MORE GROUP WHISTLEBLOWER POLICY

1. Introduction

This Policy applies to the More Group of companies ("**More**" or the "**More Group"**), including:

- More Telecom Pty Ltd;
- Tangerine Telecom Pty Ltd;
- More Services Pty Ltd;
- More Telecom Australia Pty Ltd;

More Connect Pty Ltd;

- More Bookkeeping Services Pty Ltd; and
- PayNuts Pty Ltd.

The More Group is committed to operating legally, properly, and ethically, and creating a transparent and open environment where people feel comfortable raising concerns.

This Policy is a small step in supporting this mission, and sets out the protections available to whistleblowers, what matters are reportable, how you can report your concerns without fear of backlash, and how the More Group will support and protect you.

2. Scope

This Policy applies to all past and current More Group:

- Directors;
- employees;
- contractors;
- suppliers (including their employees); and
- associates,

as well as all other relevant individuals defined under the *Corporations Act 2001* (Cth) (**Corporations Act**) as "eligible whistleblowers".

Please note that this Policy does not apply to matters relating to workplace grievances. For workplace grievances, More Group employees and contractors should refer to the More Grievance Procedure.

3. General Principles

3.1 Who is an "eligible whistleblower"?

A person making a disclosure is an eligible whistleblower covered by this Policy if they are or have been:

- an officer or employee (e.g. current and former employees who are permanent, part-time, fixed-term or temporary, interns, secondees, managers, and Directors);
- a supplier of services or goods to the More Group (whether paid or unpaid), including their employees (e.g. current and former contractors, consultants, service providers and business partners);
- an associate of the More Group; and/or
- a relative, dependant or spouse of an individual set out above (e.g. relatives, dependants or spouse of current and former employees, contractors, consultants, service providers, suppliers and business partners).

You must hold, or have held in the past, one of these roles in order to access the protections available under this Policy (even if you make a whistleblower report anonymously).

3.2 **Disclosable matters**

A "disclosable matter" involves information that the discloser has reasonable grounds to suspect concerns misconduct, or an improper state of affairs or circumstances, in relation to More (or a related body corporate of More).

Examples of this may include:

- illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- failure to comply with, or breach of, legal or regulatory requirements;
- 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.

A disclosable matter also includes conduct that may also not involve a breach of a particular law. For example, information that indicates a significant risk to public safety or the stability of, or confidence in, the financial system is also a disclosable matter, even if it does not involve a breach of a particular law.

Finally, a discloser can still qualify for protection even if their disclosure turns out to be incorrect.

3.3 **Personal work-related grievances**

Disclosures relating to personal work-related grievances do not qualify for protection under the Corporations Act, such as:

- an interpersonal conflict between the discloser and another employee;
- a decision that does not involve a breach of workplace laws;
- a decision about the employment, engagement, transfer or promotion of the discloser;
- a decision about the terms and conditions of employment or engagement of the discloser;
- a decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

A personal work-related grievance may still qualify for protection if:

- it includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report);
- More 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;
- the discloser suffers from or is threatened with detriment for making a disclosure;
- the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Corporations Act.

For personal work-related grievances, please refer to the More Grievance Procedure.

3.4 **False reporting**

It is strictly prohibited to make an intentionally false report under this Policy (i.e. a report that the discloser knows to be untrue) and disclosers found to have made an intentionally false report may face disciplinary action (including up to termination of employment or engagement).

3.5 **Who should disclosures be made to?**

We strongly encourage all disclosable matters to be reported internally in the first instance to the **Whistleblower Protection Officer** (currently the General Counsel & Head of Risk and Compliance, or in the case of their absence, the Head of People and Culture).

The Whistleblower Protection Officer is tasked with:

- managing the disclosure process (including reporting, investigations and communicating outcomes to stakeholders);
- identifying risks to an eligible whistleblower within the organisation and the workplace; and
- putting in place appropriate measures to ensure eligible whistleblowers are protected from prohibited conduct by other members of the More community.

You can make a disclosure directly to other internal "eligible recipients", particular regulators, or a legal practitioner, about a disclosable matter and qualify to receive protection under the legislation.

An "eligible recipient" can be any of the following:

- any director, officer or senior manager of any More Group company;
- an internal or external auditor of any More Group company; or
- a person or third party service provider authorised by More to receive disclosures that may qualify for protection.

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 Corporations Act are protected (even if the legal practitioner concludes that a disclosure does not relate to a 'disclosable matter').

Disclosures of information relating to disclosable matters can be made to ASIC, APRA or another Commonwealth body prescribed by regulation and qualify for protection under the Corporations Act.

3.6 **Can you remain anonymous?**

If an eligible whistleblower wishes to remain anonymous, More will maintain the confidentiality of their identity, except where required to disclose this by law, where an exception applies under the Corporations Act, or with the consent of the discloser.

When this occurs, the eligible whistleblower may still use the same processes for reporting set out in this Policy, noting explicitly that they wish to remain anonymous.

However, please be aware that where a disclosure is made anonymously, this may limit thorough investigation and proper resolution of the matter. We suggest that if you wish to remain anonymous, you should maintain ongoing two-way communication with More to allow us to ask follow-up questions as part of our investigation and to provide feedback on the process and outcome.

3.7 **Emergency disclosures**

If you have reasonable grounds to believe that information you have reported concerns a substantial and imminent danger to the health or safety of any third party, or to the natural environment, you may consider making an "emergency disclosure" to a journalist or parliamentarian, provided that:

- you have first made a disclosure of the information to an authorised regulatory body (e.g. ASIC);
- before making the emergency disclosure, you have given written notice to same regulatory body that:
    - includes sufficient information to identify the previous disclosure; and
    - states that you intend to make an emergency disclosure; and
- your disclosure must contain no more information than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

We recommend you contact an independent legal adviser before making an emergency disclosure.

3.8 **Public interest disclosures**

If you have reasonable grounds to believe that the information you have reported is in the public interest, you may consider making a "public interest disclosure" to a journalist or parliamentarian, provided that:

- at least 90 days have passed since you made an initial report to the disclosure to an authorised regulatory body (e.g. ASIC);
- you do not have reasonable grounds to believe that action is being, or has been taken, in relation to the disclosure,
- you have reasonable grounds to be believe that making a further disclosure of the information is in the public interest; and
- before making the public interest disclosure, you have given written notice to the same regulatory body that:

- includes sufficient information to identify the previous disclosure; and
- states that you intend to make a public interest disclosure.

We recommend you contact an independent legal adviser before making a public interest disclosure.

4. How to make a whistleblower report

4.1 Reporting internally

A report can be made confidentially to the More Group Whistleblower Protection Officer by:

- sending an email to wpo@more.com.au; or
- completing and submitting a report using the webform available at https://tangerinetelecom.com.au/whistleblower-reporting.

Alternatively, you can make a report directly to any other internal More Group eligible recipient using the contact details available for those individuals on More Group's internal contact directory.

For disclosures made to any More Group eligible recipient directly, the eligible whistleblower should document their concerns in writing, mark any email correspondence with "PRIVATE & CONFIDENTIAL".

You should include as much information as possible about the alleged breach in your report so that it can be investigated, including:

- the nature of the alleged breach;
- the person or persons responsible for the alleged breach;
- the facts on which the eligible whistleblower's belief, that a breach has occurred and has been committed by the person/s named, are founded; and
- the nature and whereabouts of any further evidence that would substantiate the eligible whistleblower's allegations, if known.

The above disclosures can be made anonymously, confidentially, securely and outside of business hours.

4.2 Reporting externally

If you have chosen to make a protected disclosure to an applicable regulatory body, More requests that you consider also notifying More. This is not required, but it will assist More to ensure it is doing everything possible to support and assist you.

More may also nominate external persons to whom, or agencies to which, disclosures may be made under the protections offered under this Policy. Where such a nomination is made, employees will be informed by any appropriate method.

5. What happens after a disclosure is made?

5.1 Investigation

Once a disclosure is made, More will assess whether the disclosure qualifies for protection, and whether a formal, in-depth investigation is required.

On initial assessment:

- More may commence an internal investigation, or seek further information and provide feedback to the eligible whistleblower (NB: where an investigation is warranted, More may, where appropriate, choose to have the matter investigated by an external third-party);
- depending on the nature of the matter, the information may be shared with the Board or a Board Director, subject to any confidentiality requirements;
- More may hold a meeting with the eligible whistleblower to assess the report and determine further actions;
- if More determines that it will need to investigate a disclosure, More will determine:
    - the terms of the investigation;
    - the nature and scope of the investigation;
    - the person(s) within and/or outside More that should lead that investigation;
    - the nature of any technical, financial or legal advice that may be required to support the investigation; and
    - the timeframe for the investigation.

if More determines that the disclosure is unquestionably trivial, fanciful, or is not based on reasonable grounds, More may dismiss the disclosure and notify the discloser of its decision.

If More determines that an investigation is warranted, More will keep the eligible whistleblower informed regularly (provided they have made their contact details available) at each key stage of the investigation.

More will ensure investigations are undertaken in a manner that maintains confidentiality, good document management and clear communication, and will keep appropriate records and documentation at each stage of the investigation.

5.2 **Response**

Once an investigation is concluded and finalised, the investigator will provide a report to the Whistleblower Protection Officer and the More Group directors setting out the findings and recommendations from the investigation, including next steps (if any). The method for documenting and reporting the findings will depend on the nature of the disclosure, and there may be circumstances where it may not be appropriate to provide details of the outcome to the discloser.

6. Legal protections for whistleblowers

6.1 **Overview of Protections**

Disclosers that qualify for protection under the Corporations Act receive the following protections:

- identity protection (confidentiality) (unless you give your consent to be identified or specific limited exceptions apply);
- protection from detrimental acts or omissions;
- compensation and other remedies; and
- civil, criminal and administrative liability protection.

6.2 **Identity protection (confidentiality)**

Where necessary to protect an eligible whistleblower, More will ensure:

- all personal information or reference to the eligible whistleblower witnessing an event will be redacted;
- the eligible whistleblower will be referred to in a gender-neutral context;
- where possible, the eligible whistleblower will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them; and
- disclosures will only be handled and investigated by appropriate staff.
- More will also ensure that:
- all paper and electronic documents and other materials relating to disclosures will be stored securely;
- access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;
- only a restricted number of people who are directly involved in handling and investigating a disclosure will be made aware of a whistleblower's identity (subject to the whistleblower's consent) or information that is likely to lead to the identification of the whistleblower;
- communications and documents relating to the investigation of a disclosure will not be sent to an email address or to a printer that can be accessed by other staff; and
- each person who is involved in handling and investigating a disclosure will be reminded about their confidentiality obligations (including that an unauthorised disclosure of a whistleblower's identity may be a criminal offence).

6.3 **Protection from detrimental acts or omissions**

A person cannot engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if:

- 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
- the belief or suspicion is the reason, or part of the reason, for the conduct.

In addition, a person cannot make a threat to cause detriment to a discloser (or another person) in relation to a disclosure. A threat may be express or implied, or conditional or unconditional. A discloser (or another person) who has been threatened in relation to a disclosure does not have to actually fear that the threat will be carried out.

Examples of detrimental conduct include dismissal of an employee, injury of an employee in their employment, alteration of an employee's position or duties to their disadvantage, discrimination, harassment or intimidation of a person, or damage to their property, reputation, business or financial position.

More will assess and control the risk of detriment against a discloser by taking the following steps:

- **Risk identification**: Assessing whether anyone may have a motive to cause detriment—information may be gathered from a discloser about:
    - the risk of their identity becoming known;
    - who they fear might cause detriment to them;

    - whether there are any existing conflicts or problems in the workplace; and
    - whether there have already been threats to cause detriment.
- **Risk analysis and evaluation**: Analysing and evaluating the likelihood of each risk and evaluating the severity of the consequences.
- **Risk control**: Developing and implementing strategies to prevent or contain the risks—for anonymous disclosures, More may assess whether the discloser's identity can be readily identified or may become apparent during an investigation.
- **Risk monitoring**: Monitoring and reassessing the risk of detriment where required—the risk of detriment may increase or change as an investigation progresses, and even after an investigation is finalised.

Further to the above, and where appropriate, the CEO shall designate an officer to be responsible for ensuring that the person suffers no employment-related disadvantage on account of their actions in this matter and to provide additional support for the person where necessary.

6.4 **Compensation and other remedies**

A discloser (or any other employee or person) can seek compensation and other remedies through the courts if:

- they suffer loss, damage or injury because of a disclosure; and
- More failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

All individuals are encouraged to seek their own independent legal advice if they believe the above has occurred.

6.5 **Civil, criminal and administrative liability protection**

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

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

The above protections do not however mean that disclosers can't be held responsible for their own actions. For example, making a disclosure doesn't mean that More cannot take disciplinary action against you for any misconduct that you are found to have engaged in. The protections relate to the making of the disclosure itself, and not in relation to any information that it reveals about your behaviour.

7. Responsibilities

7.1 **CEO**

Is responsible for appointing More's Whistleblower Protection Officer, receiving notifications and reports under this Policy, implementing appropriate action in response to reports and

investigations, ensuring staff comply with their obligations under this Policy, and conducting a review of this Policy every 2 years in conjunction with the Whistleblower Protection Officer.

7.2 **Whistleblower Protection Officer**

Is responsible for administering this Policy, including by ensuring it is accessible, that staff receive appropriate training and comply with it, and that the More Group complies with its legal obligations related to whistleblower disclosures.

Receives and assesses whistleblower reports, overseas investigations and corrective activities, and liaises with More Group directors in relation to all matters covered by this Policy.

7.3 **More employees**

All employees are responsible for reporting breaches of general law, organisational policy, or generally recognised principles of ethics to a person authorised to take action on such breaches.

8. Accessibility of this Policy

More will take steps to ensure that this Policy is made available to More's officers and employees and is easily accessible. For example, More will:

- store this Policy in a central location where it can be accessed by More all team members at any time;
- incorporate this Policy into its online education and training program for More team members;
- display this Policy on its website, accompanied by a webform that enables confidential reporting; and
- carry out appropriate training and education for senior managers and officers.

9. Breach of this Policy

Any breach of this Policy may result in counselling and/or disciplinary action, including up to termination of employment or cessation of engagement.

Employees must also acknowledge that a breach of this Policy may also constitute a breach of applicable legislation, which could result in legal or regulatory action (including criminal action and penalties), significant reputational damage and substantial financial loss.