



# Whistleblowing Policy





## Contents

1. An introduction to the <b>ofi</b> Whistleblowing Policy .....	3
2. No retaliation .....	4
3. Using the policy .....	4
4. Whistleblower process and the <b>ofi</b> whistleblowing channel .....	5
5. Investigation of complaints .....	6
6. Principles to be followed when investigating complaints .....	7
7. Confidentiality .....	8
8. Actions following an investigation .....	8
9. Record keeping.....	8
10. External reporting .....	9
11. Training.....	9
Appendix I – Whistleblowing process summary .....	10
Appendix II – Whistleblowing prioritization guidelines* .....	11

## Version Control

Action	Date	Change	Responsibility
Created	August 2018	New Policy	EC, SR, RK, AE
Revised	June 2019	Revised Process	ST, EC, SR
Revised	December 2021	Revision to address EU WB Directive	ST, EC



## 1. An introduction to the ofi Whistleblowing Policy

### Purpose of the Policy

Companies are expected, pursuant to various national regulations and by various regulators, to have a whistleblowing policy in place. The **ofi** Whistleblowing Policy ("**Policy**") is designed to ensure that adequate arrangements are in place to enable whistleblowers to alert the Company's management and/or competent authorities to possible infringements of regulations and policies within ofi and this document sets out the guidelines, protections and internal processes that apply when a report setting out a person's suspicions or concerns of inappropriate conduct is made (a "**Complaint**").

The Policy's essential features are that:

- a) anyone suspecting wrongdoing at work is encouraged to make a Complaint through the ofi whistleblowing channel.
- b) any Complaints raised shall be investigated properly in accordance with this Policy.
- c) the identity of the person raising a Complaint will be kept confidential to the extent they wish to remain anonymous; and
- d) anyone making a Complaint in good faith shall not be exposed, penalized, or suffer any form of retaliation, even if they are mistaken.

Questions concerning the scope, implementation, requirements of, or other matters related to, this Policy, the **ofi** whistleblowing channel or related procedures should be directed to the Global Head of Internal Audit or another member of the Internal Audit team.

### What is a Whistleblower?

Whistleblowers are generally considered to be individuals (usually employees) who may bring new information to the attention of a company's management or competent authorities to assist them in detecting serious wrongdoing, including a crime, a breach of internal policy, fraud, bribery, market manipulation, money laundering, a privacy/personal data breach or any other illegal activity, so that appropriate action can be taken.

### Who does this Policy apply to?

This Policy expects all employees, officers and directors of the Company (whether permanent or temporary) and of the Company's subsidiaries, affiliates and related corporations, whether permanent or temporary ("**Employees**") to raise concerns directly with their supervisor, local HR manager or the Internal Audit ("IA") function directly or via the **ofi** whistleblowing channel.

In addition to Employees, all employees, officers and directors of the Company's representatives, vendors, contractors, shippers, agents, customers, suppliers, consultants, business contacts, advisers, brokers, including authorized travel agents and general sales agents, and any other entity that performs services for or on behalf of the Company or any of its subsidiaries or their employees, wherever located (collectively, "**Associated Persons**") may also raise concerns via the **ofi** whistleblowing channel rely on this policy.



## 2. No retaliation

**ofi** recognizes that some individuals might be put off from raising their concerns because they fear possible retaliation. Accordingly, measures to ensure the anonymity and/or protection of the whistleblower are necessary and should address the rights of the whistleblower and, where appropriate, the accused person(s).

Retaliation against a Whistleblower is not acceptable within **ofi**. Any person who feels compelled to make a Complaint against any other person(s) within **ofi** either to their manager, or Internal Audit, or to an external regulatory body has right to protection as set out in this Policy and the **ofi** Code of Conduct.

**ofi** will not dismiss, harass, or otherwise discriminate against any Employee or Associated Person who raise concerns in good faith, even if they are mistaken.

Anyone who reports suspected or actual wrongdoing shall, where possible, be given complete anonymity and **ofi** shall support Employees against any form of action against them in relation to the making of any such report.

Any retaliation will be treated as a serious matter to be addressed under the applicable disciplinary procedure.

If you believe that you have suffered any such treatment, you should inform the LEGAL function immediately. The LEGAL function may then review or seek more information if required and decide what action to take with respect to the complaint. If appropriate, the complaint will be passed on to **ofi**'s senior management.

## 3. Using the policy

- 3.1. This Policy should only apply where there is or has been a suspected serious wrongdoing. A non-exhaustive list of examples of wrongdoing is set out below. It is not intended to apply to trivial matters or address an employee's day-to-day frustrations.
- 3.2. Where the suspected serious wrongdoing is concerned only with an individual's personal employment situation or raises questions of poor management, and where the circumstances do not appear to involve any crime or policy violation, then such matters should be addressed under the **ofi** Group Grievance Policy and raised directly to a supervisor or the HR function.
- 3.3. This Policy and the reporting mechanism should also not to be used for matters concerning an individuals' personal difficulties with their colleagues, manager, or any other person. Such matters should be reported directly to the local Human Resources ("HR") representative. Malicious or deliberately or recklessly false accusations of any kind for personal reasons are unacceptable.



3.4. Examples of concerns that may merit being raised under this Policy include, but are not limited to;

- Crime (i.e., Failure to comply with any legal obligation, by act or omission)
- Fraud, Bribery or Corruption, Money Laundering
- Price-fixing or other anti-competitive behavior
- Collusion (e.g., undue favoritism or business allocation to certain suppliers / business partners)
- Procuring goods / services for personal advantage
- Consumer protection concerns
- Misuse of Company assets or funds (e.g., utilization of company's funds to make non-company related purchases or for personal use)
- Workplace harassment
- False expense claims (e.g., understatement of cost or expenses / unreasonable deferment, claiming expenses without incurring them).
- Theft (e.g., misappropriation of Company funds, assets, stocks or inventories)
- Animal health and welfare
- Unauthorized deliveries to customers
- Food and Feed safety
- Endangering the health or safety of an individual or damaging the environment
- Any breach of **ofi**'s Code of Conduct and Policies

## 4. Whistleblower process and the ofi whistleblowing channel

Employees are encouraged to raise any concerns to local management and/or their local HR representative. In practice, however, this may not always be appropriate, or in line with the wishes of the employee and staff may therefore choose to report directly (by email) or anonymously (by the online reporting channel) to IA.

**ofi** have created a reporting channel for the reporting of any suspected crime, fraud, bribery, or other serious wrongdoing directly to IA. This can be done openly or anonymously through the latest available Whistleblowing channels as set out below.

**ofi** recognizes that some individuals prefer to report anonymously, and the Whistleblowing channel allows for this. It is important to stress, however, that if you report anonymously, it will not be possible for the team or person who receives your report, to contact you to ask for further information, so please make sure that you include as much information as possible in the initial report.

### Reporting via Whistleblowing Channel

1. Go online – <http://tinyurl.com/OlamInfo>,
2. Fill in – complete the online form as directed,
3. Click submit – your concern will be reviewed and handled appropriately by the Internal Audit function.

### Reporting via Email

Alternatively reporting can be done by simply sending an email directly to the IA function at: [ia@ofi.com](mailto:ia@ofi.com). Please note that choosing this route will not preserve the anonymity of the complainant but we are committed to ensuring that we have in place procedures that ensure



that the confidentiality of the whistleblower's identity and of any third party mentioned in the report which prevent access by non-authorized staff members.

### Information Requirements

It is important that any Complaint contains, as far as possible, a clear, full and accurate description of the suspected wrongdoing and preferably contain details of the country, product, time / date and the name of the person(s) that the report concerns.

## 5. Investigation of complaints

Complaints will be investigated in accordance with this Policy.

Where a complaint has been reported to a group other than the IA function, they should pass this information onto the IA function as soon as possible. Regardless of how a Complaint is made, the action to be taken in response to it should be consistent. Where local legislation sets out any specific timelines to reply to a person who has reported a concern non-anonymously, such timelines must be understood and met by the relevant parties who are handling the report.

The IA Investigation Lead shall be instrumental in this process and shall be a member of the IA function as selected by the Global Head of Internal Audit. An overview of the investigation process is set out in the diagram in Appendix I and explained below.

5.1. Prompt action will be taken by IA upon their receipt of a Complaint:

- a. Where a report is not made anonymously, receipt of the report will be acknowledged, and further feedback shall be provided, in line with local applicable regulations.
- b. IA shall record details of the Complaint.
- c. If the Complaint concerns a matter as described in 3.2 or 3.3 above the Complaint shall be referred by IA to the relevant HR representative.
- d. Each Complaint will be assessed by the IA Investigation Lead as High, Medium or Low priority based on guidelines set out in **Appendix II** and prioritized for further action.

5.1.1. Where the Complaint is assessed to be **High Priority**:

- a. The Complaint will be shared with the CEO (Group, Chief Executive Officer) for their assessment (and the Board Audit and Risk Committee Chair at the appropriate time).
- b. The IA Investigation Lead will anchor the investigation along with an appropriate Regional/Country team and member(s) of relevant functional team(s).
- c. If required, the IA Investigation Lead will appoint an independent investigation agency in consultation with IA Head, CEO. The outcome of all investigations will be documented and shared with the CEO and the consequent actions agreed, implemented and appropriately documented.

5.1.2. Where the Complaint is assessed to be **Medium Priority**:

- a. IA Investigation lead will anchor the investigation and decide on an appropriate team to carry out the investigation, such team members to be appropriate Regional/Country staff and member(s) of functional team(s).
- b. On conclusion of the preliminary investigation, should the IA Investigation Lead believe the outcome is of significant concern, they will escalate it to the CEO.

- c. Where the matter is not escalated to the CEO, actions will be agreed between the IA Investigations Lead and relevant Regional/Country team, documented and implemented.

5.1.3. Where the Complaint is assessed to be **Low Priority**:

- a. The Complaint should be shared with the relevant country management team, who will appoint an appropriate investigation team comprising of the BU the Complaint relates to and other local management,
- b. The outcome of the investigation will be provided to relevant country management in a written report and proposed actions.
- c. Should the country management team believe the matter is of significant concern they will escalate the issue to the IA Investigations Lead for further assessment.
- d. Where the matter is not escalated, the agreed actions will be implemented and documented.

5.2. Where the Complaint is not considered valid, or not represent any material risk, then feedback to that effect will, where possible, be provided to the complainant.

5.3. On a quarterly basis:

- a. details of all *High Priority* Complaints received and an update on the progress of all such investigations will be shared with the Chairman of the Audit and Risk Committee.
- b. a summary of all *Medium* and *Low Priority* Complaints will be shared with the CEO.

## 6. Principles to be followed when investigating complaints

The following principles should be followed for all investigations of Complaints:

- a) no individual should ever be involved in the management and/or conducting of investigation of allegations in which he or she is the accused or in any way personally involved,
- b) the investigation should take place at least one management level above the level of the most senior person against whom allegations have been made.
- c) Complaints should be reviewed promptly by the Internal Audit function.
- d) All Complaints are to be assessed and, where appropriate, investigated.
- e) It is important to note that the investigation will seek to establish the facts only. It will not make any recommendation as to a course of action, other than regarding measures for process improvement where appropriate.
- f) If the investigation uncovers substantiated issues, these will be addressed in accordance with the relevant wider **ofi** policies and procedures that are applicable.
- g) Where a report is not made anonymously feedback will be given to the reporting person in line with the local regulations.



## 7. Confidentiality

The identity of the individual raising a Complaint, where known, (and any third party mentioned in the report) shall be kept confidential outside of the investigation team and we have procedures in place to prevent access by non-authorized staff members. Accordingly, their identity should only be communicated to the extent necessary to ensure that:

- a) the matter is properly investigated and reported in line with this Policy; and
- b) all data processed in investigating a Complaint is processed in accordance with the General Data Protection Rules (GDPR)".

## 8. Actions following an investigation

In every case where serious wrongdoing has been found to have occurred within **ofi**, the relevant internal policies or controls should carefully be assessed to establish whether there has been any breakdown or failing and, if there is, what steps should be taken to prevent this from happening again. Even where no breach of policy or breakdown of internal controls has been found, careful consideration should be given as to whether or not certain steps should be taken to adjust such relevant policies and/or minimize the risk of recurrence and/or to improve the ability to detect any such recurrence. LEGAL, Finance and other relevant representatives at the appropriate level, will work collaboratively with Internal Audit to assess any appropriate remedial actions. In addition to addressing and modifying policies, systems and controls, decisions will be taken in terms of the appropriate punitive measure for any person found to be in guilty of any reported or discovered wrong doing.

The Board Audit and Risk Committee reviews arrangements by which individuals may, in confidence, raise concerns about possible inappropriate activity as detailed in this Policy. The Board Audit and Risk Committee reviews concerns raised through the Policy to make sure that any significant matters receive independent investigation and appropriate follow up action (including escalation to the full Board, if considered appropriate).

## 9. Record keeping

Records must be kept of every report received and these must be stored securely as long as required by law. Where there is no legal retention period prescribed such records shall be retained for a minimum of 5 years.

Where there are further specific requirements set out in local legislation relating to the how the report was made these must be understood and fully implemented.





## 10. External reporting

Following any investigation, should the IA Investigation Lead, regional or country management team handling the investigation believe the matter is of such a nature that it may require to be disclosed to a regulatory agency, you should refer the matter to the LEGAL function who shall evaluate the matter, advise on the requirement to report, and assist with the submission of any such report to the relevant body.

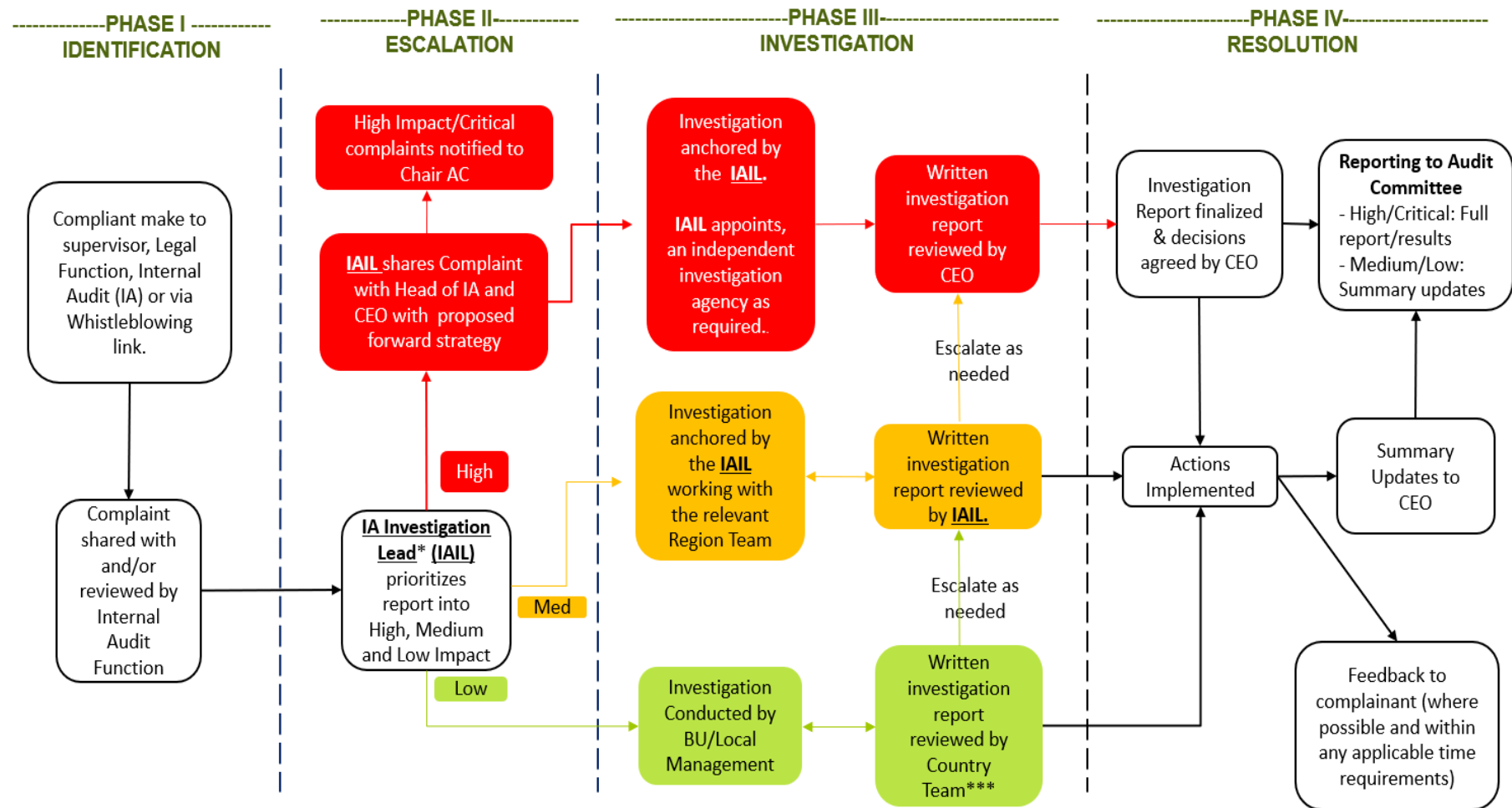
## 11. Training

The existence of the **ofi** whistleblowing channel has been shared across **ofi** via posters published and circulated in all **ofi** locations to ensure maximum reach. This information is also contained in the **ofi** Code of Conduct which is provided to all new Employees and the Policy and reporting link is available on the **ofi** external website.

Refresher information and appropriate training about the whistleblowing procedure and channel will be shared with employees and senior management periodically.



## Appendix I – Whistleblowing process summary





## Appendix II – Whistleblowing prioritization guidelines\*

Category	Financial impact	Reputation risk	Policy & legislation breach	Employee impact
High	> \$5mn	Global	<ul style="list-style-type: none"> <li>• Potential criminal charges</li> <li>• Regulatory breach with global impact</li> <li>• Breach of Anti Bribery &amp; Corruption Policy, Fraud Policy, Sanctions Policy</li> </ul>	<ul style="list-style-type: none"> <li>• Allegations against Ex Co members, their direct reports and/or SVP level employees</li> <li>• Retaliation against a whistle blower</li> </ul>
Medium	\$1mn - \$5mn	Country/Local	<ul style="list-style-type: none"> <li>• Civil action</li> <li>• Regulatory breach with regional impact</li> <li>• Repeated complaints on the same issue</li> </ul>	<ul style="list-style-type: none"> <li>• Allegations against employees in Band E to C</li> </ul>
Low	< \$1mn	None	<ul style="list-style-type: none"> <li>• Regulatory breach with local/country impact</li> </ul>	<ul style="list-style-type: none"> <li>• Allegations against employee below Band E</li> </ul>

\* Guidelines are to be used to identify the level of priority for each Compliant. Assessment to be performed by the IA Investigations Lead who may, at their own judgement, adjust the resultant category based on additional factors not referred to in these guidelines.