



Group Whistleblower Policy.

Money in Motion



Policy Overview

Purpose	<p>EML is committed to providing a safe and collaborative work environment that encourages honesty and ethical behaviour, where Wrongdoing can be raised without fear of retribution. This Policy is an important tool for helping EML to identify Wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing it.</p> <p>To qualify for the protections outlined in this Policy, you need to make a Protected Disclosure. This Policy explains how to make a Protected Disclosure and how that Protected Disclosure will be handled by EML. If you make a Protected Disclosure, additional legal protections may also apply.</p>
Policy Objective	<p>The objectives of this Policy are to:</p> <ul style="list-style-type: none">• Encourage genuine concerns about possible Wrongdoing in relation to EML to be raised as soon as possible.• Help detect, address, prevent and act on Wrongdoing that may arise.• Provide guidance in relation to how to raise concerns about Wrongdoing and make a Protected Disclosure.• Explain how Protected Disclosures will be investigated and the support and protection available to those who make Protected Disclosures under this Policy.
Policy Scope	<p>This Policy applies to all entities within EML and Eligible Whistleblowers (as set out in the Definitions section of this Policy.)</p>
Policy Ownership	<p>The Policy is owned by the Chief Risk and Compliance Officer (the “Policy Owner”) and forms part of the Risk and Compliance Policy Framework.</p>

Policy Background

Business Summary	<p>As a global organisation, EML is required to comply with distinct legal and regulatory obligations across the jurisdictions in which it operates. Accordingly, this Policy has been prepared in two parts:</p> <ul style="list-style-type: none">• the main body of the Group Whistleblower Policy which applies across EML; and• supplementary country-specific policy provisions set out in the Annexure to this Policy which may vary the terms and/or operation of this Policy to reflect local requirements. These supplementary country-specific provisions should be read in conjunction with this Policy. If there is inconsistency between this Policy and the country specific provisions or country-specific legislation, the country-specific provisions and legislation will apply to the extent of the inconsistency. <p>This Policy is not a summary of legal rights and obligations. Nothing in this policy is intended to change or take away any other protections which may be available at law. The Annexure highlights certain countries that have whistleblower related laws that may be applicable to particular circumstances. It is not intended to be an exhaustive list of countries, nor of potentially applicable laws.</p> <p>When determining how this Policy may apply to particular circumstances, first consider the main part of the Policy, and then consider the Annexure and whether any supplementary provisions apply to the country in which you are based. If you have questions about country specific obligations, please contact your business unit legal team or the Group General Counsel by email.</p>
Regulatory Landscape	<p>EML is subject to a range of whistleblowing, financial services and regulatory obligations across the jurisdictions in which it operates.</p> <p>Relevant legislative and regulatory frameworks relating to whistleblowing include, but are not limited to:</p>

Country	Laws
Australia	Corporations Act 2001 (Cth); ASIC Act 2001 (Cth); Banking Act 1959 (Cth); Financial Sector (Collection of Data) Act 2001 (Cth); Insurance Act 1973 (Cth); Life Insurance Act 1995 (Cth); National Consumer Credit Protection Act 2009 (Cth); Superannuation Industry (Supervision) Act 1993 (Cth)
Ireland	Protected Disclosures Act 2014 (Ireland), as amended; EU Whistleblower Protection Directive (EU) 2019/1937
United Kingdom	Public Interest Disclosure Act 1998 (UK); Employment Rights Act 1996 (UK), as amended
United States	Sarbanes-Oxley Act; Anti-Money Laundering Act and the Anti-Money Laundering Whistleblower Improvement Act of 2022. Please speak to the Group General Counsel should you require further advice as to State-specific laws. The Financial Crimes Enforcement Network (FinCEN) division of the Department of Treasury administers a Whistleblower Program that covers two categories of fraud: Bank Secrecy Act violations and sanctions violations.

This Policy is intended to support compliance with these laws by establishing minimum group-wide standards. Where local laws impose additional or higher requirements, those requirements are set out in Annexure B.

Policy Statement

Statement EML is committed to promoting a culture of openness and accountability and ensuring concerns about Wrongdoing can be raised without fear of retaliation or Detriment.

EML will not tolerate harassment, victimisation or any other form of Detriment against individuals who make Protected Disclosures in accordance with this Policy.

Disclosures will be handled objectively, confidentially and in a timely manner, having regard to applicable legal and regulatory requirements.

Definitions

Alternative Whistleblower	Means the Chair of the Audit & Risk Committee
Detriment	Means any threatened or actual injury, harm, prejudice, or disadvantage suffered by a Protected Discloser as a result of making a Protected Disclosure, including, but is not limited to: dismissal, suspension, demotion, or termination of your employment or engagement with EML; changes to your employment, position, or duties to your disadvantage; discrimination; threats, harassment or intimidation; harm or injury (including psychological harm); damage to property, reputation, business, or financial position.
Eligible Whistleblower	Means a person who is entitled to make a Protected Disclosure. This includes an individual who is a current and former: <ul style="list-style-type: none"> • employee or officer of EML, including temporary workers, contractors, interns and secondees. • contractor, supplier, or their employees who deals with EML. • directors or company secretaries of companies related to EML; or • spouse, relative or dependent of any of the above. <p>Note: This is not applicable to all jurisdictions, please refer to Annexure A relevant to your specific jurisdiction.</p>
EML	Means EML Payments Limited and each of its direct and indirect subsidiaries and branches.
Personal Work-Related Grievances	Has the meaning given within the Personal Work-Related Grievances section of the Policy.
Protected Disclosers	Means Eligible Whistleblowers who makes, or is entitled to make, a Protected Disclosure in accordance with this Policy and applicable law, regardless of whether the disclosure is ultimately substantiated, provided it was made with reasonable grounds at the time.

Protected Disclosure Is a concern about a Wrongdoing raised by an Eligible Whistleblower in accordance with this Policy. Senior Manager has the same meaning as in the Corporations Act and includes the Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, Chief Compliance Officer, Chief People Officer, and General Counsel/Company Secretary.

Senior Manager Means the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Risk and Compliance Officer, Chief People Officer, and General Counsel/Company Secretary.

Whistleblowing Protection Officer(s) Are the individuals identified in Annexure A of this Policy.

Wrongdoing Including information which an Eligible Whistleblower has reasonable grounds to suspect is:

- misconduct;
- an improper state of affairs or circumstances, by EML;
- dishonest, fraudulent, or corrupt conduct, including bribery or other activity in breach of the EML Anti-bribery Policy;
- illegal activity (such as theft, violence, harassment or intimidation, criminal damage to property or other breaches of state or federal law);
- unethical or breach of EML' policies (such as dishonestly altering company records or data, adopting questionable accounting practices or wilfully breaching EML's Code of Conduct or other policies or procedures);
- is potentially damaging to EML, an EML employee or a third party, such as unsafe work practices, environmental damage, health risks or abuse of EML's property or resources;
- is an abuse of authority;
- may cause financial loss to EML or damage its reputation or be otherwise detrimental to EML's interests;
- in some regions, conduct involving harassment, discrimination, victimisation or bullying, where it is not a Personal Work-related Grievance under applicable law;
- conduct that constitutes an offence against, or contravention of, a provision of any law specified in the Regulatory Landscape Section of this Policy, including applicable financial, trade or transport sanctions;
- constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more; or
- represents a danger to the public or the financial system;

Note: This is not applicable to all jurisdictions, please refer to Annexure A relevant to your specific jurisdiction.

Core Whistleblowing Framework and Reporting

How do I make a Protected Disclosure?

To be eligible for the legal protections outlined in this Policy, you must:

- be an Eligible Whistleblower.
- report your concerns to a Whistleblower Protection Officer specified in this Policy, or to Your Call (see below), or to certain other authorized persons as set out in the Annexure; and
- have reasonable grounds to suspect Wrongdoing in relation to EML.
- If your disclosure meets all three of the above criteria, it is a Protected Disclosure.

If your disclosure doesn't meet the above criteria, we still encourage you to raise your concerns with us. However, only Protected Disclosures receive the legal protections outlined in this Policy. Concerns that do not qualify as Protected Disclosures, such as certain personal grievances or workplace complaints should be raised in accordance with our grievance, complaints, or other relevant internal policies and procedures available on the EML Intranet.

Who should Protected Disclosures be made to?

Your Call

Eligible Whistleblowers are encouraged to speak up by contacting EML's external and independent whistleblower service provider named: Your Call Whistleblowing Solutions ("Your Call") to receive and manage your report with impartiality and confidentiality.

This option allows you to:

- remain completely anonymous; or
- identify yourself to Your Call only; or
- identify yourself to both Your Call and an appropriate person at EML.

You may choose to remain anonymous; however, anonymity can significantly limit thorough investigation and proper resolution of the matter.

The Your Call reporting options are set out in the table below.

Website: (24/7)	https://www.yourcall.com.au/report Log in using the unique identifier code: EML You can upload supporting documentation and/or material securely here
Telephone: (9am to 12am recognized) business days (AEST)	Australia: 1300 790 228 Outside of Australia +61 3 9895 0012 (call charges will apply)
Accessibility options	If you are deaf, or have a hearing or speech impairment, you can contact Your Call online or through the National Relay Service. Simply choose your contact method at www.relayservice.gov.au and request Your Call's hotline 1300 790 228. If you have difficulty speaking or understanding English, contact us through the Translating and Interpreting Service (TIS) 131 450 and ask for Your Call on 1300 790 228.

Your Call always remains the intermediary, receiving and forwarding communication between all parties. The Whistleblowing Protection Officers who will have access to your reports (but not your personal details if you remain anonymous or only identify yourself to Your Call), are detailed in Annexure A.

In the circumstance where all listed Whistleblower Protection Officers are unable to receive the report (for example, due to a conflict of interest), the Alternative Whistleblower Protection Officer will be notified of the report. You will be able to securely upload any relevant documentation and/or material relevant to your disclosure if you wish.

After making a disclosure, you will be provided with a unique Disclosure Identification Number (DIN) and access to a secure online Message Board. The Message Board allows you to have ongoing anonymous communication with Your Call and/or EML. Your Call always remains the intermediary, receiving and forwarding communication between all parties. The Message Board can also be used to receive updates, share further information/evidence and request support or report retaliation. If you cannot access the Message Board, you can contact Your Call via phone (above) for verbal updates.

Whistleblowing Protection Officers

Eligible Whistleblowers can also contact any of EML's Whistleblower Protection Officers (WPO's) listed in Annexure A

Other parties

Disclosures can also be made to specific people and organisations as set out in the additional country specific provisions in Annexure B.

Note that this Policy has been designed to facilitate reporting of Wrongdoing to Your Call and within EML's internal reporting structures. If you intend to make a disclosure to other parties, it is recommended that you first seek legal advice in relation to your rights and obligations to ensure that your disclosure is a Protected Disclosure.

Can a disclosure be made anonymously?

You can choose to remain anonymous when making a disclosure of Wrongdoing, during the investigation process and after the investigation is finalised. You can also decide not to answer questions that you feel may reveal your identity. However, if you choose to remain anonymous, this may affect the ability of EML to investigate and communicate with you regarding your disclosure.

If you would prefer to remain anonymous, EML encourages you to make your disclosure using Your Call and maintain ongoing two-way communication with EML via that service so that EML can ask follow-up questions and provide feedback.

What information should be provided in a disclosure?

Ideally, a disclosure should contain enough information to form a reasonable basis for investigation. The discloser should provide as much information as possible about the events and persons involved. This includes details such as:

- the nature of Wrongdoing, when it occurred or is likely to occur (date, time, location).
- name of person(s) believed to be involved in the Wrongdoing; and
- names of possible witnesses and other supporting material if available, such as emails, documents.

Even if the information is proved to be incorrect or unsubstantiated, your disclosure may still be a Protected Disclosure, provided you had a reasonable basis for believing that the information was true.

Personal Work-Related Grievances

Generally, Wrongdoing does not include Personal Work-Related Grievances and concerns of this nature are unlikely to qualify for protection as a Protected Disclosure or be covered by this Policy. However, there are some limited exceptions in Australia and the United Kingdom. Further information can be found in Annexure B.

Personal Work-Related Grievances relate to an individual's current or former employment arrangements, performance, remuneration outcomes or personal circumstances that do not have significant implications for the organisation (for example an interpersonal conflict between you and another employee, or a decision about your employment that does not breach workplace laws).

EML has dedicated processes in place to handle personal work-place grievances. For concerns of this nature, please refer to the Employee Handbook.

Investigations

Upon receipt of a report under this Policy, the Whistleblower Protection Officer (WPO) will make a preliminary assessment (Preliminary Assessment) of the evidence presented. If, on the face of the evidence presented, a potential Wrongdoing has occurred, the WPO will notify the Chair of the Audit and Risk Committee, and they shall appoint an investigator (Investigator) who is an:

- internal investigator who is independent of the area where the wrongdoing is alleged to have occurred; or
- external investigator independent of EML, where considered necessary.

The Investigator must be a trained and qualified investigator. The investigation will not be conducted by a person who may be the subject of the investigation or has significant links or connections (actual or perceived) to the person(s) or practice(s) under investigation.

EML will thoroughly, objectively, and fairly investigate all matters reported in accordance with this Policy as soon as reasonably practicable. Investigations will remain confidential. Where appropriate, EML will notify the discloser of the progress and outcome of the investigation.

EML will take reasonable precautions to store any records relating to a report of Wrongdoing securely and to permit access by authorised persons only.

Protecting the Whistleblower

Protecting your identity

If you make a Protected Disclosure, it will be treated as confidential and EML will take all reasonable steps to protect your identity. Your identity (and any information that someone could likely use to work your identity) will only be disclosed if:

- it is required or allowed by law (for example disclosure by EML to a lawyer for the purpose of obtaining legal advice).
- you consent; or
- with respect to information that is likely to identify you, it is reasonably necessary to disclose the information for the purposes of an investigation, and all reasonable steps will be taken to reduce the risk that you be identified as a result (for example by removing your personal information or other details that are likely to identify you).

Note: This is not applicable to all jurisdictions, please refer to Annexure A relevant to your specific jurisdiction.

Retaliation and Detrimental Conduct

EML is committed to protecting Protected Disclosers against Detriment or retaliatory treatment (including dismissal, disciplinary action, or other unfavourable treatment).

EML will not tolerate any reprisals, discrimination, harassment, intimidation, or victimisation against a Protected Discloser. Such treatment will be regarded as serious misconduct and may result in disciplinary action, which may include dismissal.

Unauthorised disclosure of information relating to a Protected Disclosure, the identity of a person who has made a Protected Disclosure or information from which the identity of the Protected Discloser could be inferred will be regarded seriously and may result in disciplinary action, which may include dismissal and/or any civil, criminal, or administrative liability.

EML will protect Protected Disclosers from Detriment by:

- conducting a risk assessment of the disclosure to manage the risk of Detriment to the Whistleblower.
- where applicable, making such reasonable adjustments as required to allow the Whistleblower to perform their duties at work without being potentially exposed to Detriment (e.g. by changing reporting lines or location).
- implementing strategies to help the Whistleblower minimise and manage stress, time or performance impacts or other challenges resulting from the disclosure or its investigation.
- making available support services such as access to EML's independent Employee Assistance Program (EAP).

These protections are intended to be in addition to any rights and protections otherwise available to Protected Disclosers at law. A person who makes a disclosure and is implicated in the Wrongdoing may not be entitled to all the protections outlined in this Policy.

Nothing in this Policy prevents EML from raising and addressing matters that arise in the ordinary course of engagement or employment with EML, such as managing unsatisfactory work performance in accordance with EML's performance management framework.

A Protected Discloser who believes they have suffered Detriment as a result of making a Protected Disclosure should report this to Your Call or a Whistleblower Protection Officer.

Management of a person against whom a report is made

EML recognises the principles of natural justice; that an accusation does not automatically confer guilt; and that individuals who have been made aware that an accusation has been made against them must also be supported during the handling and investigation of the matter.

Where a person is identified as being suspected of possible Wrongdoing, and EML has determined that an investigation should be conducted, the person who is the subject of the Protected Disclosure may be, within the constraints of confidentiality:

- told about the substance of the allegations.
- given a fair and reasonable opportunity to respond to the allegations before the investigation is finalised; and
- informed about the findings of the investigation and given an opportunity to respond to those conclusions before any action is taken against them (subject to legal, privacy and confidentiality requirements).

EML will give its full support to a person who is the subject of a report where the allegations contained in the report are concluded to be clearly wrong.

Record Keeping and Reporting

To the extent required by law, EML will:

- retain confidential, accurate and secure records of a Protected Disclosure and investigation made under this Policy; and

- provide the Board and the Audit and Risk Committee with a confidential, anonymized summary of reports received and investigated under this Policy as appropriate.

Where an investigation is initiated, the Investigator must ensure that any individual who is the subject of a report:

- is informed of the substance of the allegations in a timely manner;
- is given a fair and reasonable opportunity to respond before any investigation is finalised.
- is made aware of any adverse findings or comments proposed to be included in any report arising from the investigation before it is finalised; and
- has their response set out fairly and accurately in the Investigator's report.

Following the completion of an investigation and where the individual concerned has been informed of the allegations or the fact of the investigation, then the Investigator must formally notify that individual of the outcome. Pending finalisation of a group-level policy on data protection; accordingly, all obligations in this area are governed by entities own procedures and applicable legal requirements.

False Reports

If a person is found to have deliberately made a false or malicious report, this may be considered a serious matter and result in disciplinary action which may include dismissal and/or any civil, criminal, or administrative liability.

Policy Implementation

Adequate Procedures

EML maintains arrangements to support the effective operation of its whistleblowing framework and to enable the reporting, handling and protection of Protected Disclosures in accordance with this Policy and applicable law. The whistleblowing framework is supported by:

- the use of an independent external whistleblowing service provider (Your Call) to facilitate confidential and anonymous reporting;
- procedures for receiving, assessing and managing whistleblowing disclosures;
- safeguards to protect confidentiality and personal information, underpinned by EML's privacy policies and related privacy procedures;
- record-keeping and reporting arrangements to support oversight and monitoring; and
- alignment with EML's Code of Conduct and related policies that describe expected standards of behaviour and the types of matters that may be reported.

These arrangements operate together to support consistent and appropriate management of whistleblowing disclosures across EML.

Roles and Responsibilities

Group Board	Ultimate oversight of EML's whistleblowing framework and culture, ensuring appropriate arrangements exist for the receipt, handling and protection of whistleblowing disclosures.
Audit and Risk Committee	Oversight of whistleblowing arrangements on behalf of the Group Board, including review of whistleblowing reports, trends, outcomes, and the effectiveness of the whistleblowing framework.
Regional Boards	Oversight of compliance with applicable regional whistleblowing legal and regulatory requirements within their region, and escalation of material whistleblowing matters where required.
Global Risk and Compliance	Overall responsibility for maintaining this Policy, training and awareness, second line monitoring and testing of the implementation of this Policy and providing reporting to the Audit & Risk Committee and Group Board.
Global Risk	Ensuring the EML risk management framework adequately captures, manages and mitigates applicable risks.
Regional Risk and Compliance	Ensuring appropriate second line oversight arrangements (regional or global) are in place for each legal entity within their region. The Head of Regional Risk and Compliance for each region is also responsible for local board and committee reporting within their region.
Internal Audit	Providing independent assurance on the design and effectiveness of whistleblowing governance, controls and processes, without involvement in the handling or investigation of individual disclosures.
Directors and Senior Managers	Promoting a culture of ethical conduct, openness and accountability, and taking reasonable steps to support the effective operation of the whistleblowing framework within their areas of responsibility.
Whistleblower Protection Officers	Receiving, assessing and managing whistleblowing disclosures in accordance with this Policy, including maintaining confidentiality, coordinating investigations where required, and supporting Eligible Whistleblowers and Protected Disclosers throughout the disclosure process.
All applicable persons	Acting honestly and ethically, complying with this Policy and applicable laws, and reporting suspected Wrongdoing in accordance with this Policy.

Governance and Oversight

Monitoring and Reporting	<p>Whistleblowing is in scope of second line and third line monitoring and testing to provide assurance to applicable boards and committees.</p> <p>Horizon scanning is conducted in all countries in which EML is regulated. Any material changes to applicable Whistleblowing laws, regulations or guidance will be reported to the applicable regional and global committees and boards in accordance with internal reporting requirements.</p>
Training and Awareness	<p>EML will provide training to employees, Directors, Officers, and Senior Managers that includes their rights, obligations, responsibilities and required actions when disclosing or receiving a Disclosable Matter. The training will take place:</p> <ul style="list-style-type: none">• as part of their induction process; and• on annual basis thereafter.
Review, Approval and Change Management	<p>The Audit and Risk Committee will review this policy annually or as required to:</p> <ul style="list-style-type: none">• Comply with changes to applicable laws and regulations;• respond to emerging risks; or• ensure reports pursuant to, or breaches of, this Policy are appropriately recorded, investigated and responded to. <p>Any material changes to this Policy are subject to approval by the Audit and Risk Committee.</p>

Policy Governance

Approver Audit and Risk Committee on behalf of the EML Payments Group Board

Exemption Authority Group Risk and Compliance

Owner EML Payments Chief Risk & Compliance Officer

Review Cycle Annual

Next Review Date February 2027

Document Classification Policy - Internal

Material Revisions

Version	Approval Date	Effective Date	Details
3	16/12/2020	16/12/2020	First global policy
3.1	25/09/2023	25/09/2023	Routine Review. Admin error noted on version number.
4	18/06/2024	18/06/2024	Periodic review. The ownership of the policy changed to Risk and Compliance from Legal and Compliance
5	23/02/2026	23/02/2026	Reformatted to new policy template and updated to reflect regulatory changes (UK sanctions and sexual harassment disclosures); non-material policy clarifications and re-wording

Annexure A Whistleblower Protection Officers

Australian Hareta McMullin, Head of Business Partnering

North American Tonya Holmberg, Human Resources Business Partner

**Europe and
United Kingdom:** James Kaleda, Director of HR Operations and Shared Services

Staff may reference the EML Global Directory to obtain the current contact details for any of the above referenced officers.

Your Call can replace any of the above Officers with the Alternative Whistleblowing Protection Officer upon your request.

Annexure B Country Specific Whistleblowing Legal Requirements

Global Whistleblower Standard

ISO 37002 Whistleblowing management systems provides guidelines for implementing, managing, evaluating, maintaining, and improving a robust and effective management system within an organization for whistleblowing. ISO 37002 guides organizations in managing:

- How concerns of Wrongdoing are identified and reported
- How concerns of Wrongdoing are assessed
- How concerns of Wrongdoing are addressed
- How whistleblowing cases are closed.

The EML Whistleblower Policy in principle meets the ISO 37002 standards.

Australia

In addition to the protections provided by this Policy, the Corporations Act 2001 (Cth) provides that a Protected Disclosure can be made by an Eligible Whistleblower making a disclosure of a Disclosable Matter to an Eligible Recipient. Eligible Recipients under the Act include the following persons:

Eligible Recipients of a Whistleblower Complaint

- A Whistleblower Protection Officer (as specified in the Policy).
- A Director or Officer of EML.
- A Senior Manager of EML.

Disclosures to external authorities and entities

In accordance with the Corporations Act 2001 (Cth) a Protected Disclosure can also be made externally to one of the following:

- A legal practitioner for the purposes of obtaining legal advice or legal representation about the operation of the whistleblower provisions in the Corporations Act.
- ASIC, APRA, or a Commonwealth authority prescribed under the Corporations Act.
- An actuary, auditor or member of an audit team conducting an audit of EML.

A disclosure that raises concerns about the tax affairs of EML or one of its associates, may also be raised to either an Eligible Recipient (including Your Call) or:

- A legal practitioner for the purposes of obtaining legal advice or legal representation.
- The Commissioner for Taxation.
- A registered tax agent or BAS agent who provides tax agent services to EML; or
- An auditor or member of the audit team conducting an audit of EML and may be a Protected Disclosure under the Taxation Administration Act 1953 (Cth) if it meets certain criteria.

You are expected to have reasonable grounds to suspect that the information you are disclosing concerns a disclosable matter to the best of your knowledge and belief.

Other disclosures

The protections under this Policy can also apply to an Eligible Whistleblower who makes a 'public interest disclosure' or an 'emergency disclosure'. However, if a disclosure of Wrongdoing is made to the public in another way, the protections afforded under this Policy do not apply.

Public interest disclosures

A disclosure made under the pretext of being in the public interest is protected under this Policy. A disclosure in the public interest can only be made if it complies with the following strict requirements:

- the Eligible Whistleblower has disclosed a Disclosable Matter to ASIC, APRA, or a prescribed Commonwealth authority (previous disclosure).
- the Eligible Whistleblower has reasonable grounds to believe that making a further disclosure would be in the public interest.
- after at least 90 days has passed since the previous disclosure was made, the Eligible Whistleblower must give the body to which the previous disclosure was originally made, a written notification that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the Eligible Whistleblower intends to make a public interest disclosure; and
- the public interest disclosure is made to:
 - a member of the Parliament of the Commonwealth, the Parliament of a State, or the legislature

- of a Territory; or
- a journalist;
- and the extent of the information disclosed in the public interest disclosure is no greater than is necessary to inform the journalist or member of Parliament of the Disclosable Matter.

Emergency disclosures

A disclosure made under the pretext of an emergency disclosure is protected under this Policy. An emergency disclosure can only be made if it complies with the following strict requirements:

- the Eligible Whistleblower has disclosed a Disclosable Matter to ASIC, APRA, or a prescribed Commonwealth authority (previous disclosure).
- the Eligible Whistleblower has reasonable grounds to believe that information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment.
- the Eligible Whistleblower gives the body to which the previous disclosure was originally made, a written notification that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the Eligible Whistleblower intends to make an emergency disclosure; and
 - the emergency disclosure is made to:
 - a member of the Parliament of the Commonwealth, the Parliament of a State, or the legislature of a Territory; or
 - a journalist;
 - the extent of the information disclosed in the public interest disclosure is no greater than is necessary to inform the journalist or member of Parliament of the of the substantial and imminent danger.

Journalist means a person who is working in a professional capacity as a journalist for any of the following:

- a newspaper or magazine.
- a radio or television broadcasting service.
- an electronic service (including a service provided through the internet) that:
 - is operated on a commercial basis, or operated by a body that provides a national broadcasting service (within the meaning of the Broadcasting Services Act 1992); and
 - is similar to a newspaper, magazine or radio or television broadcast.

Specific protections and remedies

If you make a “Protected Disclosure”, the law provides that:

- you will not be subject to any civil, criminal, or administrative liability for making the disclosure.
- no contractual or other remedy may be enforced or exercised against you based on the disclosure.
- in some circumstances (e.g., if the disclosure has been made to a regulator), the information you provide is not admissible in evidence against you in criminal proceedings or in proceedings seeking the imposition of a penalty, other than proceedings in respect of the falsity of the information; and
- you may seek compensation and other remedies through the courts if you suffer loss, damage, or injury because of making the Protected Disclosure and EML failed to take reasonable precautions and to exercise due diligence to prevent the detrimental conduct. It is recommended that a discloser seek independent legal advice before pursuing these options.

Additional legislative protections and remedies may also be available. Please speak to the Group General Counsel should you require further advice.

Personal work-related grievances

A Personal Work-Related Grievance has implications for an individual and does not also have significant implications for the employer.

Examples include:

- an interpersonal conflict between two employees.
- a decision relating to an employee’s engagement, transfer, or promotion.
- a decision relating to the terms and conditions of an employee’s engagement.

- a decision to suspend or terminate an engagement, or otherwise to discipline an employee.

In some circumstances, a Personal Work-Related Grievance may still be a Protected Disclosure if:

- it includes information about Wrongdoing or information about a Personal Work-Related Grievance includes or is bundled with a report of Wrongdoing (mixed report).
- it relates to a breach by EML of employment or other specified laws punishable by imprisonment of 12 months or more.
- it includes information about Wrongdoing beyond an individual's personal circumstances, demonstrates a systemic issue
- within EML that has significant implications for the organisation or indicates that EML has engaged in conduct that represents a danger to the public.
- concerns Detriment to a person because they have or may be considering reporting Wrongdoing; or
- it is made to a legal practitioner for the purposes of obtaining advice or legal representation in relation to the operation of the law about whistleblowers.

**European Union
Whistleblower
Protection
Directive**

The European Whistleblower Protection Directive (Directive (EU) 2019/1937) establishes minimum standards for the protection of individuals who report breaches of EU law. Under the Directive, organisations are required to provide secure and confidential channels through which concerns can be raised. The Directive also strictly prohibits any form of retaliation against whistleblowers as unlawful and subject to penalties under national law. It protects those who decide to report through external channels, including to competent authorities.

Each EU country is responsible for transposing the Directive into national law. The Irish legislative framework implementing these requirements is outlined separately in this Policy below. Employees who require further information or clarification of the Directive or related obligations should contact the Group General Counsel.

Ireland

In Ireland, the anti-retaliation obligations set out in the EU Whistleblowing Protection Directive are implemented primarily through the Protected Disclosures Act 2014 as amended by [the Protected Disclosures \(Amendment\) Act 2022](#) (“the Protected Disclosures Act”). Under the Act retaliation against a reporting person is unlawful and may give rise to civil remedies (including compensation of up to five year’s remuneration), while certain forms of penalisation or interference with Protected Disclosures may also constitute criminal offences depending on the nature of the conduct and the penalties provided for under Irish law.

The Protected Disclosures Act provides additional statutory protection to “workers”¹ who report relevant Wrongdoing. For a disclosure to qualify as protected the worker must have a reasonable belief that the information disclosed demonstrates Relevant Wrongdoing; the information has come to the worker’s attention in a work-related context; and, the disclosure must be made in the manner set out in the Protected Disclosures Act.

In parallel, [The Central Bank \(Supervision and Enforcement\) Act 2013](#) (“the 2013 Act”) contains a provides a separate protected disclosure regime for matters relating to breaches of financial services regulation. Under Section 38 (2) of the 2013 Act, individual performing Pre-Approval-Controlled Functions' (PCFs) have a personal legal obligation to report information related to suspected breaches, offences, or the concealment/destruction of evidence, directly to the Central Bank on the [prescribed disclosure form](#). External auditors must report to the Central Bank of Ireland if they become aware of Wrongdoing during their audit (Statutory Duty Confirmation).

E-Money institutions must directly report any material breaches of legislative requirements to the Central Bank

Although the Protected Disclosures Act and the 2013 Act operate as distinct statutory regimes, all Irish regulated entities must ensure both frameworks are appropriately integrated within their whistleblowing arrangements. This Policy reflects that requirement.

Who can make Protected Disclosures?

Under the Protected Disclosures Act the definition of a worker is broad and includes individuals who may not be traditionally considered employees. The following categories are covered by this policy:

- Current or former employees
- Trainees (paid or unpaid)
- People working under a contract for services.
- Independent contractors
- Agency workers
- Individuals on work experience
- Unpaid trainees
- Board members (executive and non-executive)
- Shareholders
- Volunteers
- Job applicants

Workers are also be protected under the Acts where they make an anonymous disclosure but are later identified and penalised because they made a Protected Disclosure.

All individuals referred to above, as well as those within the definition of Eligible Whistleblower are referred to as “workers” and covered by this Policy.

¹ 1 For full definitions in this Act please see [here](#).

What can be reported as Wrongdoing?

Under the Protected Disclosures Acts, Relevant Wrongdoing includes:

- criminal offences
- conduct endangering the health and safety of individuals or the environment.
- failure to comply with legal obligations (excluding contractual employment obligations).
- miscarriage of justice that has occurred or is likely to occur.
- misuse of public funds that has occurred or is likely to occur.
- an act or omission on behalf of a public body that is oppressive, discriminatory, grossly negligent or constitutes gross mismanagement.
- an act or omission that breaches EU law in areas such as: financial services, products, markets, anti-money laundering (AML) and counter-terrorist financing, environmental protection consumer protection of Privacy and Personal Data and network and information security.
- affects the financial interests of the EU; relates to the internal market; or defeats the objects or purpose of the rules of the EU acts in any of the above areas.
- Concealment, or destruction or attempted concealment/destruction evidence relating to any Wrongdoing.

Relevant Wrongdoing may occur inside or outside Ireland. Matters not considered Wrongdoing include:

- Personal employment-related grievances that concern the worker exclusively
- disputes relating solely to the workers employment contract
- information that is disclosed in a legally privileged setting.

False or Unfounded Disclosures

A worker remains protected if the information disclosed ultimately proves to be incorrect, provided that they had a reasonable belief in its accuracy at the time of disclosure. However, it is an offence under the Act for a worker to knowingly that the information is false is an offence.

Anonymous disclosures

Under the Protected Disclosures Act, EML is not legally obliged to accept or follow up on anonymous disclosures but may choose to do so. If a worker who makes an anonymous report is subsequently identified and suffers Detriment due to making a disclosure, they will receive the same protections as a worker who made a disclosure without remaining anonymous.

How to make a Protected Disclosure

The Protected Disclosures Act provides a tiered disclosure framework. Workers may choose any of the following channels:

- Internal Reporting (EML channels)

Reports can be made via “Your Call” (independent reporting channel) or to the designated Whistleblower Protection Officer as set out in Annexures A.

The simplest route is an internal disclosure to EML. The threshold for protection is that the worker has a reasonable belief that the information disclosed shows or tends to show Relevant Wrongdoing. Disclosures can be made in writing, orally, or by requesting an in-person meeting.

- Disclosure to Prescribed Persons

Workers may report directly to a Prescribed Persons as listed in Protected Disclosures Act 2014 (Disclosure to Prescribed Persons) Order 2020. Examples include the Central Bank of Ireland, The Health and Safety Authority and the Data Protection Commission. A full list of prescriber persons is available on <https://www.gov.ie/en/collection/41798-protected-disclosures-whistleblowing-list-of-prescribed-persons/gov.ie>. This list will help workers find the right person or body to report to.

As a prescribed body for financial services, the CBI accepts reports of Wrongdoing, breaches of legislation, or unethical conduct. E-Money institutions must directly report any material breaches of legislative requirements to the Central Bank. The Regional Head of Risk & Compliance will be responsible for reporting regulatory and legislative breaches to the CBI. However, any employee may make a Protected Disclosure if they suspected wrongdoing by the Firm or an individual. Employees are encouraged to report through internal channels in the first instance.

A disclosure to a prescribed person is Wrongdoing if the worker:

- Reasonably believe the relevant Wrongdoing falls within that person’s remit.
- The information disclosed is substantially true (a higher threshold than internal reporting)
- Disclosure to the Office of the Protected Disclosures Commissioner

The Protected disclosures Commissioner, established under the 2022 Act:

- Allocate the disclosure to the appropriate Prescribed Person; or
- Where no such person exists

The Office of the Protected Disclosures Commissioner was established under the 2022 Act. It may receive disclosures from individuals or Prescribed Persons. It may:

- Allocate the disclosure to the appropriate Prescribed Person; or
- Where no such person exists, follow up directly on the report.

Workers may also seek independent advice before making a disclosure. Transparency in International Ireland publishes practical [guides](https://www.transparency.ie/helpline/guides) for workers considering whistleblowing. <https://www.transparency.ie/helpline/guides> Guides: Transparency International Ireland.

Central Bank of Ireland Whistleblowing Service	
(Protected Disclosures)	<p>Where an individual needs to make disclosure under the Central Bank Enforcement Act, 2013 complete the Protected Disclosures Form and email or post to the addresses below.</p> <p>Telephone: 1800 130 014 (9am – 5pm Monday to Friday)</p> <p>Email: confidential@centralbank.ie</p> <p>Post: Protected Disclosures Desk, Central Bank of Ireland, PO Box 559, Dublin 1</p> <p>Where a PCF holder needs to make a disclosure of an alleged offence, breach of financial services legislation or concealment or destruction of evidence of such in their firm they must make the disclosure by completing the PCF Protected Disclosure Form and submit by either e-mail or post to the addresses above.</p>
(Infringement Reports)	<p>Where the Firm needs to make an infringement report this is done by emailing paymentservicesupervision@centralbank.ie. Reference to specific regulations should be made for e.g., relating to PSD2/Payment Services the firm should use "PSD2 Protected Disclosure - Confidential!" in the subject line.</p>
Protected Disclosures Commissioner	<p>Where an individual needs to make disclosure under the Protected Disclosures Act they may make this via the following methods:</p> <p>Telephone: 01 639 5650</p> <p>Email: info@opdc.ie</p> <p>Post: 6 Earlsfort Terrace, Dublin 2, D02 W773</p>

Handling Disclosures Made to EML

Where a disclosure of Wrongdoing is made to “Your Call” or the WPO:

- EML will acknowledge your disclosure within 7 days.
- the WPO will diligently follow up, including an initial assessment and requests for further information where necessary.
- the WPO will provide feedback within 3 months on actions taken or planned (e.g., investigation, referral, closures, or re-routing to a more appropriate procedure (for example a disclosure about workplace grievances may be referred to the grievance process)).
- the WPO will inform you of the outcome of any investigation, subject to confidentiality and data privacy obligations.

If you make a disclosure to a prescribed person external to EML or to the Office of the Protected Disclosures Commissioner, those bodies will use their own independent external reporting channels and procedures for receiving, handling, and following up disclosures.

Protecting your identity

EML will take all reasonable steps to maintain confidentiality. Your identity (or any information that could identify you) will only be disclosed if:

- required or permitted by law (e.g. the purpose of obtaining legal advice).
- you consent.
- the disclosure is a necessary and proportionate under EU or Irish law in the context of judicial proceedings or investigations including to safeguard the rights of a person implicated
- the recipient demonstrates that:
 - they took all reasonable steps to avoid disclosing your identity or any information that is likely to lead to the identification of your identity; or
 - disclosure is necessary to prevent a serious risk to State security, public health, public safety, or the environment.

Where possible EML will notify you in writing before any disclosure of your identity, including reasons for disclosure, unless such notification would jeopardise an investigation prevention of a crime, or other legally recognised interests.

Data Protection & Record Retention

All whistleblowing records must be retained in secure systems with restricted access, in compliance with EU General Data Protection Regulation (GDPR). Only the information necessary for assessing, investigating, or resolving the concern will be processed in line with EU GDPR. For any questions relating to data handling, confidentiality, or data protection rights, please contact the EML DAC Data Protection Officer.

Data must be retained for only as long as necessary and proportionate to comply with relevant European legal and regulatory requirements. Personal data that is not relevant to the assessment, investigation, or handling of a Wrongdoing disclosure will not be collected; if such data is collected, it will be securely deleted without undue delay.

United Kingdom

In the United Kingdom, whistleblowers who make Protected Disclosures are entitled to protection under the Public Interest Disclosure Act 1998 (PID Act).

Who can make Protected Disclosures?

Any person who is a “worker” can make a Protected Disclosure. “Worker” is broadly defined to mean anyone who works (or worked) under a contract in the UK, including employees, casual workers, temporary or agency workers, people involved in training programs or work experience.

Anonymous disclosures

Protected Disclosures can be made anonymously.

What is a Protected Disclosure under UK Law?

Under UK Law, matters that can be reported by a worker as a Protected Disclosure are disclosures, made in the public interest, which in the reasonable belief of the person making the disclosure shows that one or more of the following has been, is being, or is likely to be committed:

- a criminal offence.
- a breach of a legal obligation.
- a miscarriage of justice.
- danger to the health and safety of any individual.
- damage to the environment; or
- the deliberate covering up of the Wrongdoing in any of the above categories.

Disclosures regarding personal grievances (for example bullying, harassment, discrimination) are not Protected Disclosures under UK Law, unless the particular case is in the public interest.

Sexual Harassment (effective 6 April 2026)

From 6 April 2026, disclosures relating to sexual harassment are protected under UK whistleblowing legislation, regardless of whether they would otherwise be characterised as a personal grievance or require a public-interest test. This reflects amendments introduced by the Employment Rights Act 2025.

How to make a disclosure

You can make a disclosure to Your Call or to the designated Whistleblower Protection Officer as set out in the Policy. If you work for EML and are not comfortable making a report in this way, or you are not satisfied with EML’s response to your disclosure, you may also contact the Financial Conduct Authority (FCA) using the information below.

FCA’s Whistleblowing Service	Telephone: +44 (0)20 7066 9200 (10am – 3pm Monday to Friday) Email: whistle@FCA.org.uk Website: https://www.fca.org.uk/firms/whistleblowing Online form to make a report
-------------------------------------	---

The FCA is a prescribed persons under the Employment Rights Act 1996 along with other organisations. You can check the complete list published by the HM Department for Business, Innovation and Skills (BIS) before making a reportable concern.

It is important to note that workers will not be protected under the PID Act in relation to disclosures made to the FCA or other external bodies unless they satisfy the criteria set out in the PID Act. You are encouraged to obtain your own legal advice before making a disclosure to an external party to ensure that the legal protections apply.

Data protection

EML will collect, use, store, transfer and process a discloser’s personal data, including transferring personal data outside the European Economic Area, in accordance with data protection regulations. Personal data that is manifestly not relevant for the handling of a Wrongdoing disclosure will not be collected, or if is collected, will be deleted without undue delay.