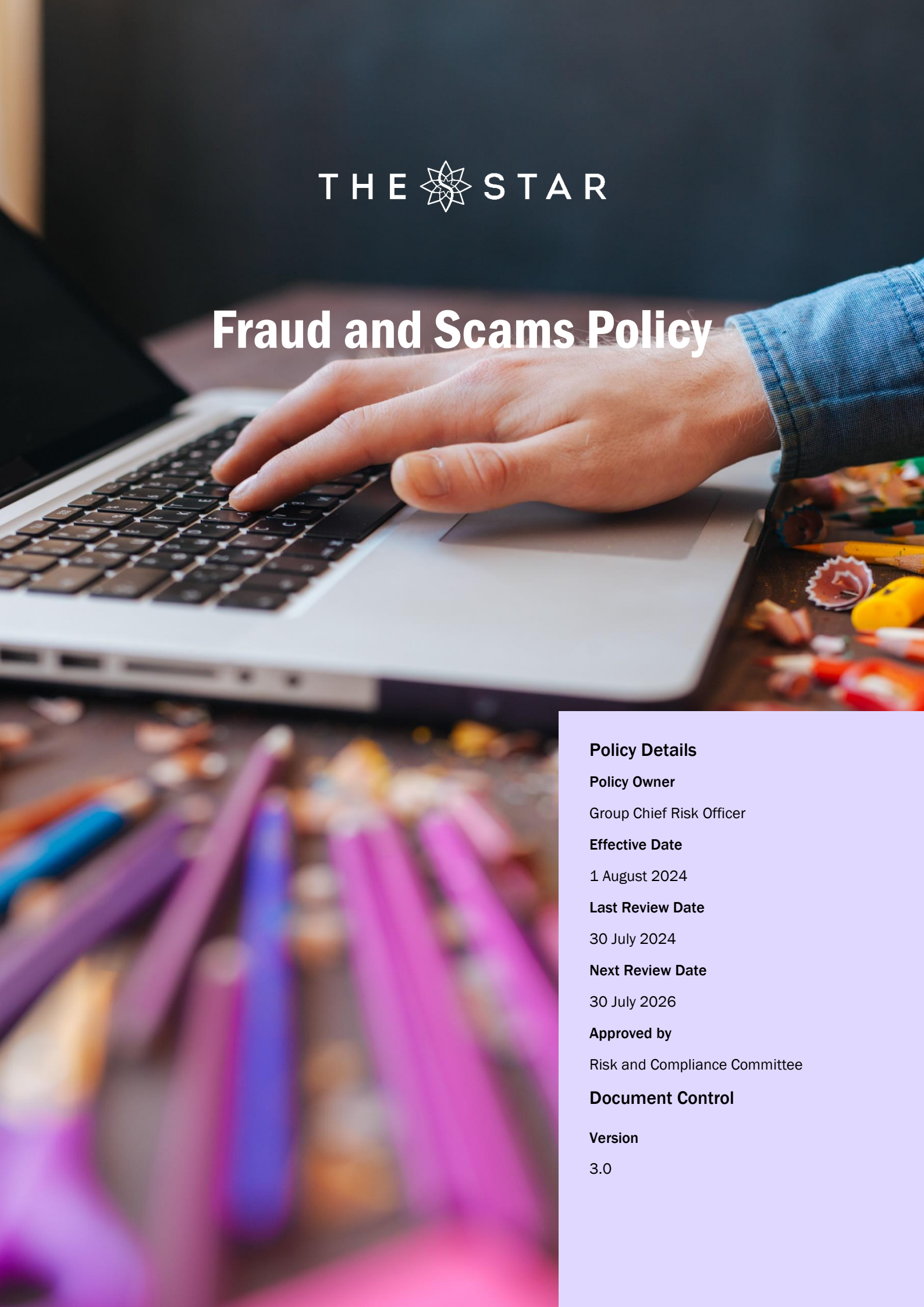

THE STAR

Fraud and Scams Policy

Policy Details

Policy Owner

Group Chief Risk Officer

Effective Date

1 August 2024

Last Review Date

30 July 2024

Next Review Date

30 July 2026

Approved by

Risk and Compliance Committee

Document Control

Version

3.0

TABLE OF CONTENTS

Version	Amended by	Reason for change	Details of changes	Date
1.0	Group Compliance	Original issue	N/A	1 June 2018
2.0	Group Compliance	Minor enhancement	N/A	29 June 2021
2.1	Group Compliance	Whistleblower service contact information updated	N/A	22 February 2023
3.0	Ritu Bhandari, General Manager Financial Crime	Policy periodic review	• Update to New Policy Template • Included Scams into the policy. • Enhanced requirement for customer support. • Included requirement for a fraud and scams risk self-assessment.	30 July 2024

01 Purpose and Scope

The Star Entertainment Group (**TSEG**) is committed to conducting business in a manner which is, ethical, professional, and compliant with our legal obligations and Code of Conduct.

To protect our customers and TSEG, the Fraud and Scams Policy (this **Policy**) sets out the minimum requirements for TSEG to identify, mitigate and manage the risk of fraud and scams.

The Policy applies to all TSEG Team Members (including Director and Executives) and Contractors at all TSEG locations.

02 Policy Requirements

2.1 Guiding Principles

2.1.1 Anyone can be impacted by fraud and scams, including our Team Members, guests, and our business. TSEG has an obligation to identify, mitigate and manage fraud and scams risk and to minimise the consequences when they occur.

2.1.2 TSEG's conduct in the management of fraud and scams is guided by the following:

- Zero Tolerance – TSEG has no tolerance for fraudulent conduct or scams committed by guests or Team Members or other third parties against guests and TSEG and will take appropriate action against any individual committing fraudulent activity or scams.
- Protect and Support our Customers – TSEG provides information about potential fraudulent conduct or scams occurring at TSEG to raise guest's awareness. TSEG also offers help to guests that may have been the victim of a fraud or scam, including providing information on what will take place through an investigation, external resources, updates on investigations, and access to the Investigations Team for information.
- Report and Escalate – Team Members must be vigilant and report any suspicions of fraudulent activity or scams to their immediate Supervisor or Manager, or through another appropriate channel.
- Assess Risk – TSEG conducts and documents risk assessments to identify and assess the risk of fraud and scams through its operations. This will inform required controls to mitigate and manage identified risks.
- Implement Controls – TSEG must have controls in place to mitigate and manage its fraud and scams risk.
- Investigation–TSEG takes allegations of fraud and scams seriously and confidentially investigates reported concerns.
- Stay Aware and Complete Training – TSEG provides resources to its Team Members on how to identify, mitigate, manage and report fraud and scams. Team Members must complete mandatory training related to their roles, including Code of Conduct training.

2.2 Identifying Fraud and Scams

Fraud

2.2.1 Fraud involves dishonestly obtaining a benefit, or causing a loss, by deception, theft, collusion or by other means.

2.2.2 Fraud can be categorised as:

- Internal Fraud – fraud committed by internal personnel, such as Team members or Contractors, or
- External Fraud – fraud committed by external persons, such as Third-Party Suppliers or customers.

2.2.3 The following table sets out examples of fraud activity that can impact our guests and TSEG.

Table 1. Examples of Fraud

Fraud Victims	Examples of Fraud Activity
Our Guests	• A third person using a guest's identification or membership card • A person stealing, including skimming, a guest's TSEG membership card or bank card • An unauthorised person accessing and using a guest's Star Account, including "friendly fraud" where a guest's family or friend may impersonate a guest of TSEG. • Stealing of chips or property from other players
TSEG	• A guest or Team Member using counterfeit currency or chips, or stealing • A guest or Team Member intentionally abusing a faulty TSEG process or system • A Team Member failing to declare a conflict of interest • A Team Member deliberately recording incorrect hours in timesheets • A Team Member submitting false expense claims for reimbursement • Any person's alteration, falsification, or fabrication of records or documents • A Team Member giving a guest access to a property or service at no cost (or a heavily discounted cost) • A guest disputing legitimate charges with merchants claiming they were unauthorised

Scams

2.2.4 Scams are when an individual is deceived into providing personal or financial information to someone with the intention of gaining a benefit.

2.2.5 The following table sets out some examples of what scams can look like for our guests and for TSEG.

Table 2. Examples of Scams

Scam Victims	Examples of scam activity
Our Guests	• Fake apps, websites, emails or social media accounts that try to impersonate TSEG, asking the guest for personal information • A call from a person claiming to be a team Member of TSEG offering a special prize but requesting credit card details to cover

Scam Victims	Examples of scam activity
	fees, or to verify credit card information due to a computer system issue. • Guests unknowingly trying to use counterfeit tickets for shows or events at TSEG. • A Team Member overcharging guests for services or unauthorised charges on their bills. • Fake Wi-Fi networks resembling TSEG's, set up to capture sensitive information when guests (or Team Members) connect.
TSEG	• Fake invoices being sent to TSEG for services or products that were not ordered. • People posing as legitimate vendors or suppliers and redirecting payments to their accounts. • Emails or messages that appear to be from legitimate sources requesting sensitive information. • Individuals claiming to be a high-level individual requesting Team Members to reveal confidential information or do something like buy gift cards for someone's birthday on their corporate card. • Individuals applying for jobs using a fake identity. • Fake bids or proposals for contracts or services being submitted with the intention of gaining confidential information or payments.

2.3 Managing and Reporting Fraud and Scams

2.3.1 Fraudulent conduct and scams can be better managed by TSEG if incidents are promptly identified and escalated by Team Members. Reporting of incidents must occur in compliance with the Incident and Breach Management Policy.

2.3.2 Team Members must report any suspicions of fraudulent activity or scams to their immediate Manager or Supervisor, or to:

- The Investigations Team via starinvestigators@star.com.au (NSW) or investigationsqld@star.com.au (QLD)
- TSEG's Whisteblower Service through star.relyplatform.com/report or 1800 319 826
- Our Cyber Security Team via Cyber@Star.com.au if it concerns a fraudulent website, app or link.

2.3.3 For any fraud or scams related to our Casino operations (i.e., in relation to the operations of gaming), an Unusual Activity Referral must be raised within 12 hours of being detected.

2.3.4 If a Team Member suspects that a guest account or identity has been compromised, they must take steps to ensure that the guest's account is secure and inform them of available support. For example, by directing the guest to the TSEG's Complaints Team, Australian Signals Directorate or Scamwatch.

2.3.5 Team Members should direct a guest that wants to report fraudulent activity or scams related to TSEG to Contact Us | The Star.

2.3.6 Business procedures dealing with frauds and scams on our guests must set out how losses claimed by guests from fraud or scams are escalated and addressed.

03 Roles and Responsibilities

Role	Responsibilities
Risk and Compliance Committee	• Communicate to TSEG Board all serious matters relating to the administration of or investigations resulting from the application of this Policy. • Receiving reports from the Investigations and Breach Team regarding breaches of this Policy. • Reviewing the effectiveness of this Policy and other measures in place to prevent and detect fraud. • Review and approve the Fraud and Scams Policy.
Group Chief Risk Officer (or delegate)	• Overseeing the application of this Policy and recommending to the Risk and Compliance Committee any amendments that may be required to maintain its ongoing effectiveness. • Review and approve the Fraud and Scams Policy.
All Team Members	• Perform their role and tasks in a manner consistent with this Policy. • Be vigilant for instances of suspected fraud or illegal activity. • Undertake all mandatory training. • Report suspicions of fraudulent activity or Scams. • Provide information that is true and correct when it is requested by investigators, regulators, or law enforcement agencies.
Group Investigations	• Investigate any reported fraud incidents. • Consult with the Group Chief Risk Officer to agree actions from findings. • Report any significant matters to the Group Chief Risk Officer and General Manager Financial Crime. • Liaising with law enforcement or regulatory bodies where necessary in relation to fraud or scams related activity.
Line 2 Financial Crime	• Review and update the Fraud and Scams Policy at least every 2 years. • Provide advisory support to business unit in identifying and managing the risk of fraud and scams.
Leaders	• Maintain business procedures which set out how frauds and scams are actioned including up to date including how losses claimed by guests from fraud or scams are escalated and addressed. • Support your teams in feeling safe to report suspected fraud or illegal activity. • Take all reports of suspected fraud or illegal activity seriously. • Escalate significant fraud reports to the Board Risk and Compliance Committee.

04 Breaches of this Policy

TSEG is committed to conducting its operations in a way that meets its commitments to regulators, guests, and the wider community. Non-conformance with a policy, including this policy, can pose a significant risk to TSEG, guests, and the wider community, potentially resulting in punitive measures against TSEG.

Team Members who become aware of an actual or possible breach of this policy must follow the established protocols set out in the Incident and Breach Management Policy. The Incident and Breach Management Policy has strict timelines in place to satisfy regulatory requirements; if a Team Member has reason to believe that a breach may have occurred it is imperative that those protocols are followed expeditiously to avoid adverse consequences.

Non-conformance with this policy may also amount to a breach of TSEG's Code of Conduct and values. Breaches of the Code of Conduct may result in disciplinary action, including termination of employment, fines, penalties, and potential prosecution.

05 Definitions

Term	Definition
Benefit	A benefit can tangible or intangible, for example cash as a tangible or information as an intangible.
Contractor	Means one of the following: • Independent contractors: self-employed individuals or are part of a proprietary company (ABN) usually engaged for project work and paid for results achieved. • Contingent workers: individuals engaged to ensure coverage or support for TSEG roles. For example, a contingent worker is in a role that is vacant, whilst the position is being recruited. • Consultants: individuals engaged to deliver set outcomes, provide advice or recommendations, and are usually paid on completion of milestones or deliverables. Procurement is to be engaged when considering using consultants to agree the terms and conditions with TSEG.
Team Member	Means full-time, part-time and casual employee of TSEG.
TSEG	The Star Entertainment Group Limited and its subsidiary.

06 Relevant Legislation and Regulations

- Corporations Act
- Crimes Act (NSW)
- Criminal Code (QLD)

07 Related Policies and Documentation

The following policies and documentation related to this policy can be found on TSEG's intranet site:

- Risk Appetite Statement

- Code of Conduct
- Whistleblower Protection Policy
- Incident and Breach Management Policy
- Cyber Resilience Standard – Threat Management

08 Feedback and Questions

Please contact the Financial Crime Policy and Risk Assessments team for any questions relating to this policy.