Australian Banking Association

18 September 2019

Andivina Uy / Geoff Hackett
Senior Adviser, Strategic Policy
Office of the Whistleblower
Australian Securities and Investments Commission
GPO Box 9827
Brisbane QLD 4001
email: whistleblower.policy@asic.gov.au

ASIC CP 321 Whistleblower policies

The Australian Banking Association (**ABA**) welcomes the opportunity to provide our response to the Australian Securities and Investments Commission (**ASIC)** Consultation Paper 321 - Whistleblower policies and the implementation of obligations under the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019* (the Act).

The banking industry has been a strong advocate of the introduction of a comprehensive and more effective corporate whistleblowing regime.

An effective whistleblowing policy and program is an essential part of a corporation's governance and overall approach to risk management. ABA member banks have undertaken significant reforms in the past few years, and in line with *ABA's Guiding Principles – Improving Protections for Whistleblowers* have put in place comprehensive whistleblowing programs which include clear reporting and investigative processes, details of the reporting channels including anonymous disclosure and organisational support available to whistleblowers.

Implementation of the legislation

Since the Act received royal assent on 12 March 2019, banks have been working to implement changes in line with the legislation. The vast majority of ABA member banks have already put in place a revised whistleblower policy, associated procedures and whistleblower program to ensure the bank's whistleblower policy and program comply with the spirit and intent of the legislation and that their employees, and others are well aware of new legislative obligations and protections. ABA members want to ensure they have the highest standard of protections for their employees.

We acknowledge that ASIC has been required to prepare regulatory guidance that applies across all industries, not just financial services. While we support the standards being set by the draft guidance, we do believe that requiring this to sit in one single policy document is overly prescriptive. The ABA has set out specific considerations in part A of this submission.

Our members are concerned (and our experience tells us) that putting too much detail in an overarching whistleblower policy can have a detrimental effect on appropriate application of the policy and may create an inflexible process that cannot be tailored to individual circumstances.

The whistleblowing policies implemented by ABA members tend to be high level 'policy statements' supported by more operational procedures and a comprehensive whistleblower program which includes procedures and practices, reporting channels, communications arrangements and training programs (Part B includes an example: Overview of whistleblower framework documentation and systems).

The high-level policy statements will include the core elements required by the legislation to ensure compliance with section 1317AI. The operational procedures and practices address the type of operational detail included in parts of the draft regulatory guidance. In its entirety, the program (comprised of the policy, procedures and practices) will generally meet the scope of the requirements outlined in the regulatory guide but is not limited to one detailed policy document.

If ASIC believes this approach (high-level policy supported by operational procedures, training etc.) complies with the regulatory guidance we ask that ASIC include express acknowledgement of this within the final regulatory guidance.

We further request that ASIC consider the following points to enhance the draft guidance:

- Recognise that entities should ensure their whistleblowing programs are comprehensive, user-friendly and supported by a number of processes and procedures that ensure that all in the organisation understand the importance of the whistleblower program. To enable policies to be easily understood across large organisations, the standards set by the guidance may be better contained in the procedures and processes that support a whistleblower program.
- Give consideration to how large corporate entities with a multitude of subsidiaries might implement a policy. The ABA suggests that ASIC include an affirmative statement regarding the sufficiency of a Corporate Group level policy with the need for more detailed/tailored procedures for individual subsidiaries only if required.
- The terms "should" vs "must" appear in both the draft regulatory guidance and the draft additional good practice guidance, for example, "should" is in both the mandatory section and good practice guidance. Where "should" is used in the mandatory section in addition to "must", we have assumed that the "should" is permissive and is akin to good practice principles however it would be helpful if this were made express. If the "should" is required to be interpreted as "must" in the mandatory section, we have some concerns with the practical implementation of the principles. We ask that ASIC clarify this in the final guidance (examples are included in part A of this submission).
- A number of ABA members operate in a number of overseas jurisdictions and ASIC's views on how the extraterritorial effect of legislation would be applied would be appreciated. The guidance would benefit from additional commentary in relation to how to address extraterritorial application in policies.

Timing of the final regulatory guidance

We are concerned that the complexity outlined and potential changes to the draft regulatory guidance will make it very difficult for many entities to have clear and user-friendly policies for potential whistleblowers in place by the 1 January 2020 implementation date. Entity whistleblower policies may need to be finalised subject to final ASIC guidance. Achieving any required changes will be challenging within ASIC's current timeframe. For example, even though a policy may be substantially compliant with the legislation, even minor amendments to the regulatory guidance will require an entity to obtain management and potentially board approval of the final policy which would not be practically achievable by 1 January 2020. Considering this uncertainty, we suggest that ASIC provide a facilitative compliance period of six months in relation to the regulatory guidance so entities can ensure they comply with all aspects of the final regulatory guidance.

The ABA appreciates the opportunity to have input into this process and looks forward to working with ASIC through this consultation process. Please contact me on … or at …if you have any questions or require anything else.

Yours sincerely,

Signed by

Amanda Pullinger
Policy Director

Australian Banking Association

Part A

REGULATORY GUIDE 000 Whistleblower policies – B Matters to be addressed by an entity's whistleblower policy

The ABA believes there are elements of the policy framework that would be better implemented through whistleblower programs or procedural documents or that we consider require clarification.

RG proposal	Concern / proposed solution
RG 000.36 - Where relevant, a whistleblower policy should outline the businesses, divisions and offices that are covered by the policy.	This could be interpreted as requiring every business unit within an organisation is listed in the policy. For large entities with numerous businesses, divisions and offices located internationally, including this level of detail in a single policy document would not be practical. Banks generally outline the broad coverage of the whistleblower policy, being clear that it applies to all the companies within the Group, and everyone who works for the Group, including in the supply of goods and services to all of those companies. More detailed information should be provided in more user-friendly channels through intranet/internet sites, procedural information, training programs, communications materials etc. We ask that ASIC consider this approach.
RG 000.40 – "if the discloser has reasonable grounds to suspect that the information indicates those entities (including their employees or officers) have engaged in conduct that: (a) constitutes an offence against, or a contravention of, a provision of any of the following (*summarised*): • Specified Acts and any instruments made under those Acts; • constitutes an offence against any Commonwealth law punishable by imprisonment for 12 months or more: • is prescribed by regulation.	The ABA agrees that an entity's policy should cover the types of disclosures that qualify for protection under the Corporations Act (i.e. 'disclosable matters') as set out in RG 000.38, however our concern with this detailed list or having to include the level of specificity in RG 000.40 (which is the same wording in the Corporations Act) is that it becomes more of the '*legal or industry jargon'* that is referred to in RG 000.193 which policies should seek to avoid. We suggest that this level of specificity (including similar "chapter and verse" restatement of sections of the Corporations Act set out in RG 000.69; RG 000.70) not be required to be recited in the policy wording, with the view of prioritising the avoidance of legal jargon and making the concepts easier to understand in plain English.

RG 000.49 – "An entity's policy should clarify that disclosures that are not about disclosable matters are not covered by the policy because they do not qualify for protection under the Corporations Act."	We recommend that entities are free to expand their policy to cover matters that might not qualify for protection under the Corporations Act. Our rationale is that a statement in an entity's policy that: "*disclosures that do not qualify for protection under the Corporations Act are not covered by its whistleblower policy*" could risk deterring possible whistleblowers from coming forward without them first attempting to navigate or consider whether their disclosure satisfies the criteria for legal protection. It would therefore be helpful for an entity to be allowed to err on the side of caution and include matters within its policy that may or may not fall within the legislation. For example, entities could adhere to the principles set out in RG 000.37 and RG 000.38 (that a policy should identify the types of wrongdoing that can be reported under the policy, outline matters not covered by the policy, and cover types of disclosures that qualify for protection under the Corporations Act), without requiring that disclosures that do not qualify for legal protection are specifically excluded from the policy.
RG 000.54 – "it is important for an entity to focus on the substance of the disclosure, rather than what they believe to be the discloser's motive for reporting" etc.	The ABA supports the intent of this guidance however suggest this point be included in good guidance for an entity's practice / process, and therefore outlined in its internal procedural documents, rather than outlined in the high-level policy document.
RG 000.76 – "whistleblower protection officer should report directly to the entity's board or audit or risk committee" and "The whistleblower investigation officer should report directly to a senior executive or officer with responsibility for legal, compliance or risk matters."	The ABA supports regular reporting by the Whistleblower Program to the board or audit committee. We suggest that the Whistleblower Protection Officer (**WPO**) should "have the ability" to report through the entity's board, audit or risk committee rather than "should report directly", to give flexibility to the range of different entities covered by the legislation and the governance structures that would be in place. In addition, the ABA suggests that at a minimum, the Whistleblower Investigation Officer (**WIO**) report to a group level function rather than be specific as to the function the role should report to, and that the WPO and WIO have different reporting lines.
RG 000.79 - It is good practice for an entity to ensure that any individual in the entity … who receives a disclosure notifies the entity's whistleblower protection officer, subject to the discloser's consent, to ensure that the entity's mechanisms for protecting and safeguarding disclosers can commence as soon as possible.	We agree that the WPO should be notified of a disclosure where there is a need to protect and safeguard the discloser. However, the requirement in RG 000.79 suggest the WPO be notified of all whistleblower matters which in a large organisation may not be practical. We recommend the WPO be notified where the whistleblower has requested that the matter be dealt by the WPO, where there are identified or materialised risks of victimisation and there has been an assessment of reprisal.

RG 000.86 – "the policy should specify the **names** of the entity's internal reporting points and the whistleblower protection officer".	The ABA suggest that this could be impractical in a large organisation where roles change regularly (particularly, for example, given whole internal audit teams, and external auditors, could be eligible recipients). We would recommend that this instead reflect the wording set out in Table 1 in Part A and RG 000.56 "an entity's WB policy must identify the **types of roles** within and outside the entity who can provide advice on or receive a disclosure….".
RG 000.120 – "the policy should explain how the entity will, in practice protect disclosers from detriment. For example…"	The ABA agrees that the entity's policy and procedures should outline how disclosures will be protected. Given each disclosure is different, it would be very difficult to cover all the possible scenarios in a policy document. An entity's procedures should cover this, e.g. as a list of possible things to consider and discuss with the discloser, as part of its risk assessment, as part of its investigation planning, to ensure there is appropriate communication about protection with the discloser, without having to spell it all out in a policy where it will not be relevant to each particular situation and may deter or confuse disclosers.
RG 000.144 – "the entity should indicate how frequently a discloser will receive an update (e.g. once a quarter)". Also mentioned in RG000.134	We agree that keeping a discloser informed will give them assurance the entity is taking their disclosure seriously (RG 000.145). However, the requirement in RG000.144 to commit to specific timing is not helpful in a policy, given each matter is so different, and could lead to unreasonable expectations. In addition, some whistleblowers do not wish to be informed about the progress of an investigation due to concerns about getting "too involved". We would recommend that communication and transparency about the investigation process and timeframes for updates (depending on the nature of the matter) should be a principle of the policy and more specific timeframes could be outlined in the entity's procedures.
RG 000.146 – "policy should indicate the information the discloser will receive at the end of the investigation".	As all matters are different it is very difficult to reference in a policy the nature of the all information that can be provided to a discloser. We would recommend that the policy state that the entity will provide information about the outcome where possible and in accordance with the Privacy Act, and as soon as practicable after the investigation has concluded.
RG 000.150 (d) an employee who is the subject of a disclosure will be advised about: • the subject matter of the disclosure as and when required by principles of natural justice and procedural fairness, and prior to any actions being	We are concerned about the requirement for the person who is the subject of a disclosure being notified about the subject matter of the disclosure and the outcome of the investigation – without any reference to the need for protection of the whistleblower. We believe that while principles of natural justice and procedural fairness should inform the way

taken—for example, if the disclosure is to be the subject of an investigation or if the disclosure is serious and needs to be referred to ASIC, APRA or the Federal Police; and • (ii) the outcome of the investigation (but they will not be provided with a copy of the investigation report).	the investigation is handled, there may be circumstances where those principles are far outweighed by the risk of disclosure of the discloser's identity and potential for retaliation. Further, it is not uncommon for organisations to first conduct covert enquiries into a disclosure and if evidence in support of the disclosure is identified, to then put that evidence to the subject to the disclosure. This can be done without the subject being informed in the investigation commenced as a result of a whistleblower disclosure. We would suggest that the policy spell out that if appropriate (given the nature of the matter and the obligations to protect the identity of the discloser) the person/s to whom the disclosure relates will be informed of any evidence against them, and an opportunity to respond, prior to any negative findings being made against them .

Australian Banking Association

Part B – Example: Overview of whistleblower framework documentation and systems

Framework documentation and systems	
Group Whistleblower Policy	A high-level Group/Corporate policy available internally and externally, setting out the key requirements as required by the legislation.
Other supporting process and procedural documents, for example: • Whistleblower Policy procedure document • Other relevant Standard Operating Procedures (SOP) • Guidance notes • Whistleblower investigation checklist	These documents provide information on how to manage whistleblower disclosures for the individual roles within the whistleblower program and teams that support them. Examples of where these documents cover the requirements within the RG include: • RG 000.93 – 000.94 (anonymous disclosures) • RG 000.107 (identity protection (confidentiality) • Many of the requirements set out in RG 000.120 (protection from detrimental acts or omissions) • RG 000.123 – 000.129 (protection from detrimental acts or omissions)
Training and awareness material, for example: • Communications plans • Communications content • eLearning modules • Face to Face training material	As set out in RG 000.154 – 000.164, a training and awareness program designed to ensure eligible recipients and teams managing whistleblower disclosures understand their obligations, as well as employee comms and training on how to raise a concerns and the channels available, as well as how and where to access the whistleblower policy.
Governance reporting and processes	Committee, Board and Board Audit reporting, as per RG 000.166 - 000.174.
Channels for making disclosures	Having systems in place for eligible persons to make a disclosure, for example: • A hotline and/or securely monitored email address • Encrypted online portal • Process for eligible recipients to receive disclosures