Document title

ANTI-FRAUD POLICY

Document type

POLICY

Version number

Version Number: 4.1

Date

06-10-2025

Number of pages

10 pages

DOCUMENT SUMMARY

Document type		Policy
Purpose of the document		Prevent, facilitate awareness of, identify and report the activities constituting fraud.
Target Audience		All staff
Classification		Public
RACI	**Responsible / Document owner**	Euronext N.V. Managing Board
	Accountable	Group Compliance
	Consulted	Internal Control / Information Security
	Informed	All staff
Reference to related documentation		Anti-Fraud Framework Document Prevention of Fraud – Fraud examples and red flags Euronext Code of business conduct and ethics Euronext Whistleblower Policy Euronext Anti-Bribery Policy Gifts, Business meals and Business entertainment Policy Anti-Money laundering and sanctions Policy and Guidance Confidential and Information Policy Cyber & Information security Policy
Regulations linked to this document		

VERSION CONTROL

REVISION NO./ VERSION NO.	DATE	AUTHOR	APPROVAL	CHANGE DESCRIPTION
2.0	27-12-2021	Compliance department	Euronext N.V. Managing Board	Annual policy update 2021
3.0	17-08-2023	Compliance department	Euronext N.V. Managing Board	Update 2023
4.0	02-06-2025	Compliance department	Euronext N.V. Managing Board	Update 2025
4.1	06-10-2025	Compliance department		New reporting channel IntegrityLog

CONTENTS

1. OBJECTIVES, OWNERSHIP AND GOVERNANCE

1.1 OBJECTIVES

Background

Fraud is a type of criminal activity that consists in an intentional or deliberate act intended to deprive another party of property or money by deception, or other unfair means.

Fraud and other illegal activities harm the financials of any entity or company.

This explains why many jurisdictions all over the world have laws and regulations in place to combat Fraud.

The European Union combats Fraud that affects the financial interests i.e. the budget of the European Union (ex: the counterfeiting of money (EUR); any form of tax evasion such as customs duties, VAT) and any illegal activities that, often combined with corruption and money laundering, are falling under applicable criminal laws.

Under national laws, Fraud is generally part of numerous legislative pieces often linked to criminal offences such as:

- Criminal laws in general (ex: any person or legal entity targeted through emails, social networking sites for the purpose of obtaining money);
- Business Criminal laws (ex: tax fraud such as Ponzi or Pyramid evading tax schemes);
- Investment fraud;
- Accounting laws (unproper book keeping of financial records);
- Customs and Tax laws (tax evasion like custom duties or VAT).

Euronext is committed to combat all forms that encompass intentional misappropriation or theft of the Company's assets that may impact negatively the financials and reputation of the Company.

Objectives

The Anti-Fraud Policy is established to prevent, facilitate awareness of, identify and report the activities constituting Fraud across the organization. In addition the Anti-Fraud Policy provides a detailed description of an investigation process, including how reports are made to management and what follow up-actions are taken.

At all times, it is the intention of Euronext to conduct business in accordance with the highest standards of ethical behavior, which includes abiding by all applicable laws.

1.2 SCOPE AND OWNERSHIP

Scope

This Policy applies to Euronext N.V. and its majority owned subsidiaries (collectively referred to as the "Company" or, "Euronext") and to all Euronext employees including consultants (among which interns and temporary staff) and agents (collectively "You" or, "Employees").

This Policy should be read in conjunction with other Euronext policies and documents such as:

- Anti-fraud Framework
- Document Prevention of Fraud – Fraud examples and red flags
- Code of Business Conduct and Ethics
- Whistleblower Policy
- Anti-Bribery Policy
- Gifts, Business meals and Business entertainment Policy
- Anti-Money Laundering and Sanctions Policy and Guidance
- Confidential and Inside information policy
- Cyber & Information security Policy

These policies along with other policies and procedures can be found on the Company's Intranext.

The scope of this Policy is to ensure that Employees understand:

- What Fraud is, and what are the various forms of misappropriation of the Company's assets;
- That any fraudulent irregularity, or suspected irregularity may involve not only Employees but also shareholders, consultants, vendors suppliers, issuers, market members, contractors, outside agencies doing business with the Company;
- That prevention of fraud works in two ways. First prevent that Euronext or any of its employees, contractors or other representatives commit or are involved in fraud, and second prevent that Euronext is used in or becomes a victim of fraud committed by external parties.
- The tools made available by the Company to them in order to report timely Fraud or suspicions of Fraud; and
- Roles and responsibilities in case of a fraud investigation.

Ownership

Owner of this policy is the Euronext N.V. Managing Board. Compliance is responsible for maintaining the policy and related documentation. The policy should be reviewed on a 2 years basis, and updated based on requirements from Euronext group.

Compliance is also responsible for securing the proper approval from the Managing Board.

1.3 GOVERNANCE

Responsibility and tasks of the Supervisory Board in connection with this policy

Suspicions or allegations of fraud related to accounting and auditing matters will be investigated under the direction and oversight of the Euronext N.V. Audit Committee.

Responsibility and tasks of the Managing Board in connection with this policy

The Euronext N.V. Managing Board has overall responsibility for the anti-fraud framework. This includes approval of policy updates. The day-to-day responsibility for implementation, management and maintenance is delegated to Compliance.

Reporting on this policy

Compliance will maintain a log of all cases of reported fraud and will prepare an annual summary for the Euronext N.V. Audit Committee.

Stakeholders' responsibilities

All Managing board members and employees are encouraged to report suspected activity that could constitute fraud.

2. DETAILED REQUIREMENTS

2.1 DEFINITIONS AND ACTIONS CONSTITUTING FRAUD

Definitions

Fraud is defined as an act of deception or of intentional misrepresentation, or concealment of a material fact for the purpose of procuring for oneself or a Third Party a personal gain, or an unjust or unlawful financial or other benefit to the detriment of the Company.

Third-Party means any third-party and/or external party to Euronext, including for example: (i) any current or prospective client, customer, vendor, provider, or supplier of Euronext, such terms to be interpreted broadly to include any person or entity that provides a service to the Company or from which the Company obtains revenues; (ii) any issuers, listed companies, market members, external market participants, business partners; (iii) any public official; (iv) any employee, representative, agent, intermediaries or other individual associated directly or indirectly with the above; (v) any Euronext Employees' family members[1] and relatives, irrespective if such Third-Party is in a business relationship with the Company or not.

Actions constituting fraud

Fraud encompasses all forms of intentional misappropriation or theft of the Company's assets. Such damaging acts or omissions include, but are not limited to:

- all forms of Company's assets destruction or alteration (which includes theft of Company's intellectual property or identity theft);
- all forms of impropriety in the handling or reporting of financials;
- false representation;
- all profit arising from the disclosure of inside and proprietary information to the Company and to Third Parties;
- abuse of a position;
- Scams or (cyber) attacks by external parties in order to steal money or other assets of the Company or to obtain valuable Company information.

An overview of 'Red Flags' to help you identify forms of fraud is included in the document 'Prevention of fraud – fraud examples and red flags'.

2.2 REPORTING PROCEDURES FOR EMPLOYEES

All Employees are encouraged to report suspected activity that could constitute Fraud. An Employee who discovers or suspects fraudulent activity is encouraged to contact/ report through either of:

- his/her manager,
- website: https://euronext.integrity.complylog.com which provides the possibility to report alleged breaches anonymously,
- his/her local compliance officer or,
- by email to: **compliance@euronext.com.**

[1] Family members as defined by EU AML Directive (EU) 2015/849

The Company will not tolerate any form of retaliation against individuals who in good faith provide information concerning suspected fraud.

While reporting suspected improprieties, Employees should be aware of the following:

- Do not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Investigation Team, your manager, or a government or regulatory agency; and,
- Do not attempt to personally conduct investigations or interviews/interrogations.

2.3 INVESTIGATION RESPONSIBILITIES

An investigation needs to take place in a short period of time to prevent further potential losses, mitigate ongoing risks, and preserve evidence, which can degrade or be tampered with over time. Swift action also helps maintain stakeholder trust and ensures regulatory compliance.

A fraud investigation is typically initiated based on a tip-off, internal audit findings, anomaly detection, or external reports. The Chief Compliance Officer (CCO) is notified of the potential fraud and responsible for the entire Fraud Investigation Process. The CCO authorizes the investigation and appoints (at least) two Compliance Officers ("Investigation Team") from the Compliance Department to lead the investigation. Appointment of the Compliance Officers can depend on location, capabilities, expertise on the topic and availability. Since any investigation needs to be executed within a short period of time for reasons as described above, the Investigators need to be relieved from their ongoing responsibilities as much as possible. The Investigation Team develops a detailed investigation plan outlining the scope and objectives of the investigation, methodologies, timelines, the departments involved and the potential impact.

Based on the nature of the allegations, members of Information Security ("InfoSec"), Risk, FinanceInternal Audit, Human Resources and Legal may participate in the investigation. Should potentially Compliance staff be involved in the Fraud case, Legal must take over the process from here. Connecting with experts from other departments can only take place after the Investigations Team have ensured these departments are out of scope for the entire investigation.

If the allegation is related to Accounting and Auditing matters the Company will investigate the breach under the direction and oversight of the Company's Audit Committee.

Decisions to prosecute or refer the investigation results to the appropriate law enforcement and/or regulatory agencies will be made by Legal, Compliance, Information Security and senior management.

Any investigative activity will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

Members of the Investigation Team will have:

- free and unrestricted access to all Company records and premises, whether owned or rented;
- the authority to gather, examine and copy relevant documents, such as financial records, emails, contracts, and other pertinent data and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.[2] The Investigation Team will involve InfoSec to perform digital forensics if electronic data is involved. This includes collecting and analyzing logs, emails, and other digital footprints;
- the authority to engage finance experts to perform detailed financial analysis to identify discrepancies, anomalies, or patterns indicative of fraud and legal experts for consultation on legal implications and potential breaches;
- access to use data analytics tools if available to detect irregularities and trends that may indicate fraudulent activity;
- the authority to conduct interviews with key personnel who may have information about the suspected fraud.

The Investigation Team will not gather evidence by means that are unlawful, unfair or that are disproportionately incompatible with the rights of individuals and the internal investigation must be conducted in an impartial manner considering both incriminating and exculpatory evidence.

2.4 RECORD KEEPING, REPORTING AND FOLLOW UP

The Investigation Team will document all findings, including evidence collected, analysis performed, and conclusions drawn and ensure that all evidence is handled properly to maintain its integrity and admissibility in potential legal proceedings.

The Investigation Team will first prepare a preliminary report summarizing initial findings and any immediate actions taken. Secondly, the Investigation Team will compile a comprehensive final report detailing the investigation process, findings, conclusions, and recommendations for implementing corrective actions and will present the findings to the CCO for review and further action.

When needed, corrective actions will be implemented based on the investigation's findings, such as process improvements, policy changes, training and awareness sessions and disciplinary actions, and ongoing monitoring mechanisms will be established to ensure compliance with the new measures and to prevent future fraud.

[2] Provided that applicable law requirements are complied with when accessing an employee's email or electronically stored material. Within OBVPS in Norway, the policy is supplemented by a local internal instruction that present specific law requirements applicable when accessing an employee's email or electronically stored material.

2.5 CONFIDENTIALITY

All necessary measures are taken by the Investigation Team to protect the confidentiality of an allegation or investigation, the identity of the persons involved and of the information gathered, i.e. data protection, record keeping and archiving procedures, especially for personal data. Also, when an investigation is closed, the investigation report and all related information and documentation that were gathered must be archived in a way that guarantees restricted access strictly reserved for authorized persons in compliance with the personal data protection requirements.

2.6 SANCTIONS FOR POLICY VIOLATIONS

An Employee who engages in any form of fraud will be subject to disciplinary action, up to and including termination. Disciplinary actions towards employees are not determined by the Investigation Team or the CCO, but by senior management (or another relevant body) in consultation with HR and Legal to ensure actions are proportionate to the events and legally possible / allowed.In addition, the Company may take all reasonable steps to recover losses incurred as a result of fraud.

Finally, the investigation will formally be closed after all actions have been completed and documented and a post-investigation review will be conducted to evaluate the process and identify areas for improvement.