
1012A
1012B
1012C
1017BA
1017BB(1)
1020A(1)
1021E
1021G

1309(2)
General Licensee Obligations
792A(a), (c), (d), (e), (f), (g), (h), (i)
821A (aa), (a), (c), (d), (e), (f), (g), (h)
904A(b), (c)
912A(a), (aa), (ca), (d), (e), (f), (g), (h), (j)
Credit Act s47 (a), (b), (e), (f), (g), (h), (i), (j), (k), (l), (m)
Insurance Contracts Act 1984
13(1)
33C(1)
Credit Code Obligations
24
39B(1)
154
155
156(1)
174(3)
179U
179V

Table D: Complete list of new infringement notice provisions

Current civil penalty provisions (Corporations Act)
188(1) and (2)
962P
962S(1)
963E(1) and (2)
963G(1)
963J
963K
964A(1)
964D(1) and (2)
964E(1)
985E(1)
985J(1)
985J(2)
985J(4)
985L
Proposed civil penalty provisions (Corporations Act)
792B
821B
912D
941A
941B
946A
1012A
1012B
1012C
1017BA
Current civil penalty provisions (National Consumer Credit Protection Act)
31(1)
70(1)
124A(1)
124B(1)
133AC(2)
133AD(2)
133AE(2)
133BC(1)
133BD(1)

133BG(1)
133BH(3)
133BJ(1)
133CA(1)
133CB(1)
133CC(1)
133DB(1)
133DC(2)
133DD(2)
133DE(1) and (2)
160B(1)
160C(1)
160E(2) and (3)
Current and proposed civil penalty provisions (National Consumer Credit Code)
17(3), (4), (5), (6), (8), (9), (11), (15), (15A)
23(1)
24
32A
39B
32AA(2)
34(6)
35(1)
72(4)
177B(4)
Insurance Contracts Act
33C

Appendix A: Principles for the review of penalties

Penalties should represent a credible deterrent

An important principle in any penalty regime is that penalties should have the capacity to deter prospective offenders from the objectionable conduct. This is especially so in respect of civil penalties, the purpose of which is to set a price for offending behaviour sufficient to promote compliance (see below). The ALRC Principled Regulation report implicitly recognised this principle in making its recommendation that:

“In setting civil penalties, legislators should have regard to whether the level set will achieve the aim of deterrence, which is the principal purpose of civil penalties.”⁹⁶

The High Court recently emphasised in the Fair Work Decision that the primary purpose of civil penalties is ‘primarily if not wholly protective in promoting the public interest in compliance’.⁹⁷ The Taskforce considers it important that courts have the flexibility to meet this objective when imposing penalties. There should be power to properly ‘price’ the offending behaviour for the purposes of deterrence, especially where large gains are made as a result of a contravention or where the offender’s capacity to pay is very substantial:

“The emphasis in deterrence theory is both on pricing the illegal behaviour and having a penalty large enough to deter a well-resourced corporate offender. If large gains can be made then the maximum ought to reflect this. This is the purpose of a high maximum such as the \$10 million penalty for a breach of Part IV of the TPA.”⁹⁸

The question can reasonably be asked as to whether there should be any upper limits on penalties at all. In the United Kingdom there are no maximum limits on amounts that can be imposed in respect of comparable contraventions to those under ASIC-administered legislation. The Taskforce has, however, stopped short of adopting this approach. Although the Australian courts are well versed in imposing sentences from first principles (see for example *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* [2016] FCAFC 181, where the Full Court of the Federal Court calculated a penalty largely by reference to profit made, after concluding that “in a practical sense, the overall maximum penalty was so great that there was no maximum penalty”), the Taskforce’s view is that a nominal maximum provides valuable guidance to courts faced with the task of imposing a penalty appropriate to the case before them.

The Taskforce believes, however, that nominal penalty maximums (by which is meant maximums expressed in penalty units) should be supplemented, at least in respect of corporations, with amounts limited only by reference to benefit gained or loss avoided as a result of particular contraventions, and by reference to a portion of annual turnover. This would ensure that there is flexibility in the regime sufficient to prevent circumstances arising where a fixed maximum expressed in penalty units would not be large enough to deter the offender due to the size of the benefit, for example.

⁹⁶ Recommendation 26-1.

⁹⁷ *Commonwealth v Director, Fair Work Building Industry Inspectorate* [2015] HCA 46; (2015) 326 ALR 476 at 490 [55] referring to French J in *Trade Practices Commission v CSR Ltd* [1990] FCA 521; (1991) ATPR 41-076

⁹⁸ Performance of ASIC report, page 798.

Penalties should reflect gravity of conduct, as well as the purpose for which they are imposed (relationship of criminal and civil penalties)

Penalties available for criminal offences should reflect the fact that this kind of conduct is of a more serious nature than for civil contraventions, however, this principle should be applied subject to the considerations that:

1. For individuals, the effect of imprisonment and conviction must be taken into account, as must the fact that liability is, potentially, to imprisonment *and* the maximum fine.
2. Criminal fines, unlike civil penalties, may be converted to imprisonment in some cases.
3. The legislation allows for both civil *and* criminal penalties to be imposed in respect of the *same* conduct (this is rarely occurs in practice but nevertheless must be taken into account in assessing the comparative liability that results from engaging in particular conduct).

These are the kind of factors that likely led the ALRC Principled Regulation report, as well as the AGD guide, to recognise that financial penalty maximums for civil contraventions may, in some cases, exceed those for criminal offences involving similar conduct, especially in respect of offending by individuals. However, the Taskforce notes that the ALRC expressed considerable doubt about the justification for this principle in respect of offending by corporations, who are not subject to imprisonment and to whom the consequences of conviction more broadly are less severe.⁹⁹

There are many instances in Commonwealth legislation where civil penalty maximums are greater than criminal penalty maximums in respect of comparable conduct for both individuals and corporations. In addition to the principles outlined above, this may reflect the view, now expressly endorsed by the High Court in the Fair Work case (see above), that the purpose of civil penalties is primarily if not wholly about deterrence (as opposed to criminal penalties which, as well as deterrence, involve considerations of punishment and retribution). The high maximums allowed for civil penalties may, on that view, be directed at ensuring the courts have discretion to impose a penalty that meets “the price of deterrence” in any given circumstance.

Nevertheless, the Taskforce shares some of the misgivings expressed by the ALRC regarding the justification for the difference between civil and criminal penalty maximums in respect of corporations. In light of the matters outlined above, the Taskforce does not go so far as to suggest parity in all cases between maximum civil and criminal penalties for corporations. On the other hand, the concern could be addressed somewhat by the Taskforce’s adoption of the view that criminal penalty maximums for corporations should generally represent a higher multiple of the maximum for individuals than is currently the case. The suggestion is that generally the multiple for corporations should be 10 times that for individuals.

The penalties regime should be clear and consistent

The penalties framework for corporate, financial services and market misconduct should be transparent and consistent, and avoid, as far as possible, unnecessary complexity. Public confidence is more likely in a system that is clear and easy to understand.

⁹⁹ See conclusion at paragraph 26.64 of the report.

Challenges arise when considering the regimes administered by ASIC as they span across different legislation, covering hundreds of offences and types of misconduct some of which overlap. The drafting styles adopted differ among provisions in the legislation due to the fact that they have been implemented and amended at different points in time. This applies even within the Corporations Act. An example can be found in the directors' duties provisions in sections 181 to 184. Sections 181 to 183 are drafted as simple civil penalty provisions. Section 184 operates to convert sections 181 to 183 to criminal offences where dishonesty or recklessness are present. This approach is not taken uniformly throughout the Act. In relation to insider trading, for example, a contravention of the one provision can give rise to a criminal offence and a civil penalty consequence. The latter approach leaves the choice of penalty to the regulator with the consequence that there is less clarity for the regulated as to the consequences of engaging in different forms of misconduct. The Taskforce would prefer that the consequences for engaging in different forms of misconduct was always clear from reading the legislation itself, however, this would require revision to a range of provisions to address this kind of issue and others to ensure consistent application of the fault elements in the *Criminal Code Act 1995* (Cth) (Criminal Code). Such an exercise is beyond the scope of this review, although the Taskforce considers there would be merit in it.

Despite the inconsistency in the legislation, the Taskforce has sought, wherever possible and appropriate, to develop recommendations that adopt a simple, standardised approach to penalties and apply a consistent rationale. One result of this approach is that the Taskforce has recommended that criminal fines for Corporations Act offences should be determined by reference to a standard formula calculated on the basis of the number of months of a maximum term of imprisonment times 10 for individuals and multiplied by a further 10 for corporations. The formula approach would represent an increase in maximum criminal fines for most offences and provides for consistency as offences with the same maximum term of imprisonment will have the same applicable fines, which is not currently the case. This would replace a diffuse regime that sets maximum fines on an inconsistent basis across the legislation.

The Taskforce also considers that as far as possible similar conduct should give rise to similar consequences. Accordingly, it has recommended that criminal penalties for the most serious criminal offences in the Corporations Act should be increased to the highest terms of imprisonment and fines available under that Act, which are currently applicable to market misconduct and insider trading. Offences of comparable seriousness given the nature of the offending and/or the consequences for the market or financial consumers should give rise to the same penalties. This forms the basis for a number of recommendations of this review.

The Taskforce noted the increases to financial penalties proposed for the Australian Consumer Law following a review of that law.¹⁰⁰ In addition, the Taskforce notes the proposals for substantial penalties in relation to the BEAR. These, together with other provisions of the Competition and Consumer Act, broadly provide for maximum penalties for individuals of around \$500 000, and for Corporations of around \$10 million (or 3 times benefit or 10% of annual turnover). The Taskforce considers that these figures represent a sensible benchmark and that the alignment of

¹⁰⁰ Australian Consumer Law Review Final Report, March 2017, <http://consumerlaw.gov.au/review-of-the-australian-consumer-law/final-report/>.

ASIC-administered legislation across these broadly comparable regimes would achieve consistency and simplicity.



Chapter 8 – ASIC’s directions power

ASIC ENFORCEMENT REVIEW

Summary of recommendations

<i>Chapter 8: ASIC's directions powers</i>	
Number	Description
46	ASIC should have the power to direct financial services or credit licensees in the conduct of their business where necessary to address or prevent risk to consumers.
47	The directions power should be triggered where ASIC has reason to suspect that a licensee has, is or will contravene AFS or credit licensing requirements (including relevant laws).
48	ASIC should be able to make an interim direction without a hearing, for a period of time, if the direction is to cease a type of activity and a delay in making a direction would be prejudicial to the public interest.
49	A licensee should have an opportunity to be heard before the direction is made, and the ability to review a direction at the Administrative Appeals Tribunal.
50	The requirement to comply with a direction should be an obligation of licensees, and there should be a civil penalty provision for non-compliance.

8. ASIC's directions power

Overview

A person who carries on a financial services business in Australia must hold an AFS licence, subject to certain exemptions, including where the person provides a financial service as a representative of an AFS licensee.¹⁰¹ Similarly, a person must not engage in a credit activity unless the person holds an Australian credit licence, or engages in the activity as a credit representative or as an employee or director of a credit licensee or related body corporate.¹⁰²

When it grants a licence, ASIC can require that a licensee put in place internal systems or restrict its activities in appropriate ways. However after a licence is granted, imposing such requirements or restrictions can be slow, resource intensive and difficult.

The Taskforce has reviewed ASIC's existing powers to modify an AFS or credit licensee's ongoing systems and conduct after the relevant licence has been granted. These powers include:

- Varying, suspending or cancelling the licence if ASIC can establish the licensee has breached the law, and the breach justifies this action;
- Applying to the court for an injunction; or
- Negotiating an enforceable undertaking with the licensee (with their cooperation).

Current status of ASIC's directions powers

ASIC's existing powers to require licensees to adopt internal systems or to restrict their activities have three shortcomings. First, applying to a court for an injunction involves significant time, resources and costs in investigating and preparing a case to the required standard to commence court proceedings. In urgent matters involving a licensee, there is utility in providing ASIC with an efficient and quick mechanism to require a licensee to put in place or modify internal systems or restrict its activities in appropriate ways to address risks to consumers.

Secondly, the resources and procedural requirements necessary to impose additional conditions, or to suspend or cancel a licence¹⁰³ can result in delay between concerns arising and ASIC achieving a protective outcome. This can leave financial consumers at risk in the interim period as surveillance and hearings take place.

Thirdly, enforceable undertakings must be agreed to by a licensee and are generally negotiated as an alternative to ASIC exercising its administrative powers or initiating court proceedings. This requires acknowledgement by the licensee of ASIC's concerns. The outcome also depends on the strength of the evidence available to support ASIC's concerns and the nature of the alternative remedies that could be pursued by ASIC.

Particular difficulties arise where a licensee has taken some steps to rectify identified compliance concerns but ASIC remains concerned that those steps are not sufficient to ensure that there will not

¹⁰¹ Section 911A of the Corporations Act.

¹⁰² Section 29 of the Credit Act.

¹⁰³ Generally, ASIC may only suspend, cancel or make changes to the licence after giving the licensee an opportunity to appear, or be represented, at a private hearing before ASIC, and to make submissions to ASIC in relation to the matter. Additionally a licensee may apply to the AAT for a review of any decision made by ASIC.

be further breaches by the licensee of its obligations, or additional measures are required to ensure that the impact on clients or former clients is identified and, where necessary, remediated. For example a licensee may make appropriate amendments to its systems and processes to address how a breach occurred but may not have established an appropriate remediation program to assess whether compensation is payable to consumers affected by the breach. The case study below illustrates another potential scenario where ASIC might need a directions power to minimise risks to consumers.

Case study

ASIC received a complaint alleging that an authorised representative (AR) of an AFS licensee had misappropriated substantial funds from a client's account and put these to his own use. The complaint further raised a concern that the AR may seek to transfer funds from other client accounts (to which he had access as their adviser) to cover the shortfall in the first client's account.

ASIC commenced an investigation into the alleged conduct and advised the AR that it intended to inform the AR's licensee of the allegations and ASIC's investigation, pursuant to s916G of the Corporations Act. The AR informed the licensee himself, in response to which the licensee advised ASIC that it had suspended the AR from dealing with clients. ASIC requested that the licensee conduct a review of payments out of the AR's clients' accounts to identify any other potentially misappropriated funds, which the licensee in this case agreed to do.

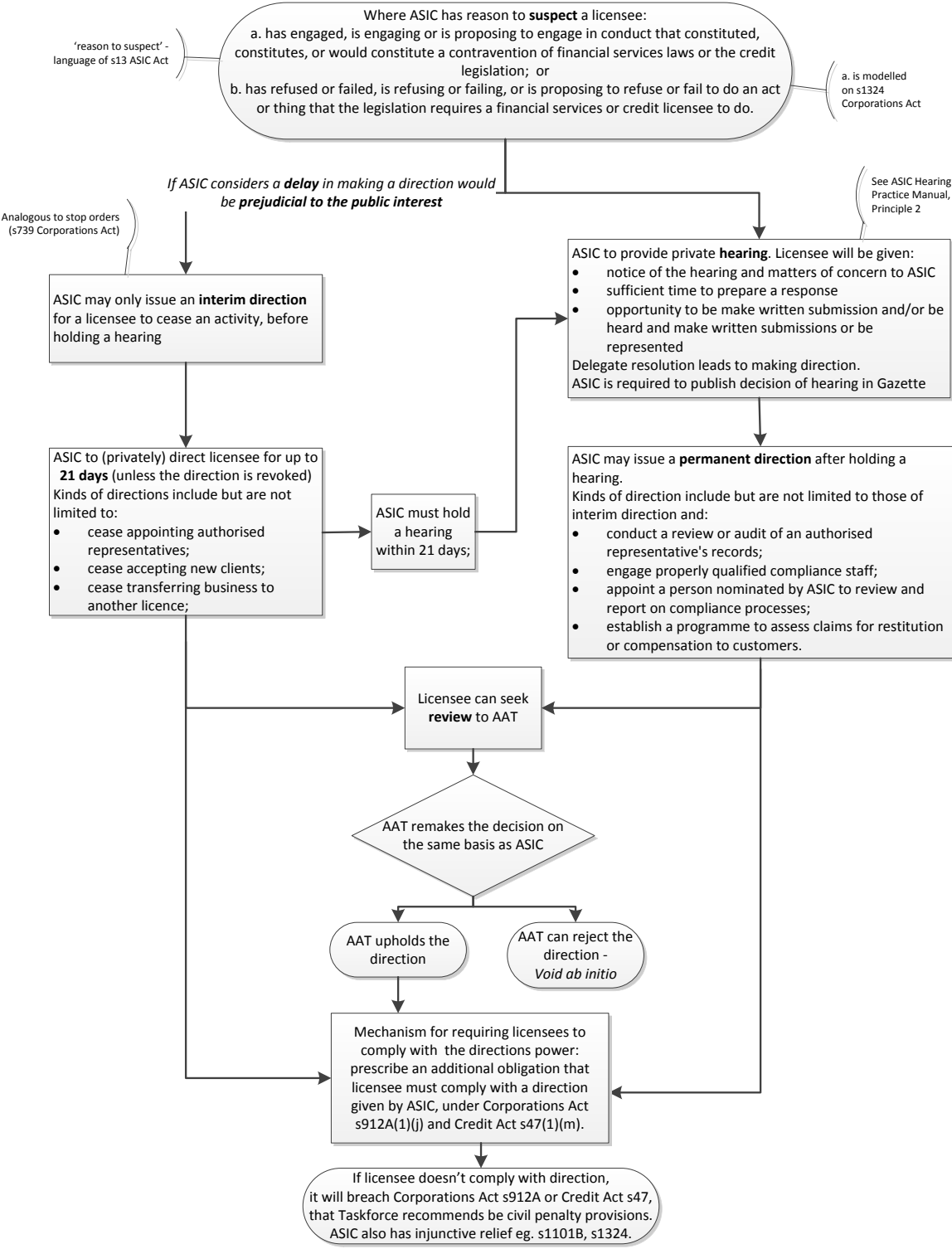
However, without the licensee's agreement, there is no clear basis upon which ASIC could have required the licensee to undertake this review. In circumstances of this nature, a directions power could enable ASIC to direct the licensee to take urgent action that may be necessary to protect clients' interests.

Triggering the directions power

The Taskforce considers that, to the extent practicable, ASIC should be able to require compliance with AFS or credit licence obligations in real time, and that the regulator should be given powers to direct licensees to take or refrain from taking actions where appropriate for this purpose, particularly where there is a need to protect financial consumers.

The proposed process for the directions power is explained in the recommendations below, and briefly illustrated in Figure 1.

FIGURE 1: PROPOSED ASIC DIRECTIONS POWER



Recommendation 46

ASIC should have the power to direct financial services or credit licensees in the conduct of their business where necessary to address or prevent risks to financial consumers.

The Taskforce recommends that ASIC should be able to give a direction to a financial services or credit licensee in the conduct of their financial services or credit business where necessary to address or prevent risks to financial consumers. Such a power will provide ASIC with an efficient mechanism to require a licensee to put in place or modify internal systems or restrict activities in appropriate ways to prevent detriment to consumers.

There were mixed views about the necessity for a directions power, with some stakeholders suggesting that ASIC has sufficient alternate powers such as injunctions, and that delays due to procedural fairness and evidence gathering are appropriate. It was also noted, however, that a directions power could help ASIC pursue graduated engagement with stakeholders, with this power filling the middle ground between informal engagement and more serious measures such as licensing action, court injunctions or enforceable undertakings.

Consistent with the principles guiding the ASIC Enforcement Review, the Taskforce believes ASIC should have a range of administrative powers appropriate to the efficient exercise of its functions. The Taskforce considers that a directions power could aid ASIC in graduated engagement, as the directions power can be triggered by a lower threshold of evidence and carries less serious consequences compared to a licence variation, suspension or cancellation.

Some stakeholders argued that a power directing credit licensees was not necessary as there is a smaller potential for credit customers to be harmed by being offered an unsuitable product compared to the potential loss of wealth that financial services consumers may face. The Taskforce considers, however, that the risks and potential for harm are equivalent. An unsuitable loan can have serious consequences particularly if it results in the credit customer defaulting, and systemic poor conduct by a credit licensee with a large number of credit representatives can impact many customers. Accordingly, the Taskforce recommends that the directions power apply to AFS and credit licensees.

The legislation should set out the types of directions that ASIC can make including but not limited to:

- Cease appointing authorised representatives;
- Cease accepting new clients for a period, or until a specified condition is met;
- Cease transferring business to another licence;
- Conduct a review or audit of an authorised representative's records;
- Engage properly qualified compliance staff;
- Appoint a person nominated by ASIC to review and report on compliance processes; and
- Establish a suitable programme to remediate clients, including assessing claims for restitution or compensation to customers.

Setting out a list of possible directions in the legislation will provide certainty for industry and ASIC about the types of directions that may be given. While there were mixed views on the legislation

providing for additional matters to be included by regulation, the Taskforce considers this will enable the legislation to be updated to take into account new circumstances and risks.

Public consultation raised concerns about giving ASIC the ability to make a direction requiring a licensee to 'cease accepting new clients' on the basis that it could threaten the viability of the business. To clarify the intent of this direction the Taskforce modified it as above, limiting its duration to a period set out in the direction, or until a specified condition has been met. Further, when making any direction ASIC will need to ensure that the decision, as for all administrative decisions, is made in furtherance of the objectives of the relevant legislation and is for a protective purpose. There was also concern that a direction to 'establish a suitable program for restitution or compensation to customers' could interfere in business decisions and threaten the viability of the business. The Taskforce notes that only the court would be able to direct payments to be made and the amount of any such payment. The directions power proposed by the Taskforce is intended to enable ASIC to ensure that any remediation program established by a licensee provides a suitable process for addressing the impact of a breach on customers including, for example notifying customers about the program, identifying potential claimants, processes for assessing claims and rights to appeal decisions made where appropriate.

In considering whether a power to give a direction to AFS and credit licensees is appropriate the Taskforce noted the product intervention power (PIP) that is currently being developed. Some stakeholder submissions raised concerns of overlap between the two powers; however the Taskforce notes that the focus of the directions power should be on regulating licensee conduct whereas the PIP's focus is on financial products. To further distinguish the powers, the preliminary suggestion of a direction to require licensees to 'cease making specific representations about products' has been removed. The Taskforce notes however, when the PIP legislation has been finalised there may be utility in further considering a direction to require licensees to cease providing or marketing a product, as there may be scenarios where there is a concern around licensee conduct rather than the actual product (which would be addressed by PIP). The Taskforce understands that the PIP legislation will be designed to address risks of, or actual incidences of, significant consumer detriment associated with a newly issued financial product, its features or method of distribution and could involve requiring licensees and product issuers to: amend product marketing and disclosure materials; impose consumer warnings and labelling changes; restrict how a product is distributed; and ban products. The directions power contemplated by the Taskforce should not be inconsistent with or undermine the limits to be imposed on the exercise of the proposed PIP.

Recommendation 47

The directions power should be triggered where ASIC has reason to suspect a licensee has, is, or will contravene financial services or credit licensing requirements (including relevant laws).

The Taskforce recommends that the power to make a direction should be triggered where ASIC has reason to suspect that an AFS or credit licensee:

- Has engaged, is engaging or is proposing to engage in conduct that constituted, constitutes, or would constitute a contravention of financial services laws or the credit legislation;¹⁰⁴ or

¹⁰⁴ As defined in section 761A of the Corporations Act and section 5 of the Credit Act respectively.

- Has refused or failed, is or is proposing to refuse or fail to do an act or thing that the legislation requires a financial services or credit licensee to do.

The Taskforce changed the threshold to “reason to suspect” considering that this would enable ASIC to address a range of concerns about a licensee’s business practices at an early enough stage in the investigative process to afford sufficient protection for financial consumers.¹⁰⁵ At the same time the Taskforce considers that before a direction is made a licensee should be given an opportunity to appear or be represented at a private hearing and make submissions about the matter, as is discussed in Recommendation 49 below. The lower threshold for triggering the power to make a direction is balanced against the additional procedural requirements before making the direction, and ASIC will be required to take into account submissions made by the licensee before making a direction.

There was negative stakeholder feedback to the initial position released for consultation that the power would be triggered where ASIC had “reason to believe” a licensee has, is, or will contravene financial services or credit licensing requirements. Other concerns included the lack of clarity around how ASIC will arrive at a conclusion concerning a licensee’s actual or proposed breach of the law. The Taskforce considers that these concerns will be adequately addressed by additional procedural requirements and safeguards it now recommends.

There was also concern that a direction that could be triggered by a licensee ‘proposing’ to engage in a breach would create uncertainty for licensees, given the general nature of the obligations a licensee must uphold. The Taskforce notes however that ‘proposing’ to engage in a breach is also a trigger for injunction and the Taskforce considers that preventing potential contraventions is important to ensure ASIC can make directions to prevent harm to financial consumers before it occurs.

Interim directions

Recommendation 48

ASIC should be able to make an interim direction without a hearing, for a period of time, if the direction is to cease a type of activity and a delay in making a direction would be prejudicial to the public interest.

The Taskforce recommends that ASIC should also be able to issue an interim direction for a specified period of time, before holding a hearing, but only if ASIC considers a delay in making a direction would be prejudicial to the public interest, as for interim stop orders.¹⁰⁶ These interim directions would be limited to directions to cease an activity, including:

- Cease appointing authorised representatives;
- Cease accepting new clients; and
- Cease transferring business to another licence.

ASIC would be able to privately direct the licensee for up to 21 days, but within that period must hold a hearing as is required for a permanent direction. If ASIC wants to make a direction permanent, it could then seek to do so following the hearing process. Both the procedure for review and the

¹⁰⁵ Note this language is used in section 13 of the ASIC Act to trigger general powers of investigation.

¹⁰⁶ Section 739(3) of the Corporations Act.

enforcement would be the same as for the permanent direction described under Recommendations 49 and 50.

Stakeholders held mixed views around the necessity for an interim direction power, with concerns raised about the extent of types of directions that could be made and the risk of reputational damage before the licensee can be heard. The recommended interim directions power limits the types of direction, is private and maintains appropriate avenues of appeal for licensees. The Taskforce considers an interim direction power will enable ASIC to act quickly in any urgent cases where a delay even for a hearing would be prejudicial to the public interest.

Licensee compliance with directions

Recommendation 49

A licensee should have an opportunity to be heard before the direction is made, and the ability to review a direction at the Administrative Appeals Tribunal.

The Taskforce recommends that a licensee should have an opportunity to be heard before a direction is made and also to have that decision reviewed, as is the existing process for ASIC administrative powers including licence variation, suspension or cancellation.

The Taskforce listened to concerns raised through the consultation process around licensee rights to procedural fairness under the preliminary position, with submissions suggesting ASIC would act as investigator and judge. The final recommended process would see ASIC provide licensees a private hearing. The licensee would be given notice of the hearing and matters of concern to ASIC and sufficient time to prepare a response, as well as opportunity to make written submission and/or be heard or be represented at the hearing.

The ASIC delegate at the hearing would then make a direction with the decision to be published in the ASIC Gazette. This process provides appropriate procedural fairness for licensees to be heard, acknowledging that “reason to suspect” is a lower threshold that will enable ASIC to act earlier in the investigative process to protect financial consumers. This balances the right of a licensee to be heard against the immediate risk of poor licensee conduct causing detriment to financial consumers.

If a licensee disagrees with the decision made they can seek a review at the AAT. They may also seek orders to stay the operation of the direction pending the AAT’s decision. The AAT could decide whether or not to stay the direction, and then review ASIC’s decision and in appropriate cases may make a new decision taking into account the same matters ASIC is required to consider in making its original decision. This addresses stakeholder concerns about a licensee’s right to review any direction made.

Recommendation 50

The requirement to comply with a direction should be an obligation of licensees, and there should be a civil penalty provision for non-compliance.

The Taskforce recommends that non-compliance with a direction (including an interim direction) should be a breach of an obligation of the licensee.

This can be achieved by requiring all financial services and credit licensees to comply with a direction given by ASIC, and making a failure to do so a civil penalty provision.¹⁰⁷

The Taskforce considers that this will provide an appropriate means to encourage licensees to comply with directions given by ASIC (subject to the licensee's right to seek a review in the AAT). Failure to comply will enable ASIC to take administrative action against the licensee to suspend or cancel the licence. This would be subject to the requirement to offer a hearing and usual considerations in administrative matters including the need to exercise the relevant powers to serve a protective purpose and to further the objectives of the legislative scheme.

A civil penalty for non-compliance with a direction would be consistent with the civil penalty provisions set out in Recommendation 43, where the Taskforce recommends most subsections of the licensee obligations be made civil penalty provisions.¹⁰⁸

Several stakeholders suggested that a sanction for a direction should be proportionate to the breach which enlivened the directions power. The Taskforce considers that in some cases, particularly where the failure to comply causes consumer detriment, it may be appropriate to impose a financial penalty for non-compliance. In addition, this will enable ASIC to take appropriate action where cancellation or suspension of the licence may not be warranted despite the seriousness of the failure to comply.

¹⁰⁷ For example, the Corporations Regulation 7.6.03B and the Credit Regulation 11 could be amended to require AFS and credit licensees respectively to comply with directions powers, using the regulation making power in subsection 912A(1)(j) of the Corporations Act and subsection 47(1)(m) of the Credit Act.

¹⁰⁸ Table C of Penalties chapter sets out the civil penalty provisions.