

Fraud Risk Management Policy

1 INTRODUCTION

- 1.1 Fraud is a major issue affecting individuals and businesses in every country and in every sector.
- 1.2 Fraud can be incredibly damaging. It can affect us in two ways, i.e. where an organisation:
 - 1.2.1 is the intended victim of the fraud; and
 - 1.2.2 fails to prevent an associated person committing fraud intending to benefit our organisation, or in some cases, our customers.
- 1.3 We run our operations with integrity and in an honest and ethical manner. All of us must work together to ensure it remains untainted by fraud.
- 1.4 This policy applies to Fred. Olsen Limited, Fred. Olsen Travel, Fred. Olsen Logistics and Forrest Estate (hereafter referred to as the Company) and has the full support of the Board. It sets out the steps all of us must take to prevent fraud in our Company and to comply with relevant legislation.

2 WHAT IS FRAUD AND HOW DOES IT AFFECT US?

- 2.1 Generally, fraud is a crime that involves deception or theft to gain an advantage.
- 2.2 The Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023) introduced a corporate failure to prevent fraud offence, which captures a wide range of fraud offences committed for the benefit of the Company, including:
 - 2.2.1 fraud by false representation;
 - 2.2.2 fraud by failing to disclose information;
 - 2.2.3 fraud by abuse of position;
 - 2.2.4 obtaining services dishonestly;
 - 2.2.5 participation in a fraudulent business;
 - 2.2.6 fraudulent trading; and
 - 2.2.7 cheating the public revenue.
- 2.3 There is only one relevant defence to the corporate offence of failure to prevent fraud: when the fraud offence was committed, the Company had reasonable prevention procedures in place, or that it was not reasonable to have any such procedures in place (e.g. if the risk of fraud being committed was extremely low).
- 2.4 The government has published detailed guidance on the failure to prevent fraud offence and reasonable prevention measures it expects organisations to adopt, and we have factored this guidance into this policy and related procedures. This policy is central to those prevention procedures.
- 2.5 Individuals found to have committed fraud face heavy criminal penalties. See further section: 14.

3 THIS POLICY

- 3.1 We take pride in the ethical way we conduct our business. This policy and related procedures embody the standards we expect from all staff and anyone associated with us. It applies to us all.
- 3.2 Fraud risk management is also about managing the risk of the Company itself falling victim to fraud, and this policy and related procedures are designed to protect us too.
- 3.3 Our fraud risk management policy and procedures do not operate in isolation; they form part of and should be read and followed alongside our other crime prevention measures, including our:
 - 3.3.1 Anti-bribery and corruption policy;
 - 3.3.2 Prevention of criminal facilitation of tax evasion policy;
 - 3.3.3 Speak up (Whistleblowing) policy; and
 - 3.3.4 Employee code of conduct.

4 Please read this policy thoroughly to ensure you understand what is expected of you. If you have any questions about this policy, or our fraud risk management procedures, please contact the Compliance Team at compliance@fredolsen.co.uk.

5 OUR APPROACH AND COMMITMENT TO MANAGING FRAUD RISK

- 5.1 The Company will not tolerate any fraud committed on its behalf.
- 5.2 This ethical stance is good for our organisation, core to our organisation and non-negotiable. We expect all our staff, contractors, suppliers and other business partners to always behave with honesty, with integrity and to act in accordance with our legal and ethical obligations.
- 5.3 Involvement in fraud exposes the Company and the person committing the fraud to criminal offences, which carry severe penalties. It also damages our reputation and the confidence of our customers, suppliers and business partners.

6 SENIOR MANAGEMENT COMMITMENT

- 6.1 The Board is committed to preventing persons associated with the Company from committing fraud, even if this results in short-term business loss, missed opportunities, or delays. Fraud is never acceptable, and we reject profit based on, or assisted by, fraud.
- 6.2 We are also committed to protecting the Company from falling victim to fraud.
- 6.3 Our commitment extends to:
- 6.3.1 ensuring there is clear governance across the Company in respect of our fraud prevention framework - see section: 7;
 - 6.3.2 leading by example, including by challenging misconceptions and reducing the rationalisation of fraudulent behaviour, e.g. ‘fraud is a victimless crime’; and
 - 6.3.3 fostering an open culture where fraud is never acceptable and staff feel empowered to speak up early if they encounter fraudulent practices, or have any ethical concerns, no matter how minor.

7 RESPONSIBILITY FOR OUR FRAUD RISK MANAGEMENT POLICY AND PROCEDURES

- 7.1 While the Board plays a leadership role in relation to fraud prevention, particularly in relation to reviewing and signing off our risk assessment, responsibility for the day-to-day operation of our fraud risk management policy and related procedures rests with the Compliance Team. They have the full support of the Board, which will ensure direct access to our most senior people as they think necessary, even where their primary reporting lines differ.
- 7.2 The Data Protection and Compliance Officer is responsible for the development and implementation of our fraud risk management procedures, including:
- 7.2.1 assisting the Board conduct appropriate fraud risk assessments—see section: 8;
 - 7.2.2 developing fraud **detection** measures;
 - 7.2.3 developing fraud **prevention** measures;
 - 7.2.4 reporting to the Board as appropriate, including ensuring appropriate management information is collected and shared to facilitate an understanding of the fraud risks we face, and the effectiveness of our risk management procedures;
 - 7.2.5 supporting the development and monitoring our whistleblowing procedures—see section: 10;
 - 7.2.6 investigating reports where fraud is detected or suspected;
 - 7.2.7 ensuring appropriate and adequate records are maintained; and
 - 7.2.8 monitoring this policy and its implementation.
- 7.3 Fraud prevention is the responsibility of everyone associated with the Company, including staff, agents, and other associated persons. We encourage colleagues and those we work with to challenge views that tend to support or seek to ‘normalise’ fraudulent behaviours. We also encourage you to speak up if you encounter unethical behaviour, or you are concerned about anything, however minor it may seem. For more on reporting concerns, see section: 10.

8 RISK ASSESSMENT

- 8.1 Our procedures to prevent fraud by persons associated with us, and to manage the risk of falling victim to fraud, are proportionate to the fraud risks we face.
- 8.2 We have assessed the nature and extent of our exposure to the risk of employees, agents and other associated persons committing fraud and of our exposure to the risk of falling victim to fraud.
- 8.3 While it is not possible to anticipate all potential fraud risks, our fraud risk assessment covers various key pinch-points, e.g.:
- 8.3.1 opportunity, e.g. weak controls and inadequate oversight;
 - 8.3.2 motive, e.g. financial stress and meeting targets; and
 - 8.3.3 rationalisation, e.g. no harm and resentment.
- 8.4 While there are some natural overlaps with our risk assessments in other areas of crime prevention (e.g. anti-bribery, and tax evasion facilitation prevention), this assessment is specifically tailored to and focussed on fraud risk. Our fraud risk assessment is reviewed and signed off by our Board.
- 8.5 Our procedures take account of the level of control and supervision we are able to exercise over our operations, particularly in relation to people acting on our behalf, including, for example, staff and contractors.

9 FRAUD RISK MANAGEMENT PROCEDURES

This section of the policy contains details of the procedures we have put in place to manage the fraud risks we face, both in terms of the failure to prevent fraud offence and falling victim to fraud.

9.1 Our people

- 9.1.1 The definition of ‘associated person’ under ECCTA 2023 is wide. We have identified types of associated persons relevant to this organisation as follows:
- (a) staff in high-risk roles;
 - (b) agents;
 - (c) contractors providing services for or on our behalf;
 - (d) sub-contactors.
- 9.1.2 Our risk assessment recognises that different associated persons may present different fraud risks.
- 9.1.3 We undertake pre-employment vetting checks plus ongoing vetting checks for roles we believe present a higher risk of fraud.
- 9.1.4 We keep our reward and recognition systems, including commissions, bonuses, financial targets, etc, under regular review.
- 9.1.5 All staff receive fraud risk management training, and compliance is evaluated and monitored—see section: 11.
- 9.1.6 We have supervision processes for staff and anyone acting on our behalf.

9.2 Due diligence

- 9.2.1 We apply due diligence measures, taking a risk-based approach, in respect of third parties who perform services for us or on our behalf.
- 9.2.2 Our procedures include:
- (a) background and identity checks;
 - (b) screening tools and internet searches;
 - (c) reviewing contracts with those providing services, to consider compliance obligations and suitability of termination provisions; and
 - (d) credit checks.

9.3 Our operations

- 9.3.1 We recognise that different departments/roles can present greater fraud risk, e.g. finance, procurement, and sales and marketing, and ensure appropriate training is developed for these departments/roles—see section: 11.
- 9.3.2 However, we apply an appropriate level of scrutiny to our smaller transactions and lower-risk operations, too.
- 9.3.3 This section of the policy contains information on our procedures around various aspects of our operations, including:

Operation	Section
Customer onboarding	9.4
Sales and marketing	9.5
Procurement	9.6
Finance	9.7
Sensitive/commercial information	9.8

9.4 Customer onboarding

- 9.4.1 We have robust customer and matter onboarding processes.
- 9.4.2 Customer onboarding measures include:
- (a) taking steps to identify our customers;
 - (b) considering the level of risk customers may present;
 - (c) being alert to the need to exercise reasonable additional caution where we do not meet our customers in person.

9.5 Sales and marketing

- 9.5.1 Any reward and recognition systems for our staff are reviewed regularly. This includes any commissions, bonuses, targets, etc.
- 9.5.2 We will provide tailored training and support for our sales and marketing staff

9.6 Procurement

- 9.6.1 We manage fraud risks throughout the procurement process, i.e. in a request for proposal, a tender, contract management, and during project delivery and project extension.
- 9.6.2 Contracts include appropriate terms for associated persons.

9.7 Financial operations

- 9.7.1 We use best practice with regard to financial reporting including segregation of duties, reconciliation of accounts, suitable sign-off arrangements.

9.8 Sensitive or commercial data

- 9.8.1 Our procedures for limiting access to sensitive and/or commercial data and identifying potentially unauthorised access are set out in our Information Security Risk Management Process Policy and Information Security Management System Policy.
- 9.8.2 These procedures are subject to regular monitoring and review.

10 REPORTING CONCERNS

- 10.1 Fraud is never acceptable. You are encouraged to speak up early if you encounter fraudulent practices, or have any ethical concerns, no matter how minor.
- 10.2 It is essential that you promptly raise any concerns in relation to possible fraudulent activity, of whatever nature.
- 10.3 The correct reporting mechanism will depend on the nature of the suspected activity, e.g.:
 - 10.3.1 where you are concerned that a member of staff or agent is committing or has committed fraud, a whistleblowing report may be appropriate. Our whistleblowing arrangements are usually the best way to report concerns of fraudulent behaviour. These are contained in our [Speak Up \(Whistleblowing\) Policy](#);
 - 10.3.2 where you have concerns relating to fraudulent activity that may also involve an element of money laundering, terrorist financing, or proliferation financing, submitting a [suspicious activity report form](#) (SARF) may be the only way to ensure protection under the Proceeds of Crime Act 2002;
 - 10.3.3 where you are concerned that the organisation has been the victim of fraud, please raise this with your line manager in the first instance.
- 10.4 Make your report as soon as reasonably practicable. You may be required to explain any delays.
- 10.5 You can raise concerns anonymously, if you wish through our Speak Up (Whistleblowing) procedure.
- 10.6 Our training program includes whistleblowing awareness¹¹.
- 10.7 The Company will investigate and respond to all internal concerns appropriately and in a timely manner. We will provide feedback to reporters, as appropriate.
- 10.8 The Company will always seek to learn from any issues raised by reporters, and, where appropriate, use these learnings to improve our fraud risk management measures.

11 AWARENESS AND TRAINING

- 11.1 All staff will receive regular training on fraud. New joiners will receive training as part of the induction process. Further training will be provided as a minimum once every two years.

12 RESPONDING TO A FRAUD INCIDENT

- 12.1 In the event that the Company falls victim to, or is used for fraudulent activity, we shall ensure the incident is managed swiftly and effectively.
- 12.2 Central to our response procedures is early detection, so prompt reporting of any concerns or suspicions is vital. We rely on you to remain vigilant and promptly report anything that does not feel right, in the correct way, as soon as possible. See section 10 for information on how to report concerns.
- 12.3 We will investigate all internal concerns raised appropriately and in a timely manner.
- 12.4 Where a fraud incident is confirmed, the specific actions we take will depend on the nature of the fraud, but generally we may:
 - 12.4.1 consider whether to take any legal action, e.g. obtain an injunction or freeze assets;
 - 12.4.2 make necessary and appropriate notifications, e.g. to our bank, insurers, customers, etc;
 - 12.4.3 seek external expert advice;
 - 12.4.4 consider whether it is necessary and appropriate to self-report to prosecution authorities.
- 12.5 We will feed any fraud events into subsequent risk assessment activities.

13 MONITORING AND REVIEW

- 13.1 The nature of fraud risks faced by our organisation changes and evolves over time, e.g. as a result of external developments, changes in our activities, etc.
- 13.2 The Data Protection & Compliance Officer has overall responsibility for this policy and monitors it to make sure it is being effective. In doing so they act in the interest of the Company as a whole, and it is therefore the responsibility of all of us to help them in this.

14 CONSEQUENCES FOR BREACHING OUR PROCEDURES, THIS POLICY, AND FOR COMMITTING FRAUD

- 14.1 The Company will not tolerate fraud. The consequences of committing fraud cannot be overstated:
 - 14.1.1 individuals can be sentenced to long prison sentences for committing fraud.
 - 14.1.2 the Company can be prosecuted under ECCTA 2023 for failing to prevent fraud.
 - 14.1.3 the Company could be liable to pay significant financial penalties.
 - 14.1.4 reputational damage.
 - 14.1.5 losses for our customers or suppliers.
- 14.2 Failing to comply with this policy, and related procedures, could weaken our fraud prevention framework and thereby leave us vulnerable to falling victim to fraud. Again, this can cause immeasurable reputational damage and potential losses for our customers or suppliers.
- 14.3 As such, the Company takes compliance with this policy and related procedures very seriously.
- 14.4 Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. Any non-employee who breaches this policy is liable to have their contract terminated with immediate effect.

Owner: Data Protection & Compliance Officer
Version: 1.0
Board Approval: 6 October 2025
Classification: Internal Only