KPMG
Tower Two
Collins Square
727 Collins Street
Melbourne Vic 3008

GPO Box 2291U
Melbourne Vic 3001
Australia

ABN: 51 194 660 183
Telephone: +61 3 9288 5555
Facsimile: +61 3 9288 6666
DX: 30824 Melbourne
www.kpmg.com.au

Mr Warren Day
Executive Director, Assessment and Intelligence
ASIC
Australian Securities and Investments Commission
GPO Box 9827
Brisbane QLD 4001

Via Email: whistleblower.policy@asic.gov.au

18 September 2019

Dear Warren,

KPMG Response to Consultation Paper CP 321 Whistleblower Policies

We are pleased to have the opportunity to respond to Consultation Paper - *CP 321 Whistleblower Policies* (**CP321**) published by ASIC on Wednesday, 7 August (**the Guidance**). We welcome the proposed Guidance, which provides useful information on how to establish, implement and maintain a compliant whistleblowing policy.

The insights and recommendations in this submission draw on KPMG's practical experience in:

- advising Australian companies on developing better practice whistleblower policies and procedures;
- conducting complex investigations of whistleblowing reports;
- providing advice to organisations on how to appropriately respond to, investigate and remediate whistleblowing disclosures; and
- operating the "FairCall" whistleblower hotline service for clients since 1998.

This has enabled us to develop an understanding of the challenges faced by disclosers, as well as the complexities faced by recipients of disclosures. Our clients include large listed corporations as well as government agencies and not-for-profit organisations.

We agree with the objectives of the Guidance, and consider that a robust and clear whistleblowing policy, which is appropriately implemented and periodically reviewed, provides a solid platform for encouraging a 'speak up' culture within an organisation, as well as ensuring compliance with the whistleblower protections in the *Corporations Act 2001* (Cth) and the *Taxation Administration Act 1953* (Cth).

Attachment A to this letter provides KPMG's response to selected aspects of CP321. Our feedback relates to the following themes:

1. Cutting through complexity

We strongly support the better practice recommendation from ASIC that the policy be 'clear and easy to understand', written in plain English, and adopt a simple structure. Lengthy and overly detailed policies will be less accessible for disclosers and may have the unintended effect of discouraging reports. In Attachment A, we identify several areas where large volumes of detailed information could be moved to process documents, resulting in a simpler and more effective whistleblowing policy.

2. Expanding certain aspects of the Guidance

The Guidance would benefit from the inclusion of practical examples in cases where the law and the explanatory memorandum do not provide explicit direction. Given that the whistleblower protection legislation is new, and there is, as yet, no judicial guidance, many organisations are struggling to translate their obligations into practical compliance steps. In Attachment A, we provide examples of clarification points and further practical guidance for ASIC's consideration.

3. Clarifying Legal Obligations and Good Practice

We welcome ASIC's inclusion of 'good practice' guidelines for the many organisations that are seeking to move beyond mere compliance, but note that for an entity implementing a whistleblowing policy for the first time, it may take several years to reach this level of maturity. From the perspective of these entities, the Guidance would benefit from greater clarity as to which aspects of the Guidance are strictly required by the law, and which aspects are 'good practice'. In Attachment A, we provide examples and recommended edits to the Guidance.

4. Embracing Realistic Timeframes for adoption of 'good practice'

Many organisations have proactively implemented new whistleblowing policies after the enactment of the new whistleblower protections, without the benefit of the Guidance. Where the Guidance differs from the approach that these entities have taken, they will now need to undertake a second review process and obtain Board approval before 1 January 2019. For those organisations that have already published a revised policy and conducted training, making further amendments within a short period may create confusion. We suggest that the Guidance encourage organisations to implement the 'good practice' elements of the Guidance by 1 January 2021. This will allow sufficient time for organisations to adopt "good practice" in an authentic way, as part of the first annual review of their whistleblowing policy.

We would be pleased to discuss this submission further with you. Should you wish to do so please contact our subject matter experts Lauren Witherdin (02 9335 7591) or Elizabeth Ticehurst (02 9335 7073).

Yours sincerely

Martin Dougall

KPMG
Tower Two
Collins Square
727 Collins Street
Melbourne Vic 3008

GPO Box 2291U
Melbourne Vic 3001
Australia

ABN: 51 194 660 183
Telephone: +61 3 9288 5555
Facsimile: +61 3 9288 6666
DX: 30824 Melbourne
www.kpmg.com.au

Attachment A: KPMG response to Consultation Paper 321 – Whistleblower Policies (7 August 2019) | Detailed observations on the Guidance and recommendations

We outline in the table below our feedback and recommendations in respect of selected aspects of the Guidance.

1. Cutting through Complexity

	Requirement	**Feedback**	**Recommendation**
A	*RG 000.120 An entity's policy should explain how the entity will, in practice, protect disclosers from detriment. For example, it should explain:* *(a) how whistleblower protection officer(s) will protect the welfare of disclosers;* *(b) processes for assessing the risk of detriment against a discloser and other persons (e.g. other staff who might be suspected to have made a disclosure) as soon as possible after receiving a disclosure;* *I support services (including counselling or other professional or legal services) that are available to disclosers;* *(d) strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation* *(e) the specific actions the entity will take to protect a discloser from risk of detriment (e.g. the entity could allow the discloser to perform their duties from another location, reassign the discloser to another role at the same level, make other*	We acknowledge the importance of entities demonstrating how they will in practice protect disclosers from detriment. However, we consider that the policy document is not necessarily the best place to document this. The risk with including all of the detail within RG000.120 is that the policy will become lengthy and consequently less likely to be well-understood by readers. A lengthy and complicated policy may have the unintended consequence of deterring disclosers from coming forward.	We recommend that RG 000.120 be amended to require entities to provide examples of how the entity will protect disclosers from detriment, with a fuller explanation being provided in a supporting procedural document that can be accessed if the reader wishes to see further details.

	Requirement	Feedback	Recommendation
	modifications to the discloser's workplace or the way they perform their work duties, or reassign or relocate other staff involved in the disclosable matter); *(f) how the entity will ensure that management are aware of their responsibilities to:* *(i) maintain the confidentiality of a disclosure;* *(ii) address the risks of isolation or harassment;* *(iii) manage conflicts; and* *(iv) ensure fairness when managing the performance of, or taking other management action relating to, a discloser;* *(g) procedures on how a discloser can lodge a complaint if they have suffered detriment, and the actions the entity will take in response to such complaints (e.g. the complaint could be investigated as a separate matter by an officer who is not involved in dealing with disclosures and the investigation findings will be provided to the board or audit or risk committee); and* *(h) the specific interventions the entity will take to protect a discloser if detriment has already occurred (e.g. the entity could investigate and address the detrimental conduct—such as by taking disciplinary action—or the entity could:* *(i) allow the discloser to take extended leave;* *(ii) develop an alternative career development plan for the discloser, including new training and career opportunities; or* *(iii) the entity could offer compensation or other remedies.*		
B	*RG 000.130 to RG 000.138* *(Handling and investigating a disclosure and Process for investigating a disclosure)*	We acknowledge the importance of providing disclosers with access to information in respect of the investigation process. However - rather than housing large amounts of detailed investigation information in the whistleblowing	We recommend that the Guidance recognises that organisations may include 'high level' information about how it will investigate disclosures in it's whistleblower policy.

	Requirement	Feedback	Recommendation
		policy (over and above the requirements of s1317AI(5)(d)), we suggest that a more appropriate forum is an organisation's investigations procedure document.	We recommend that the Guidance suggests that detailed information be documented within a separate investigations procedure document.
C	*RG 000.107 An entity's policy should outline the measures the entity has in place for ensuring confidentiality. An entity should establish secure record-keeping and information sharing procedures. It should ensure that:* *(a) all paper and electronic documents and other materials relating to disclosures are stored securely;* *(b) all information relating to a disclosure can only be accessed by those directly involved in managing and investigating the disclosure;* *(c) only a restricted number of people who are directly involved in handling and investigating a disclosure are made aware of a discloser's identity or information that is likely to lead to the identification of the discloser;* *(d) communications and documents relating to the investigation of a disclosure are not sent to an email address or to a printer that can be accessed by other staff; and* *(e) each person who is involved in handling and investigating a disclosure is reminded that they should keep the identity of the discloser and the disclosure confidential and that an unauthorised disclosure of a discloser's identity may be a criminal offence.*	We acknowledge the importance of the entity establishing secure record-keeping and information sharing procedures. However, we consider that detailed information on these procedures is better located within a separate procedure document.	We recommend that RG 000.107 is deleted as a policy requirement.

2. Expanding certain aspects of the Guidance

	Requirement	Feedback	Recommendation
A	*RG 000.68 - An entity's policy should explain that disclosures can be made to a journalist or parliamentarian under certain circumstances and qualify for protection: see s1317AAD.*	The guidance does not clearly require an entity to stipulate the criteria for public interest disclosures and emergency disclosures. This may result in a scenario where a discloser reports a matter to a journalist under the misleading impression that their disclosure is protected. The impact of this action may be detrimental on both the discloser and the entity.	We recommend RG 000.68 is amended as follows: *"An entity's policy should explain that disclosures can be made to a journalist or parliamentarian and qualify for protection under certain circumstances: see s1317AAD.* *The policy should clarify that a disclosure must have been previously made to ASIC /APRA or another Cth body and written notice provided to the body to which the disclosure was made."*
B	RG 000.71 – *It is good practice for an entity's whistleblower policy to include a statement suggesting that a discloser should contact the entity's whistleblower protection officer or an independent legal adviser to ensure a discloser understands the criteria for making a public interest or emergency disclosure that qualifies for protection.*	This guidance may tend to infer that the whistleblower protection officer can provide the same level of advice as a legal practitioner. Given the complexity of the whistleblower protections legislation, a whistleblower protection officer may not be appropriately equipped to provide the discloser with advice in this situation. However, the whistleblower protection officer should be able to point the discloser to further resources or information.	We recommend that RG 000.71 be amended as follows: "*It is good practice for an entity's whistleblower policy to include a statement suggesting that a discloser ensure they understand the criteria for making a public interest or emergency disclosure that qualifies for protection. A discloser can contact an independent legal adviser to obtain further advice, or may contact the whistleblower protection officer for guidance on where to find additional information and resources*."
C	*RG 000.103 A person can disclose the information contained in a disclosure without the discloser's consent if:* *a) The information does not include the discloser's identity;* *b) The entity has taken **all reasonable steps** to reduce the risk that the discloser will be identified from the information; and* *c) It is reasonably necessary for investigating the issues raised in the disclosure.*	We have received feedback from numerous organisations that they are unclear on what "reasonable steps" may entail. Moreover, the law and the explanatory memorandum are silent in this regard. We consider that there is an opportunity for ASIC to provide guidance in this respect.	We recommend that the Guidance provides some practical examples of "reasonable steps" an entity can take to reduce the risk that the discloser will be identified from the information. In our experience operating the FairCall service, we have found the following steps to be effective in reducing the risk that an anonymous discloser will be identified:

	Requirement	Feedback	Recommendation
			• Ensure that the discloser is referred to in a gender neutral context; • Redact any personal information or reference to the discloser witnessing an event; • Where possible, directly speak with the discloser to discuss whether certain aspects of their report could inadvertently identify them; and • Ensure that any investigator appointed to investigate the issues raised in a disclosure is suitably qualified in whistleblowing processes.
D	*RG 000.112 The policy should also provide examples of actions that are not detrimental conduct. In practice, administrative action that is reasonable to protect a discloser from detriment (e.g. when the disclosure relates to wrongdoing in the discloser's immediate work area) will not be considered as detrimental conduct. Protecting a discloser from detriment also does not prevent the entity from managing a discloser's unsatisfactory work performance, if the action is in line with the entity's performance management framework. It is important for an entity to ensure that a discloser understands the reason for the entity's administrative or management action.*	In our experience, disclosures are often made in circumstances where the discloser is under performance management or their employment is otherwise under threat. We note that the Guidance deals with the situation where a protected disclosure has been made directly to the entity. For completeness, it should also cover the situation where a protected disclosure has been made to another party, such as ASIC/APRA or a legal practitioner.	We recommend that the following paragraph is added to RG 000.12: "*The policy may also note that in circumstances where the entity is unaware of a protected disclosure (e.g. where it has been made to ASIC/APRA or a legal practitioner and not to the entity) any detrimental conduct will not be considered to have been made because of a protected disclosure."*

	Requirement	Feedback	Recommendation
E	*RG 000.113 - An entity's whistleblower policy should outline that a discloser (or any other employee or person) can seek compensation and other remedies through the courts if:* *(a) they suffer loss, damage or injury because of a disclosure; and* *(b) the entity failed to prevent a person from causing the detriment.*	We believe RG 000.113 requires amendment to accurately reflect the requirements of the Corporations Act. Section 1317AE(3) provides that a court may have regard to whether the entity took reasonable precautions and exercised due diligence to avoid the detrimental conduct.	We recommend that *RG 000.113 be* amended as follows: *"An entity's whistleblower policy should outline that a discloser (or any other employee or person) can seek compensation and other remedies through the courts if:* *(a) they suffer loss, damage or injury because of a disclosure; and* *(b) the entity failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct".*
F	RG 000.165 *To ensure disclosers outside an entity can access the entity's whistleblower policy, the policy should be available on the entity's external website.*	We consider that a better practice policy that meets ASIC's guidance criteria and is appropriately tailored to an individual entity, is likely to contain significant information that would not be relevant or useful to external disclosers. It may also not be appropriate for some of this information to be in the public domain – for example, the names and contact phone numbers of internal eligible recipients for employees.	We recommend that RG 000.165 is amended as follows: *"To ensure that disclosers outside an entity can access the entity's whistleblower policy, the policy (**or alternatively, a summary of the policy)** should be available on the entity's external website.* *We note that recommendation 3.3 of the ASX Corporate Guidance principles require all listed entities to publish their policy, however personal or confidential information may be redacted."*

3. Clarifying Legal Obligations and Good Practice

	Requirement	Feedback	Recommendation
A	*RG 000.86 It should specify the names of the entity's internal reporting points and the whistleblower protection officer.*	The law requires that the policy include "information about to whom disclosures that qualify for protection under this Part may be made". A requirement to name all of the entity's internal reporting points appears to go beyond this requirement, and may also cause some practical privacy issues should this information be made available to persons outside the organisation.	We recommend that RG 000.86 be amended as follows: "*RG 000.86 It is good practice for the policy to specify the names of the entity's internal reporting points and the whistleblower protection officer. However, this may not be practical in every organisation."*
B	*RG 000.93 The policy should also explain that a discloser may choose to adopt a pseudonym for the purposes of their disclosure, and not use their true name. This may be appropriate in circumstances where the discloser's identity is known to their supervisor, the internal reporting point or whistleblower protection officer, but the discloser prefers not to disclose their identity to others.*	The law requires that the policy contain "*information about how the company will support whistleblowers and protect them from detriment*". The use of a pseudonym is an example of how the entity could protect and support whistleblowers, but the use of the word "should" tends to indicate that it is a mandatory part of the policy.	*We recommend that the Guidance clearly differentiate between legal requirements and good practice in respect of RG 000.93.*
C	*RG 000.106 An entity's policy should include information about how a discloser can lodge a complaint with the entity about a breach of confidentiality. It should also explain that a discloser may lodge a complaint with a regulator, such as ASIC or APRA, for investigation.*	Corporations Act section 1317AI (5) does not require this information to be included in a whistleblowing policy, however the use of the word "should" tends to indicate that this is a mandatory part of the policy, rather than a good practice recommendation.	*We recommend that the Guidance clearly differentiate between legal requirements and good practice in respect of RG 000.106.*