Arteva Funding Group Whistleblower Policy

Table of contents

Section	Description	Page
1.	Background to this policy	2
2.	Content of this policy	2
3.	Purpose of this policy	3
	Why a whistleblower policy is important	4
4.	Who this policy applies to	4
	Examples of eligible whistleblowers	4
5.	Matters this policy applies to	5
	Examples of disclosable matters	6
	Personal work-related grievances	6
6.	Who can receive a disclosure?	7
	Disclosures to non-company parties	8
	Public interest disclosures and emergency disclosures	8
7.	How to make a disclosure	9
	Anonymous disclosures	10
8.	Legal protections for disclosers	11
	Identity protection (confidentiality)	11
	Protection from detrimental acts or omissions	11
	Compensation and other remedies	12
	Civil, criminal and administrative liability protection	12
9.	Support and practical protection for disclosers	13
10.	How the company will handle and investigate a disclosure	13
	Limitations on the investigation process	14
11.	Ensuring fair treatment of individuals mentioned in a disclosure	15
12.	Ensuring this policy is easily accessible	15
13.	Roles, reporting and review	16
	Version history of this policy	17

PF HoldCo Pty Ltd ACN 646 201 489, ABN 66 646 201 489

PF MidCo Pty Ltd ACN 646 202 093, ABN 32 646 202 093

PF FinCo Pty Ltd ACN 646 202 717, ABN 72 646 202 717

PF BidCo Pty Ltd ACN 646 214 262, ABN 35 646 214 262

Principal Finance Pty Ltd ACN 008 081 712, ABN 40 008 081 712

Premium Funding Pty Ltd ACN 057 306 171, ABN 34 057 306 171

PF Advance Pty Ltd ACN 611 434 229, ABN 66 611 434 229

Arteva Funding NZ Limited, NZ company no. 8555154, NZBN 9429051019136

Whistleblower Policy

Effective 16th September 2024

1. Background to this policy

Under the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act* 2019 (Cth),[1] which is effective from 1st January 2020, persons (such as employees of companies) who disclose the company's unlawful act or other misconduct internally or to regulatory bodies are granted strengthened protections against disclosure of identity, dismissal, discriminatory behaviour or other detriment.

Also, "large proprietary companies"[2] need to have a written "whistleblower policy" available from 1st January 2020, and which explains the protections to their directors, staff and others.

The Arteva Funding Group comprises four operational entities, being Principal Finance Pty Ltd, Premium Funding Pty Ltd, PF Advance Pty Ltd and Arteva Funding NZ Limited. They are wholly owned by a series of wholly-owned companies, being, in ascending order, PF BidCo Pty Ltd, PF FinCo Pty Ltd, PF MidCo Pty Ltd and PF HoldCo Pty Ltd.

This policy was prepared for Principal Finance Pty Ltd, and promulgated effective from 1st January 2020, solely as a matter of good governance and risk management because, as at that time, that company was not a large proprietary company. On 29th January 2021, PF BidCo Pty Ltd acquired Principal Finance Pty Ltd, Premium Funding Pty Ltd and PF Advance Pty Ltd and, as a result, it became a large proprietary company on 30th June 2022. So did all of its holding companies, given a company is a large proprietary company if it and the entities it controls meet the criteria. Due to subsequent consolidation, Principal Finance Pty Ltd also became a large proprietary company on 30th June 2024.[3]

On 13th November 2019, ASIC issued a guide as to the content of a whistleblower policy, being Regulatory Guide RG270.[4] This policy has been prepared in line with RG270.

In this policy, "the Act" means the *Corporations Act* 2001, "discloser" means a whistleblower making a protected disclosure, and "the company" means each Arteva Group entity listed above and includes all their businesses, divisions and subsidiaries, all of which are bound by, and must comply with, this policy.

[1] See http://classic.austlii.edu.au/au/legis/cth/num_act/tlawpa2019638/. The new Act effects the new protections principally by way of amendments to the *Corporations Act* 2001 and the *Taxation Administration Act* 1953.
[2] In line with companies that have obligations of mandatory financial reporting to ASIC, large proprietary companies are defined as those which, for itself and the entities it controls, satisfy at least two out of the following three criteria: (1) consolidated financial year revenue of equal to or greater than $50m; (2) consolidated gross assets at the end of the financial year of equal to or greater than $25m; and (3) group employees at the end of the financial year of equal to or greater than 100. See s.45A(3) of the *Corporations Act* and the *Corporations Amendment (Proprietary Company Thresholds) Regulations* 2019.
[3] The Arteva Funding Compliance Plan elaborates on when and why Group companies became "large proprietary companies".
[4] See https://download.asic.gov.au/media/5340534/rg270-published-13-november-2019.pdf.

2. Content of this policy

Section 1317AI(5) of the Act[5] requires a whistleblower policy to have information about:

(a) the protections available to whistleblowers, including under the Act;

(b) to whom disclosures that qualify for protection under the Act may be made, and how they may be made;

(c) how the entity will support whistleblowers and protect them from detriment;

(d) how the entity will investigate disclosures that qualify for protection under the Act;

(e) how the entity will ensure fair treatment of its employees who are mentioned in disclosures that qualify for protection under the Act, or to whom such disclosures relate;

(f) how the policy will be made available to officers and employees of the entity; and

(g) any matters prescribed by regulations.[6]

This policy provides information about each of these matters.

According to ASIC,[7] a whistleblower policy should also include information about the protections under the tax whistleblower regime in the *Taxation Administration Act* 1953.[8] Under s.14ZZT of that Act, disclosers of certain information relating to taxation matters to the ATO and other "eligible recipients" are protected. References to the tax whistleblower laws are included in this policy where relevant.

ASIC has also stated[9] that it expects a company to periodically review and update its whistleblower policy to address any issues which may become apparent. This has been provided for in Section 13.

Although called a "guide", Regulatory Guide RG270 sets out information which ASIC considers a whistleblower policy must contain, as well as information which a policy could, or should, address as a matter of good practice, but which ASIC considers is not mandatory.

In this policy, all the material that ASIC considers mandatory is included, as well as most of the material it considers to be good practice, although it is sometimes modified or re-written.

3. Purpose of this policy[10]

The purpose of this policy is to –

(a) provide a tool which assists in the identification of wrongdoing;

(b) encourage disclosures of wrongdoing;

(c) help deter wrongdoing, and promote a more ethical culture and better compliance with the law (because potential wrongdoers realise there is a higher risk they will be reported);

(d) provide a transparent and practical framework for receiving, handling and investigating disclosures, and for ensuring disclosures are dealt with appropriately and on a timely basis;

(e) ensure individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported; and

(f) demonstrate professionalism and commitment by the company in respect of good governance, risk management and compliance.

The measures in this policy also ultimately serve to support and enhance the company's values of integrity, ethical behaviour, honesty and fairness, and to protect the company's reputation and hence its

[5] See http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/index.html.
[6] No matters have been prescribed as at the date of this policy.
[7] RG270.12.
[8] See http://classic.austlii.edu.au/au/legis/cth/consol_act/taa1953269/index.html.
[9] RG270.13(c).
[10] RG270.39-270.40. Also, RG270.1-270.2.

long-term sustainability. Consequently, this policy serves to enhance good risk management and corporate governance.

Why a whistleblower policy is important

Transparent whistleblower policies help uncover misconduct that may not otherwise be detected. Often, such wrongdoing only comes to light because of individuals (acting alone or together) who are prepared to disclose it, sometimes at great personal and financial risk.

In this respect, the company encourages any employee (or non-employee) who is aware of any possible wrongdoing to report it, and affirms that they should have confidence they will be protected if they do.

4. Who this policy applies to

The Act specifies the types of disclosers within and outside a company who can make a disclosure of wrongdoing that qualifies for protection under the Act.

Such a person, who is called in the Act, and in this policy, an "eligible whistleblower",[11] is any individual who is, or has been –

(a) an officer or employee of the company;

(b) a supplier of goods or services to the company (whether paid or unpaid);

(c) an employee of a supplier of goods or services to the company (whether paid or unpaid);

(d) an associate of the company; or

(e) a relative or a dependant or a spouse of an individual specified in (a), (b), (c) or (d).[12]

The Act defines "associates" of companies, as mentioned in (d) above, as including directors, secretaries[13] (both of which are officers in any case), related body corporates (which do not qualify as they are not "individuals"), and directors and secretaries of related body corporates.[14]

A "related body corporate" means a subsidiary company, a holding company, or other subsidiaries of a holding company.[15] Accordingly, "eligible whistleblowers" include any director or company secretary of those entities (and also their relatives, dependants and spouses).

Examples of eligible whistleblowers

Accordingly, examples of the types of disclosers covered by this policy include current and former –

(a) directors and company secretaries of the company and its subsidiaries

(b) permanent, part time, fixed term or temporary employees of the company, and interns, secondees and managers of the company

(c) sellers, contractors, consultants, service providers, business partners and other suppliers of goods or services to the company, and their current and former employees

(d) relatives, dependants and spouses of the above-listed individuals.

5. Matters this policy applies to

A discloser qualifies for protection as a whistleblower under the Act if they are an eligible whistleblower (see the previous Section) in relation to the company and they have made a disclosure –

(a) of information relating to a "disclosable matter" (see below) directly to –

(i) an "eligible recipient" (see next Section 6) or

[11] RG270.43, s.1317AAA of the *Corporations Act* and s.14ZZU of the *Taxation Administration Act*.
[12] Also, any individual prescribed by the regulations, but none have been.
[13] Which means a company secretary in the context of the Act.
[14] S.11. Also, apparently, persons acting in concert with the company under s.15 of the *Corporations Act*.
[15] Such entities being "related body corporates" as defined in s.50 of the *Corporations Act*.

(ii) ASIC, APRA, or another Commonwealth body prescribed by regulation;[16]

(b) to a legal practitioner for the purposes of obtaining legal advice or legal representation about the operation of the whistleblower provisions in the Act; or[17]

(c) which is an "emergency disclosure" or a "public interest disclosure"[18] (see below).

However, the disclosure must also be of a "disclosable matter"[19] that is, information which the discloser has reasonable grounds to suspect –

(a) concerns misconduct (defined in s.9 of the Act to include "fraud, negligence, default, breach of trust and breach of duty"), or an improper state of affairs or circumstances, in relation to the company or a related body corporate or

(b) indicates that the company, or any officer or employee of the company (or a related body corporate or any of its officers or employees) has engaged in conduct that –

(i) constitutes an offence against, or a contravention of any provision of –

- the *Corporations Act* 2001
- the *Australian Securities and Investments Commission Act* 2001
- the *Banking Act* 1959
- the *Financial Sector (Collection of Data) Act* 2001
- the *Insurance Act* 1973
- the *Life Insurance Act* 1995
- the *National Consumer Credit Protection Act* 2009
- the *Superannuation Industry (Supervision) Act* 1993
- any instrument made under any of the above listed legislation or

(ii) constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more, or

(iii) represents a danger to the public or the financial system or

(iv) is conduct prescribed by the regulations.[20]

The phrase "improper state of affairs or circumstances" is not defined and, according to ASIC,[21] is intentionally broad, and "may not involve unlawful conduct in relation to the entity or a related body corporate of the entity but may indicate a systemic issue that the relevant regulator should know about to properly perform its functions. It may also relate to business behaviour and practices that may cause consumer harm."

The phrase "reasonable grounds to suspect" requires that the discloser's suspicion be objectively reasonable. ASIC says[22] this ensures that a discloser's motive for making a disclosure, or their personal opinion of any person involved, does not prevent them from qualifying for protection. ASIC further says that a mere allegation with no supporting information is unlikely to qualify as "reasonable grounds to suspect", but also notes that a discloser does not need to prove their allegations.

Note that "disclosable matters" include conduct that may not involve a contravention of a particular law. For example, information that suggests a significant risk to public safety or the stability of, or confidence in, the financial system is a disclosable matter, even if it does not involve a breach of a particular law.

[16] S.1317AA(1).
[17] S.1317AA(3).
[18] S.1317AAD.
[19] Being the heading to ss.1317AA(4) and (5) of the Act, which list the "disclosable matters" listed here.
[20] No conduct has been prescribed as at the date of this policy.
[21] RG270.52.
[22] RG270.53.

Note also that a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

Examples of disclosable matters

Examples of disclosable matters that relate specifically to the company's business operations and practices would include:

(a) illegal conduct, such as theft, dealing in, or use of, illicit drugs, violence or threatened violence, and criminal damage against property;

(b) fraud, money laundering or misappropriation of funds;

(c) offering or accepting a bribe;

(d) financial irregularities;

(e) failure to comply with, or breach of, legal or regulatory requirements; and

(f) engaging in or threatening to engage in detrimental conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

Personal work-related grievances

Disclosure of information concerning a personal work-related grievance of the discloser doesn't qualify for protection under the Act.[23]

However, this exception doesn't apply if the information concerns a detriment (see Section 8 below) or threat of detriment to the discloser arising from an actual or potential whistleblower disclosure.[24]

"Personal work-related grievances"[25] are grievances that relate to the discloser's current or former employment and have, or tend to have, implications for the discloser personally, but –

(a) don't have significant implications for the company (or another entity) that do not relate to the discloser; and

(b) don't relate to any conduct, or alleged conduct, about a "disclosable matter".

Examples[26] of "personal work-related grievances" include:

(a) an interpersonal conflict between the discloser and another employee;

(b) a decision that does not involve a breach of workplace laws;

(c) a decision about the engagement, transfer or promotion of the discloser;

(d) a decision about the terms and conditions of engagement of the discloser; and

(e) a decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

A grievance can be personal work-related, but may still qualify for protection if –

(a) it includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance;

(b) the entity has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct beyond the discloser's personal circumstances;

(c) the discloser suffers from or is threatened with detriment for making a whistleblower disclosure ("detriment" is discussed further in Section 8 below); or

[23] S.1317AADA(1)(a).
[24] Ss.1317AADA(1)(b) and 1317AC.
[25] S.1317AADA(2).
[26] Note to s.1317AADA.

(d) the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Act.[27]

NOTE: Any employee having a "personal work-related grievance", or other type of issue or concern that is not covered by this policy, is encouraged to resolve the same, and to that end to raise it with their supervisor or manager, and if appropriate to also request that the matter be treated in confidence. It may also be appropriate for the employee to seek independent external legal advice about their rights and protections under employment or contract law.[28]

6. Who can receive a disclosure

A discloser needs to make a disclosure directly to one of the company's "eligible recipients" to be able to qualify for protection as a whistleblower under the Act (or as a whistleblower under the *Taxation Administration Act*, if that applies).

For the company, an "eligible recipient"[29] means:

(a) an officer or senior manager of the company or its related body corporate;

(b) the internal or external auditor (including a member of an audit team conducting an audit) or an actuary of the company or its related body corporate; and

(c) a person authorised by the company to receive disclosures that may qualify for protection.

"Officers" of a company include directors and company secretaries.

"Senior managers"[30] includes executives, other than a director or company secretary, who –

(a) make or participate in making decisions that affect the whole, or a substantial part, of the business of the company; or

(b) have the capacity to significantly affect the company's financial standing.

Although it is not a pre-condition to obtaining whistleblower protection, employees and other potential disclosers are encouraged to make a disclosure in the first instance to internal eligible recipients. This may serve to address an issue sooner.

Disclosures to non-company parties

As noted in the previous Section, disclosures to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the whistleblower provisions in the Act are protected (even if the practitioner concludes that a disclosure does not relate to a "disclosable matter").[31]

Whistleblower protections also apply to disclosures of information relating to disclosable matters to ASIC, APRA or another Commonwealth body prescribed[32] by regulation.[33]

Information about making disclosures to ASIC is at https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/how-asic-handles-whistleblower-reports/.

Information about making disclosures to APRA is at www.apra.gov.au/become-a-whistleblower-and-make-a-public-interest-disclosure.

Information about making disclosures to the ATO is at www.ato.gov.au/general/gen/whistleblowers/.

---

[27] RG270.63.
[28] Note also that disclosures that are not about "disclosable matters", and hence do not qualify for protection under the Act, may still be protected under other legislation, such as the *Fair Work Act* 2009 (Commonwealth).
[29] S.1317AA(2), together with the "eligible recipient" definition in Section 1317AAC(1). Similarly, s.14ZZT(2) of the *Taxation Administration Act*.
[30] S.9, *Corporations Act*.
[31] S.1317AA(3). Similarly, s.14ZZT(3) of the *Taxation Administration Act*.
[32] No other Commonwealth bodies are presently prescribed.
[33] S.1317AA(1). Under s.14ZZT(1) of the *Taxation Administration Act*, the disclosure must be to the ATO.

Public interest disclosures and emergency disclosures

Certain disclosures of information to journalists[34] or parliamentarians[35] may also qualify for protection.

A "public interest disclosure"[36] is a disclosure of information to a journalist or a parliamentarian where –

(a) at least 90 days have passed since the discloser made a protected disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;

(b) the discloser does not have reasonable grounds to believe that action is being, or has been taken, to address their disclosure;

(c) the discloser has reasonable grounds to believe that making a further disclosure of the information would be in the public interest;

(d) before making the public interest disclosure, the discloser has given written notice to the body in (a) (i.e. the body to which the previous disclosure was made) that:

(i) includes sufficient information to identify the previous disclosure; and

(ii) states that the discloser intends to make a public interest disclosure;

(e) the extent of the information disclosed is no greater than is necessary to inform the journalist or parliamentarian of the "disclosable matter" (see Section 6 above).

A "emergency disclosure"[37] is a disclosure of information to a journalist or a parliamentarian where –

(a) the discloser has previously made a protected disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;

(b) the discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;

(c) before making the emergency disclosure, the discloser has given written notice to the body in (a) (i.e. the body to which the previous disclosure was made) that:

(i) includes sufficient information to identify the previous disclosure; and

(ii) states that the discloser intends to make an emergency disclosure;

(d) the extent of the information disclosed is no greater than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

It is essential that a discloser understand that there are criteria that must be met to make a protected public interest or emergency disclosure.

Specifically, the disclosure must have previously been made to ASIC, APRA or a prescribed body, and prior written notice must be provided to that body to which the disclosure was previously made.

Also, in the case of a public interest disclosure, at least 90 days must have passed since the previous disclosure.

A discloser should contact an independent legal adviser before making a public interest disclosure or an emergency disclosure.

[34] In summary, a professional journalist working for a newspaper or magazine, or in radio, TV or a similar electronic or internet service. See s.1317AAD(3) if in doubt for a fuller definition.
[35] A member of Parliament of the Commonwealth, a State or a Territory: s.1317AAD(1)(f)(i) and (2)(d)(i).
[36] S.1317AAD(1).
[37] S.1317AAD(2).

7. How to make a disclosure

A whistleblower can make a disclosure to any of the following (and they are authorised by the company to receive it):[38]

Internal:	Chief Executive Officer Daniel Gronert In person in the office at Ground Floor, 99 Frome Street, Adelaide SA 5000 By post to Daniel Gronert, Ground Floor, 99 Frome Street, Adelaide SA 5000 (marked Confidential) By telephone on 1300 137 037 or 0402 458 119 By email at daniel.gronert@arteva.com.au
External:	Non-executive Director Stephen Palyga (our Compliance Director) In person at 56 Cooper Road, Mylor SA 5153 By post to Stephen Palyga, PO Box 5, Mylor SA 5153 By telephone on 0433 213 141 By email at s.palyga@outlook.com
External:	To the Group's auditors Ernst & Young, attention Brad Tozer In person in the office at 111 Eagle Street, Brisbane Queensland 4000 By post to Brad Tozer, Ernst & Young, 111 Eagle Street, Brisbane Queensland 4000 By telephone on 07 3243 3333 or 07 3243 3721 By email at brad.tozer@au.ey.com

A whistleblower can make a disclosure outside of business hours to any of the above.

A whistleblower can request confidentially in making a disclosure.

Without making a disclosure, an employee can also seek accurate and confidential information about the following from the Whistleblower Protection Officer named in Section 13 below:

(a) how the company's whistleblower policy works;

(b) what the policy covers; and

(c) how a disclosure might be handled.

Anonymous disclosures[39]

A disclosure can be made anonymously and still be protected under the Act.[40]

A discloser can choose to remain anonymous while making a disclosure, over the course of the investigation, and after the investigation is finalised.

A discloser can refuse to answer questions that they feel could reveal their identity at any time, including during follow-up conversations with a recipient or investigator.

However, a discloser who wishes to remain anonymous should maintain ongoing two-way communication with the company or person to whom a disclosure is made, to enable them to ask follow-up questions or provide feedback. Otherwise, proper investigation of the disclosure may be compromised, and the procedure thwarted as a result.

---

[38] The external option allows that an employee may not be comfortable to make a disclosure internally, or feel it is inappropriate to do so, for example, because of barriers such as the potential threat of detriment. It also better enables the entity's non-employees (e.g. former employees and current and former suppliers) to make a disclosure to the entity: RG270.81.
[39] If a disclosure comes from an email address from which the person's identity cannot be determined, and the discloser does not identify themselves in the email, it should be treated as an anonymous disclosure: RG270.85.
[40] S.1317AAE.

If a whistleblower wishes to make a disclosure anonymously, they might do so –

(a) by anonymised email;

(b) via a telephone or mobile with Caller ID switched off, and to a recipient who would not recognise their voice (most likely being an "external" recipient), in which case arrangements should be made for the discloser to ring back to enable the recipient to ask follow-up questions or provide feedback;

(c) via a telephone or mobile with Caller ID switched on, but having a telephone number which would not be known to, and could not be determined by, the recipient (most likely being an "external" recipient who would also not recognise their voice); or

(d) by anonymous letter sent by mail (most likely to an "external" recipient who would not recognise the writing), and preferably giving an untraceable return address to enable the recipient to ask follow-up questions or provide feedback.

A discloser may also adopt a pseudonym for the purpose of their disclosure. This may be appropriate in circumstances where the discloser's identity is known to their supervisor, the Whistleblower Protection Officer or other recipient of the disclosure, but the discloser prefers that other persons not be aware of their identity.

8. Legal protections for disclosers

The following legal protections are available under the Act to disclosers who qualify for protection as a whistleblower.

They apply not only to internal disclosures, but to disclosures to legal practitioners, regulatory and other external bodies, and public interest and emergency disclosures that are made in accordance with the Act.

Identity protection (confidentiality)

A person cannot disclose the identity of a discloser, or information that is likely to lead to the identification of the discloser (and which they obtained directly or indirectly because the discloser made a disclosure that qualifies for protection).[41]

This requirement applies whether or not confidentiality is requested. The discloser must specifically consent to their identity being revealed.

Exceptions to this confidentiality requirement apply when a person discloses the identity of a discloser –

(a) to ASIC, APRA, or a member of the Australian Federal Police;[42]

(b) to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Act);

(c) to a person or body prescribed by regulations;[43] or

(d) with the consent of the discloser.

Further, the identity protection requirement does not extend to other information contained in a disclosure. A person can disclose it with or without the discloser's consent if –

(a) the information does not include the discloser's identity;

(b) the company 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.

It is thus important to note that it is illegal for a person to identify a discloser, or disclose information that is likely to lead to the identification of the discloser, outside the above listed exceptions.

[41] S.1317AAE(1) of the *Corporations Act* and s.14ZZW(1) of the *Taxation Administration Act*.
[42] Or the ATO in the case of a tax disclosure: see s.14ZZW(2)(a) of the *Taxation Administration Act*.
[43] No persons or bodies have been prescribed as at the date of this policy.

A discloser can lodge a complaint with the company about a breach of confidentiality. The complaint should be lodged with the company's Whistleblower Protection Officer (named in Section 13 below).

A discloser may also lodge such a complaint with a regulator, such as ASIC, APRA or the ATO.

Protection from detrimental acts or omissions

There are laws protecting a discloser, and any other person, from detriment in relation to a disclosure.

Specifically, it is an offence for a person to engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if –

(a) the person believes or suspects that the discloser (or another person) made, may have made, proposes to make, or could make, a disclosure that qualifies for protection; and

(b) the belief or suspicion is the reason, or part of the reason, for the conduct.[44]

It is also an offence to make a threat to cause detriment to a discloser (or another person) in relation to a disclosure or potential disclosure. The threat may be express or implied, or conditional or unconditional. It need not be proved that the person threatened actually feared that the threat would be carried out.[45]

"Detriment"[46] is defined to include:

(a) dismissal of an employee;

(b) injury of an employee in his or her employment;

(c) alteration of an employee's position or duties to his or her disadvantage;

(d) discrimination between an employee and other employees of the same employer;

(e) harassment or intimidation of a person;

(f) harm or injury to a person, including psychological harm;

(g) damage to a person's property;

(h) damage to a person's reputation;

(i) damage to a person's business or financial position; or

(j) any other damage to a person.

Examples of actions that are not detrimental conduct include:

(a) administrative action that is reasonable for the purpose of protecting a discloser from detriment (e.g. moving a discloser who has made a disclosure about their immediate work area to another office to prevent them from detriment); and

(b) properly managing a discloser's unsatisfactory work performance.

Compensation and other remedies

A discloser (or any other employee or person) can seek compensation, injunctions and other remedies through the courts if they suffer loss, damage or injury because of a disclosure.

In deciding whether to grant a remedy, a court may take into account whether the entity concerned took reasonable precautions, and exercised due diligence, to avoid the detrimental conduct.[47]

Disclosers considering such court action should consult a lawyer.

Civil, criminal and administrative liability protection[48]

[44] S.1317AC(1). Also s.14ZZY(1) of the *Taxation Administration Act*.
[45] S.1317AC(2)-(5). Also s.14ZZY(2)-(4) of the *Taxation Administration Act*.
[46] S.1317ADA. Also s.14ZZZAA of the *Taxation Administration Act*.
[47] Ss.1317AD and 1317AE. Also s.14ZZZA of the *Taxation Administration Act*.
[48] S.1317AB. Also s.14ZZX of the *Taxation Administration Act*.

A discloser is protected from any of the following in relation to their disclosure:

(a) civil liability (e.g. any legal action against the discloser for breach of an employment contract, duty of confidentiality or another contractual obligation);

(b) criminal liability (e.g. attempted prosecution of the discloser for unlawfully releasing information, or other use of the disclosure against the discloser in a prosecution, other than for making a false disclosure); and

(c) administrative liability (e.g. disciplinary action for making the disclosure).

However, the protections do not grant immunity for any misconduct a discloser has engaged in that is revealed in their disclosure.

9. Support and practical protection for disclosers

This Section sets out how the company plans to take practical steps to support disclosers, and protect them from detriment. It is not intended to be exhaustive. Nor is it the case that every step listed may be necessary or appropriate in any given situation. It will depend on the circumstances of the case.

Examples of how the company will or might protect the confidentiality of a discloser's identity are:

(a) personal information and references to the discloser may be redacted;

(b) the discloser may be referred to in a gender-neutral manner;

(c) the discloser will be consulted as to how their disclosure might identify them;

(d) disclosures will be handled and investigated by qualified staff;

(e) all paper and electronic documents and other materials will be stored securely;

(f) the same will not to be sent to an email or printer accessible by other staff;

(g) access to the same will be limited to those people handling or investigating the disclosure;

(h) the number of those people will be limited as far as possible; and

(i) those people will be reminded about the confidentiality requirements and offences.

The Whistleblower Protection Officer named in Section 13 is responsible for discussing with a discloser the measures proposed to better ensure their identity remains confidential.

However, disclosers need to be aware that others may be able to guess their identity if, for example, they have been told the relevant information by those other people, or if they are one of a small number of people privy to that information.

Examples of how the company will or might protect the discloser from detriment are:

(a) the risk of harm, isolation, harassment and other detriment (including to other staff who might be suspected to have made a disclosure) will be assessed (and addressed) promptly;

(b) if detriment has already occurred, steps to protect a discloser will be devised and enacted;

(c) the discloser may be moved to another location, or reassigned to another (equivalent) role;

(d) other staff involved in the disclosable matter may be suspended, reassigned or relocated;

(e) a discloser will be advised of their rights as regards detriment, and to make a complaint;

(f) support services (such as counselling) may be made available to a discloser;

A discloser may seek independent legal advice or contact regulatory bodies, such as ASIC, APRA or the ATO, if they believe they have suffered detriment.

10. How the company will handle and investigate a disclosure

This Section outlines the key steps the company will take after it receives a disclosure. However, it is to be noted that the process (including timelines given) may vary depending on the nature of the disclosure.

Firstly, within 3 business days, the recipient will acknowledge receipt of the disclosure to the discloser (if contactable) in writing, and also assess the disclosure to determine if –

(a) it qualifies for protection; and

(b) a formal, in-depth investigation is required.

Secondly, if an investigation is required, then within a further 10 business days, the recipient will determine the following (and also advise the discloser in writing as to the same):

(a) the nature and scope of, and the key steps to be taken in, the investigation;

(b) the person(s) within and/or outside the company that should lead the investigation;

(c) the nature of any technical, financial or legal advice that may be required to support the investigation; and

(d) the timeframe for the investigation.

Generally, the investigation proper should commence no later than 10 business days after those determinations. However, if the discloser has any feedback to provide regarding those determinations, it should be provided within 5 business days to the recipient of the disclosure, who must then consider that feedback and, if he or she deems it appropriate, modify those determinations accordingly.

After commencing, the investigation is generally to proceed in accordance with the key steps and timeframe so determined.

During that process, the discloser (if contactable) will be provided with regular updates on progress, the frequency of which may vary depending on the nature of the disclosure, and the nature of the process.

In the investigation process, the company must ensure appropriate confidentiality is maintained. It must also ensure investigations are objective, fair and independent (that is, independent of the discloser, the individuals who are the subject of the disclosure, and the department or business unit involved). Further, it must ensure appropriate records and documentation for each step in the process are prepared and kept.

A written report of the investigation, once finalised, will be prepared and provided to the discloser (provided contact details for the discloser have been given, and noting, however, that there may be circumstances where it may not be appropriate to provide some or all details to the discloser).

The contents of the report will depend on the nature of the disclosure (particularly the seriousness and extent of alleged wrongdoing) but, generally, the report must document the disclosure, summarise the investigation process including persons spoken to and documents sighted, and record the findings of the investigation, and the reasons for them.

Also, the documented findings must, at the same time, be provided to those responsible for oversight of this policy (see Section 13 below), but preserving confidentiality as required (see Section 8 above).

Limitations on the investigation process

Disclosers should note that certain constraints may impose limitations on the investigation process.

As outlined in Section 8 above, in the investigation process, those involved cannot disclose information to others that is likely to identify the discloser without their consent. There is an exception allowing the disclosure of information as reasonably necessary for investigating the issues raised provided it does not name, or tend to identify, the discloser (see Section 8 above).

However, it is possible that, if consent to identify is refused, or limited to disclosure of identity to the proposed investigator, the company may be restricted to investigating a disclosure by way of conducting a broad review on the subject matter or the work area disclosed, which may result in a limited outcome.

There may be other limitations on the investigation process. For example, the company may not be able to progress an investigation if it is not able to contact the discloser (e.g. if a disclosure is made anonymously and the discloser has refused to provide, or has not provided, a means of contacting them).

Also, if a discloser is dissatisfied with the outcome, the company will not reopen the investigation, unless new information is available (except in the case where it would not change the findings). A dissatisfied discloser may, however, lodge a complaint with a regulator, such as ASIC, APRA or the ATO.

11. Ensuring fair treatment of individuals mentioned in a disclosure

To ensure fair treatment of individuals mentioned in a disclosure, the company must, where applicable –

(a) handle disclosures confidentially, when it is practical and appropriate;

(b) ensure every disclosure is assessed as to whether it should be investigated;

(c) make it the clear objective of any investigation to determine whether there is enough evidence to substantiate or refute the matters reported;

(d) ensure any investigation is objective, fair and independent;

(e) ensure that any 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 taken; and

(f) ensure that any such employee has access to support services (e.g. counselling).

In particular, but subject to what follows, the company must ensure that any individual who is mentioned in a disclosure is aware that they will be the subject of an investigation, and also has a proper opportunity to respond to any allegations, before making any adverse finding against them.

However, in some cases, informing the individual at an early stage of an investigation may compromise the effectiveness of the investigation, such as when there may be concerns that the individual may destroy information, or the disclosure needs to be referred to ASIC, APRA, the ATO or the police.

12. Ensuring this policy is easily accessible

The company is required by law to make this policy available to its officers and employees.[49]

ASIC also expects the company to ensure it is widely disseminated to, and easily accessible by, them.[50]

The company will do so by –

(a) posting this policy on the company website and intranet (to ensure both staff and external disclosers have access to it);

(b) immediately after 1st January 2020, as well as immediately after any updated policy is issued, progressively holding briefing sessions for all staff to be briefed about the relevant laws and any updates to this policy, as appropriate;

(c) incorporating briefing sessions or materials into employee inductions (and which include information as to where an employee can access the full policy); and

(d) undertaking periodic "refresher training" by repeating steps outlined above as appropriate.

Any change to, or update of, this policy in future following a review must also be widely promulgated to all staff and other interested persons in similar manner.

The company will also –

(a) periodically train managers in how to effectively deal with disclosures; and

[49] S.1317AI(2)(b).
[50] RG270.129.

(b) ensure that its eligible recipients named in Section 7 of this policy receive training in the company's processes and procedures for receiving and handling disclosures, including training relating to confidentiality, the prohibitions against detrimental conduct, and their obligations under the Act (and the *Taxation Administration Act*, where applicable).

13. Roles, reporting and review

The company's Whistleblower Protection Officer is Compliance Director Stephen Palyga. His details are set out in Section 7 above.

The Whistleblower Protection Officer is appointed by the Board of Directors of the company, and the Board may also remove and replace him or her at any time.

The Whistleblower Protection Officer has responsibility for –

(a) the day-to-day oversight of the processes and procedures of this policy, and its effectiveness;

(b) protecting and safeguarding disclosers;

(c) ensuring the integrity of the processes provided for in this policy;

(d) the privacy, security[51] and confidentiality of personal and other information received in a disclosure and any investigation;

(e) arranging for training, education and communications about this policy;

(f) periodically reviewing and updating this policy, as elaborated below;

(g) implementing any amendments to this policy; and

(h) the other actions elsewhere assigned to him or her in this policy.

The Whistleblower Protection Officer may co-opt the company's legal counsel and human resources staff to assist him or her in carrying out those responsibilities, or with specific investigations.

The company's Board of Directors has ultimate oversight of the processes and procedures of this policy, and its effectiveness, as well as responsibility for approving any updates proposed to this policy.

The company's Whistleblower Protection Officer must periodically report to the Board of Directors of the company on any disclosures made, including (to the extent confidentiality permits):

(a) the subject matter of each disclosure;

(b) the investigation action taken for each disclosure;

(c) the timeframe for finalising each disclosure; and

(d) the outcome of each disclosure.

The Whistleblower Protection Officer may also consult the Board of Directors of the company as to how to deal with any disclosure made, or he or she may escalate a matter to it if appropriate.

The Whistleblower Protection Officer will also periodically review this policy.[52] The purpose of the review is to ensure this policy, and the measures it contains, are effective, up-to-date, relevant and robust, and have adequately dealt with any disclosures that may have arisen.

If appropriate, the company will engage an external person to assist in that review or, alternatively, conduct an independent review.

Upon any such review, the Whistleblower Protection Officer may suggest amendments to this policy to the Board of Directors of the company for consideration and adoption.

---

[51] See Regulatory Guide 270, paragraphs RG270.147-RG270.149, for guidance on ensuring privacy and security.
[52] See Regulatory Guide 270, paragraphs RG270.158-RG270.160, for suggested inquiries and actions for such a review. Paragraphs RG270.153-RG270.156 also refer to statistical and other information which might be collected to inform any review.

Version history of this policy

The original version of this policy was written for Principal Finance Pty Ltd in late 2019 and promulgated effective from 1st January 2020. Principal Finance Pty Ltd, Premium Funding Pty Ltd and PF Advance Pty Ltd were acquired in January 2021 by PF BidCo Pty Ltd which, as a result, became a large proprietary company on 30th June 2022, as did its holding companies. Also as noted above, Principal Finance Pty Ltd became a large proprietary company on 30th June 2024.

Consequently, this policy was re-written to specifically extend to all large proprietary companies in the Arteva Funding Group, as well as reviewed by both the Chief Experience Officer Sally Richardson and the Whistleblower Protection Officer for currency, accuracy and robustness, and this version was issued for Board approval on 16th September 2024.