PRIVACY POLICY FOR "REPORT A SCAM"

Website: www.strategyindia.com
Effective Date: 10 October 2025
Last Updated: 20 November 2025

1. INTRODUCTION AND LEGAL FRAMEWORK

This Privacy Policy governs the collection, use, disclosure, and protection of personal data submitted through Strategy India's "Report A Scam" fraud reporting system (the "System"). The System enables victims, informants, complainants, and witnesses (collectively, "Reporters" or "you") to report suspected multilevel marketing (MLM) fraud and other deceptive business operations deploying unlawful MLM compensation plans.

This Policy is issued in compliance with India's Digital Personal Data Protection Act, 2023 (DPDP Act) and the rules, notifications, and directions issued thereunder, as amended from time to time, and applies to all personal data processed in connection with fraud reports submitted to Strategy India.

CRITICAL NOTICE

This System is an intelligence-gathering and public awareness mechanism, not a law enforcement platform. Strategy India is not a government agency and does not conduct criminal investigations. Information you provide may be shared with law enforcement authorities to facilitate investigations and protect the public from fraudulent schemes.

2. DATA FIDUCIARY AND GRIEVANCE OFFICER

Data Fiduciary
Strategy India
Level 17, Unit No. 1701–1704, Wing B & C
One BKC Centre, Plot No. C-66, G Block
Bandra Kurla Complex
Bandra East, Mumbai 400051
India
Email: info@strategyindia.com
Phone: +91-22-40238899

Grievance Officer (DPDP Act)
Name: Akshay Y
Designation: Legal Officer & Grievance Officer
Email: info@strategyindia.com
Phone: +91-22-6807 3106
Address: Level 17, Unit No. 1701–1704, Wing B & C
One BKC Centre, Plot No. C-66, G Block
Bandra Kurla Complex
Bandra East, Mumbai 400051
India
Business Hours: Monday to Friday, 09:30–18:00 Indian Standard Time (IST) (excluding public holidays)

The Grievance Officer is your primary point of contact for all privacy-related queries, rights requests, and complaints under the DPDP Act.

3. CATEGORIES OF PERSONAL DATA COLLECTED

3.1 Reporter Information
When you submit a fraud report, Strategy India may collect the following:
Identity Data:

- Full name
- Contact details (email address, telephone number, postal address)
- National identification, if voluntarily provided (PAN, Aadhaar, Voter ID, driving licence)
- Relationship to the alleged fraud (victim, witness, family member, former participant, concerned citizen)

Victimisation Data (if applicable):

- Financial loss information (investment amounts, dates, payment methods, transaction records)
- Duration and nature of involvement with the alleged fraudulent scheme
- Psychological, emotional, or other impacts experienced
- Family members or associates affected

Evidence and Documentation:

- Copies of contracts, enrolment forms, compensation plans, promotional materials
- Screenshots, photographs, video recordings, audio recordings
- Bank statements, payment receipts, tax documents
- Email correspondence, WhatsApp/SMS messages, social media posts
- Website URLs, mobile application details, and presentation materials

3.2 Third-Party Data
Information about individuals or entities you believe are operating fraudulent schemes, deploying unlawful MLM compensation plans:

- Names of promoters, directors, founders, stakeholders, senior leaders, and beneficiaries
- Company/entity names (registered and trading names)
- Business addresses, websites, social media profiles
- MLM compensation plan structure and payout commitments
- Product/service descriptions (or absence thereof)
- Recruitment tactics and misleading representations
- Organisational structure and hierarchy

Important: By submitting third-party data, you represent and warrant that you have obtained such information lawfully and that its disclosure is necessary for fraud reporting purposes.

3.3 Technical Data

- IP address and device information (automatically collected upon access/submission to the System)
- Date, time, and method of submission
- Email metadata and submission timestamps

4. PURPOSES OF PROCESSING AND LEGAL BASES

Strategy India processes personal data from fraud reports for specific, lawful purposes, grounded in legal bases under the DPDP Act (Section 4):

Purpose	Categories of Data	Legal Basis
Fraud analysis and intelligence	all categories	consent (voluntary submission) + Legitimate use (prevention/detection of fraud under DPDP Act Section 7)
Law enforcement coordination	reporter information, scheme details, and evidence	Legitimate use (prevention/detection/investigation/prosecution of offence) + Legal obligation
Public awareness and early warning	Anonymised scheme information,	Consent + Legitimate use (public interest in fraud prevention)

	anonymised victim data	
Reporter protection	Reporter identity and contact details	Legitimate use (security safeguards) + Legal obligation (whistleblower protection principles)
Research and policy advocacy	Aggregated, anonymised data	Legitimate use (research and statistical purposes with irreversible anonymisation)
Legal compliance and defence	All relevant data	Legal obligation + Legitimate use (establishment/exercise/defence of legal claims)
Communication with Reporters	Reporter contact details	Consent + Performance of contract (provision of reporting service)

5. CONSENT AND VOLUNTARY SUBMISSION

5.1 Nature of Consent
By submitting a fraud report through the System, you provide your free, specific, informed, unconditional, and unambiguous consent for Strategy India to process your personal data for the purposes outlined above.
Your consent is demonstrated through:

- Reading this Privacy Policy and associated Terms of Use before submission.
- Completing the fraud report form with accurate information
- Clicking "Submit" or sending the report via email with acknowledgement of these terms

5.2 Voluntariness
Submission of fraud reports is entirely voluntary. You are under no obligation to report suspected fraud to Strategy India. However, if you choose to report, you must provide sufficient information to enable meaningful analysis and potential law enforcement referral.
Strategy India does not:

- Charge fees for submitting fraud reports
- Condition any other service on your submission of a fraud report
- Exercise coercion, undue influence, fraud, or misrepresentation in obtaining consent

5.3 Informed Decision-Making
Before submitting a report, you should understand:

- What data is collected (Section 3 above)
- How it will be used (Section 4 above)
- With whom it may be shared (law enforcement, public via anonymised alerts)
- Your rights (access, correction, erasure, withdrawal, grievance redressal)
- Limitations (Strategy India cannot guarantee investigation, prosecution, or recovery of losses)
- Risks (submission does not create attorney–client privilege; information may be used in legal proceedings)

6. INFORMANT AND VICTIM IDENTITY PROTECTION

Strategy India recognises the heightened sensitivity and vulnerability of fraud victims, as well as the potential risks faced by informants and whistleblowers.

6.1 Confidentiality Protections
Default Confidentiality:

- Your identity (name, contact details, identification documents) is treated as strictly confidential.
- Reporter information is stored separately from fraud scheme data in secure, access-restricted systems.

- Only authorised Strategy India personnel involved in fraud analysis and law enforcement coordination have access to Reporter identities.

Public-Facing Materials:

- Scam alerts, case studies, website listings, and media communications are fully anonymised.
- No names, locations, specific financial amounts, or other identifying details of Reporters are disclosed publicly without explicit written consent.
- Third-party fraud scheme details (promoter names, company names) may be published as necessary for public warning purposes.

6.2 Disclosure to Law Enforcement

Disclosure Framework:
When sharing fraud reports with law enforcement agencies, Strategy India follows these principles:

i. Threshold Assessment: Information is shared only when there is a credible indication of potentially unlawful activity warranting investigation
ii. Necessity Limitation: Only data necessary and relevant to the investigation is disclosed; extraneous personal details are redacted where possible
iii. Authorised Recipients: Disclosure is limited to:
    a. Police departments (including cybercrime cells and Economic Offences Wings).
    b. Central agencies (including the Enforcement Directorate and the Central Bureau of Investigation for multi-state schemes, and the Serious Fraud Investigation Office).
    c. Regulatory and specialised enforcement authorities (including the Ministry of Consumer Affairs, State consumer commissions, the Reserve Bank of India, and the Securities and Exchange Board of India, as applicable).
    d. Competent authorities under the Whistleblower Protection Act, 2014 and other applicable laws.
iv. Reporter Identity: Your identity may be disclosed to law enforcement:
    a. With your explicit consent (if you opt to be identifiable to authorities), or
    b. When legally compelled (court order, summons, statutory obligation), or
    c. When necessary for investigation (authorities require your contact for a witness statement, clarification, or evidence corroboration)
v. Confidentiality Requests: Strategy India communicates to receiving authorities that the Reporter's identity should be protected and not disclosed publicly unless required by law or with the Reporter's consent
vi. No Control Over Authority Actions: Once information is provided to law enforcement, Strategy India cannot control how authorities use, store, or further disclose the data. Authorities are governed by their own legal frameworks (including the Bharatiya Nagarik Suraksha Sanhita, 2023, and applicable investigation manuals, as amended from time to time).

6.3 Retaliation Prevention

Strategy India does not tolerate retaliation against Reporters. If you experience or fear victimisation, harassment, threats, or other retaliatory conduct related to your fraud report:

- Notify our Grievance Officer immediately.
- Document incidents with dates, descriptions, and evidence
- We will assess appropriate measures, which may include:
    - Notifying law enforcement of threats
    - Providing guidance on legal protections available under the Whistleblower Protection Act, 2014, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and other applicable laws.
    - Adjusting confidentiality protocols

Note: Strategy India cannot provide physical security, legal representation, or financial compensation for retaliation. Reporters facing threats should contact the police immediately.

7. DATA SHARING AND DISCLOSURE

Strategy India does not sell, rent, or trade personal data from fraud reports.

We may share personal data with the following categories of recipients:
Law Enforcement Agencies (police, Economic Offences Wings, Enforcement Directorate, Central Bureau of Investigation, consumer protection authorities)

- Purpose: Investigation and prosecution of fraud, money laundering, and consumer protection violations
- Safeguards: Disclosure limited to necessary data; identity protection requested; legal basis under DPDP Act Section 4 (prevention/detection/investigation/prosecution of offence)

Legal Advisors and Forensic Experts

- Purpose: Analysis of complex schemes, legal opinion on reporting obligations, expert testimony
- Safeguards: Bound by professional confidentiality and attorney–client privilege; Data Processing Agreements executed

IT Service Providers

- Purpose: Hosting, data storage, email services, and cybersecurity
- Safeguards: Data Processing Agreements mandating DPDP compliance, confidentiality, security measures, and deletion upon termination

Courts and Tribunals

- Purpose: Compliance with subpoenas, court orders, legal proceedings involving reported schemes or Strategy India's fraud analysis
- Safeguards: Disclosure as legally compelled; protective orders sought where feasible

Regulatory and Government Authorities

- Purpose: Compliance with statutory obligations (Data Protection Board inquiries, Ministry of Corporate Affairs filings)
- Safeguards: Limited to legally required information

No disclosure to third parties for marketing or commercial purposes.

7.1 Anonymised and Aggregated Data
Strategy India may publicly share or use for research purposes aggregated, anonymised data that cannot be used to identify Reporters or individual victims:

- Statistical trends (e.g., "70% of reported schemes involve cryptocurrency products")
- Geographic distribution of fraud complaints
- Typologies and modus operandi of MLM fraud
- Policy recommendations based on fraud patterns

Such anonymisation is irreversible and does not constitute personal data under the DPDP Act.

8. DATA RETENTION AND DELETION

8.1 Retention Principles
Personal data from fraud reports is retained only for as long as:

1. Purpose remains valid: Investigation is ongoing, law enforcement case is active, public warning is necessary
2. Legal obligation exists: Statutory retention mandates, legal hold due to litigation or inquiry
3. Legitimate interest persists: Fraud intelligence value, policy research, defence against legal claims

8.2 Retention Periods

Data Category	Retention Period	Justification
Active case files	Duration of investigation + 5 years post-closure	Law enforcement coordination; potential related cases; criminal limitation periods (3–7 years depending on offence)
Closed case files	7 years from case closure	Historical intelligence; typology research; potential delayed enforcement; standard archival practice.
Reporter contact information	3 years from last communication	is adequate for follow-up queries; the civil claims limitation period.
Evidence materials	same as case file retention	evidentiary value; potential future legal proceedings
Anonymised public alerts	Indefinitely	Public interest in fraud awareness; no personal data retention (fully anonymised)
System logs and audit trails	1 year minimum (DPDP Rules requirement)	Security monitoring, compliance audits, and incident investigation

8.3 Exceptions and Extensions
Legal Hold:
If a fraud report becomes subject to litigation, government investigation, court proceedings, or regulatory inquiry, retention is extended indefinitely until the matter is fully resolved (including appeals).
Reporters will be notified of legal holds where practicable and legally permissible.
Ongoing Fraud Schemes:
For schemes that remain operational and pose ongoing public risk, retention of case intelligence continues as long as the scheme operates or until law enforcement action is taken.

8.4 Deletion Process
When retention criteria are no longer met:
Step 1 – Assessment: Quarterly reviews identify case files eligible for deletion.
Step 2 – Deletion Notice: If we have contact information and you have requested updates, a deletion notice is sent:
"Your fraud report regarding [Scheme Name] submitted on [Date] is scheduled for deletion on [Date]. This data will be permanently erased from our systems. If you have concerns or wish to retrieve a copy, contact us immediately."
Step 3 – Secure Deletion:

- Primary databases: Data permanently deleted and overwritten
- Backups: Flagged as deleted; overwritten on next backup cycle (typically 30–90 days)
- Data processors: Deletion instructions propagated to all service providers (cloud storage, email systems)
- Physical records: Shredded/destroyed with certificate of destruction

Step 4 – Confirmation: Deletion completion logged in the audit trail.
Step 5 – Anonymised Retention: If public interest justifies continued alert, scheme information is retained in fully anonymised form (no link to Reporter or identifiable victims).

9. DATA SECURITY MEASURES

Given the highly sensitive nature of fraud victim data and the potential risks to informants, Strategy India implements enhanced security safeguards:

9.1 Technical Security

Encryption:

- Data in Transit: TLS 1.3 for all communications (email, web forms, file uploads)
- Data at Rest: AES-256 encryption for databases, file storage, backups
- End-to-End Encryption: For highly sensitive submissions (threats of violence, organised crime involvement), secure messaging platforms are available

Access Controls:

- Role-Based Access Control: Only the fraud investigation team and senior management have access to Reporter identities
- Multi-Factor Authentication: Required for all system access
- Access Logging: All access to fraud reports logged with user ID, timestamp, actions taken; logs reviewed quarterly
- Data Segregation: Reporter identity data stored separately from fraud scheme data; elevated privileges required for access

Network and Application Security:

- Firewalls, intrusion detection/prevention systems
- Regular vulnerability scanning and penetration testing (annually minimum)
- Secure development practices (input validation, injection attack protection)
- Anti-malware and anti-ransomware tools

9.2 Organisational Security

Personnel:

- Background checks for all staff handling fraud reports
- Confidentiality and non-disclosure agreements bind all employees and contractors
- Annual data protection and security awareness training
- "Need-to-know" principle strictly enforced

Physical Security:

- Restricted access to offices and data storage areas (biometric/keycard)
- Secure document disposal (shredding, certified hard drive destruction)
- CCTV monitoring of physical access points

Third-Party Management:

- Due diligence before engaging data processors (security certifications, track record)
- Data Processing Agreements with comprehensive security obligations
- Periodic compliance audits

9.3 Incident Response and Breach Notification

Data Breach Protocol:

In the event of unauthorised access, disclosure, loss, alteration, or destruction of personal data from fraud reports:

Immediate Response (0–24 hours):

- Contain breach (isolate affected systems, revoke compromised credentials)
- Preserve forensic evidence
- Assess scope (what data accessed, how many Reporters affected, likelihood of harm)

Investigation (24–72 hours):

- Root cause analysis
- Determine risk to Reporters (identity exposure, retaliation risk, financial fraud risk)

Notification (within 72 hours of breach awareness):

- Data Protection Board of India: Detailed report including nature of breach, data categories, number of affected Reporters, measures taken, contact information
- Affected Reporters: If real risk of harm exists, individualised notification via email/telephone, including:
    - Description of breach
    - Categories of data compromised
    - Likely consequences and risks
    - Measures taken to mitigate harm
    - Guidance on protective actions
    - Grievance Officer contact for questions

Law Enforcement (if applicable):
- Notify police if breach involves criminal conduct (hacking, data theft)
- Coordinate with authorities to assess risks to Reporters

Remediation:
- Implement corrective measures to prevent recurrence
- Offer support to affected Reporters (identity monitoring services, legal guidance referrals)
- Post-incident review and security enhancements

Penalties: The DPDP Act imposes penalties up to ₹250 crore for failure to implement adequate security safeguards and up to ₹200 crore for failure to notify breaches.

10. DATA PRINCIPAL RIGHTS UNDER DPDP ACT

As a Reporter/Data Principal, you have the following rights:

10.1 Right to Access

You may request:
- Confirmation of whether Strategy India processes your personal data
- Summary of your fraud report(s) and related data held
- Copy of personal data in a structured, machine-readable format

How to Exercise: Email Grievance Officer with sufficient details to identify your report (approximate submission date, scheme name, contact email used for submission).
Response Time: Within 30 days (may be extended by 15 days for complex requests with notice).
Fee: The first request in 12 months is free. Subsequent requests may incur a reasonable administrative fee (maximum ₹500) if excessive or repetitive.

10.2 Right to Correction

You may request correction of inaccurate, incomplete, or outdated information in your fraud report.
Process:
- Identify specific data to be corrected and provide accurate information
- We verify the correction (may request supporting documentation)
- Corrections made within 15 days
- Updated information propagated to law enforcement if already shared (with explanation that the reporter corrected)

10.3 Right to Erasure / Right to Be Forgotten

You may request deletion of your fraud report and personal data when:
- Purpose has been fulfilled (investigation completed, scheme shut down)
- You withdraw consent, and no other legal basis exists
- Data is no longer necessary
- Processing was unlawful

Exceptions (we may refuse erasure if):
- Legal obligation: Court order, regulatory inquiry requires retention
- Legal claims: Ongoing litigation or potential claims involving the reported scheme or Strategy India's fraud analysis

- Law enforcement needs: Active investigation or prosecution where evidence is required
- Public interest: Scheme remains operational and poses ongoing public risk (may retain anonymised version)

Response: Within 30 days, either confirmation of deletion or a reasoned refusal citing the applicable exception.

10.4 Right to Withdraw Consent
You may withdraw consent for processing your fraud report at any time.
How: Contact the Grievance Officer stating your intent to withdraw consent.
Consequences:

- Processing for consented purposes ceases within 48 hours (except for legal retention obligations)
- Does not affect the lawfulness of processing prior to withdrawal
- Strategy India may retain an anonymised version for public warning.
- If the report has already been shared with law enforcement, we cannot "unshare" it, but we will notify you of the extent of any prior disclosure.

Note: Withdrawal may limit our ability to assist with investigations or provide case updates.

10.5 Right to Grievance Redressal
You may file complaints regarding:

- Alleged violations of the DPDP Act or this Privacy Policy
- Refusal of rights requests
- Security concerns or suspected breaches
- Misuse of Reporter information
- Retaliation or victimisation

Internal Grievance Mechanism:
Step 1 – File Complaint:

- Email: info@strategyindia.com
- Telephone: +91-22-6807 3106
- Written Notice: Strategy India, Level 17, Unit No. 1701–1704, One BKC Centre, Bandra Kurla Complex, Mumbai 400051

Required Information:

- Your name and contact details
- Fraud report reference (if applicable)
- Description of complaint with specific details
- Evidence or supporting documents
- Desired resolution

Step 2 – Acknowledgement:

- Unique complaint reference number assigned
- Acknowledgement within 3 business days

Step 3 – Investigation:

- Grievance Officer reviews complaint, consults internal teams, examines records
- May request additional information from you

Step 4 – Resolution:

- Response within 15 business days (may extend to 30 days for complex matters with notice)
- Response includes: findings, corrective action taken or justification for no action, right to escalate

External Escalation:
If dissatisfied with Strategy India's response, you may file a complaint with:

Data Protection Board of India
(Address: TBD upon full operationalisation)
The Board may investigate, request information from Strategy India, issue directions, and impose penalties.

10.6 Right to Nomination

You may nominate an individual (family member, trusted person) to exercise your data principal rights on your behalf in the event of your death or incapacity.
How:

- Submit a nomination in writing with the nominee's name, contact details, relationship, and scope of authority
- Update or revoke at any time

11. SPECIAL CONSIDERATIONS FOR VULNERABLE REPORTERS

11.1 Minor Victims (Under 18)

If the fraud victim is under 18 years of age, verifiable parental/guardian consent is required before processing personal data.
Process:

- Parent/guardian submits fraud report on behalf of minor
- Verification of parent–child relationship (ID proof, birth certificate)
- Consent obtained from parent/guardian with understanding of purposes and risks

Prohibited: Tracking, behavioural monitoring, or targeted actions directed at minors.

11.2 Psychological Support

Fraud victimisation can cause significant emotional distress. While Strategy India is not a counselling service, we can provide:

- Referrals to victim support organisations
- Information about consumer protection forums and compensation schemes
- Guidance on legal remedies available

11.3 Financial Vulnerability

We recognise that many Reporters have suffered substantial financial losses. However:

- Strategy India does not provide financial compensation, loans, or recovery assistance
- We do not guarantee recovery of lost funds
- We may refer to legal aid services or pro bono attorneys where appropriate

12. LIMITATIONS AND DISCLAIMERS

12.1 No Attorney–Client Privilege

Submitting a fraud report to Strategy India does not create an attorney–client relationship, nor does it establish any legal privilege protecting your communications from disclosure.
Information you provide may be disclosed to law enforcement and used in legal proceedings. If you require confidential legal advice, consult a licensed attorney before submitting a report.

12.2 No Investigation Guarantee

Strategy India analyses fraud reports and shares intelligence with law enforcement, but:

- We do not conduct criminal investigations (we are not a law enforcement agency)
- We cannot guarantee that authorities will investigate your report
- We cannot compel enforcement actions, arrests, prosecutions, or asset recovery
- Law enforcement prioritisation and resource allocation are beyond our control

12.3 No Liability for Third-Party Actions

Strategy India is not responsible for:

- Actions or inactions of law enforcement agencies
- Outcomes of investigations or prosecutions
- Decisions by courts or regulatory bodies
- Continued operation of fraudulent schemes despite reporting
- Retaliation by scheme operators against Reporters (though we take measures to protect identity)

12.4 Reporter Responsibility for Evidence
You are responsible for ensuring that the evidence and third-party data you submit:
- Is obtained lawfully and does not violate the privacy rights of others
- Is accurate to the best of your knowledge
- Does not contain defamatory, false, or malicious content

Strategy India is not liable for the reporter's unlawful data collection or false reporting.

13. INTERNATIONAL TRANSFERS

If fraud reports involve international MLM schemes or evidence stored on servers outside India:
Cross-Border Transfers:
- Personal data may be transferred to jurisdictions where alleged fraudsters operate, where authorities have jurisdiction, or where the cloud infrastructure is located.
- We implement safeguards: Data Processing Agreements, encryption, and access controls.
- Transfers comply with DPDP Act requirements (adequacy determination or consent-based transfers as applicable)

Reporter Notice: By submitting a fraud report involving international schemes, you acknowledge potential cross-border data flows necessary for investigation and enforcement.

14. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy to reflect:
- Changes in the DPDP Act, Rules, or regulatory guidance
- Enhancements to security measures or data handling practices
- Feedback from Reporters or law enforcement
- Best practices in victim data protection

Notification of Changes:
- Updated "Last Updated" date at the top of the Policy
- Material changes (affecting purposes, sharing, retention, rights): email notification to Reporters with active contact information at least 14 days before the effective date
- Prominent notice on "Report A Scam" page

Acceptance: Continued use of the System after the effective date of an updated policy constitutes acceptance. If you disagree with the changes, you may withdraw your consent and request the deletion of your data (subject to legal retention exceptions).

15. MALICIOUS PROSECUTION AND DEFAMATION SAFEGUARDS

15.1 Good-Faith Reliance on Reporter Information
Strategy India's assessment, publications, and communications regarding any reported scheme are based on a combination of:
- Information and evidence voluntarily provided by Reporters
- Independent analysis of publicly available material

Strategy India does not warrant that such information is complete, current, or free from error. To the maximum extent permitted by law, Strategy India shall not be liable for any claim alleging defamation, malicious prosecution, or other harm arising from its good-faith reliance on fraud reports and supporting materials submitted by Reporters acting under these Terms.

15.2 No Malicious Prosecution by Strategy India
Strategy India does not initiate criminal proceedings and has no authority to prosecute offences. Any decision to register FIRs, file charge sheets, or prosecute alleged fraudsters is taken solely by competent law enforcement and prosecutorial authorities in the exercise of their independent statutory powers.

Strategy India's limited role in providing information or expert analysis to such authorities shall not, by itself, constitute "prosecution" or "malicious prosecution" in law, and Strategy India shall not be liable for any claim premised on such characterisation.

15.3 Opinion and Public-Interest Commentary
Scam alerts, typology notes, and other public communications issued by Strategy India concerning reported schemes are expressions of opinion based on disclosed facts, analysis of available material, and concern for consumer protection. Such communications are made in the public interest and are not statements of undisputed fact or determinations of guilt.
To the extent they are capable of being defamatory, they are intended to fall within recognised defences of truth, fair comment, and qualified privilege under Indian law.

15.4 No Duty of Exhaustive Verification
While Strategy India undertakes reasonable checks to assess credibility and coherence of reports received, it does not assume, and expressly disclaims, any obligation to conduct exhaustive verification, forensic investigation, background checks, or audits of Alleged Fraudsters or schemes. No omission to undertake such further steps shall give rise to any claim of negligence, want of due care, or malicious intent against Strategy India.

15.5 No Agency or Joint Responsibility for Reporter Acts
Reporters act entirely in their personal capacity. Strategy India does not authorise, direct, or control how Reporters obtain information or what allegations they choose to make. The submission of a Fraud Report does not create any partnership, agency, employment, joint venture, or joint-tortfeasor relationship between Strategy India and the Reporter.
Strategy India shall not be treated as vicariously liable for any unlawful, defamatory, or malicious act of a Reporter.

15.6 Internal Legal Review for High-Risk Publications
Alerts or publications that name specific individuals or entities as Alleged Fraudsters, or that may reasonably be anticipated to cause profound reputational or economic impact, are subject to an internal escalation and review process, which may include legal consultation.
The existence of such a process evidences Strategy India's intent to act cautiously and in good faith, and shall be relevant to rebut any allegation of malice or reckless disregard for the truth.

15.7 Safe Harbour for Law-Enforcement Cooperation
To the fullest extent permissible under applicable law, no civil or criminal action shall lie against Strategy India merely for:

- Furnishing information, documents, or expert analysis to law enforcement, regulators, or courts
- Complying with summons, notices, or orders
- Giving evidence as a witness or expert

Any such cooperation is undertaken under legal compulsion or in good-faith furtherance of public interest in crime prevention.

15.8 Reporter Certification of Good-Faith Motive
By submitting a Fraud Report, you confirm that your primary motive is consumer protection and lawful enforcement of rights, and not to harass, extort, defame, or gain a competitive advantage over any person or entity. Any departure from this confirmation shall be solely your responsibility and risk.

15.9 Evidence of Good-Faith Handling in Litigation
In the event Strategy India is implicated or named in proceedings arising from a Fraud Report, Strategy India may, at its sole discretion, place on record its internal logs, review notes, and correspondence demonstrating its good-faith handling of the report.
Such material may include evidence of anonymisation efforts, verification attempts, and internal legal review, and may be relied upon to rebut allegations of malice, recklessness, or improper purpose.

15.10 Enhanced Indemnification Against Malicious Prosecution Claims
Without limiting the scope of indemnification provisions elsewhere in the Terms of Use, you agree that the indemnity covers any claims, notices, legal proceedings, or demands brought by Alleged Fraudsters or third parties alleging:

- Defamation, loss of reputation, or commercial disparagement
- Malicious prosecution, wrongful initiation of proceedings, or abuse of process
- Any other civil or criminal liability said to arise from Strategy India's transmission of your report, your evidence, or Strategy India's public-interest communications that rely in whole or in part on your submissions.

15.11 Applicable Law and Qualified Privilege
Strategy India's cooperation with law enforcement, regulators, and courts, including the provision of information, documents, or expert analysis concerning reported schemes, is undertaken in good faith in furtherance of the public interest in fraud prevention. To the fullest extent permitted under applicable Indian law (including the Bharatiya Nyaya Sanhita, 2023) and common law principles governing defamation and malicious prosecution, such cooperation is protected by qualified privilege and shall not, by itself, give rise to liability for defamation, malicious prosecution, or abuse of process.

16. CONTACT AND GRIEVANCE INFORMATION

For Privacy-Related Enquiries:
Privacy Team
Strategy India
Email: privacy@strategyindia.com
Telephone: +91-22-40238899
Address: Level 17, Unit No. 1701–1704, Wing B & C, One BKC Centre, Plot No. C-66, G Block, Bandra Kurla Complex, Bandra East, Mumbai 400051

For Rights Requests and Complaints:
Grievance Officer
Name: Akshay Y
Email: info@strategyindia.com
Telephone: +91-22-6807 3106
Address: Level 17, Unit No. 1701–1704, Wing B & C, One BKC Centre, Plot No. C-66, G Block, Bandra Kurla Complex, Bandra East, Mumbai 400051
Business Hours: Monday–Friday, 09:30–18:00 IST (excluding public holidays)
For Urgent Security Incidents:
If you believe your fraud report data has been compromised or you are experiencing retaliation:

- Email: security@strategyindia.com (monitored 24/7)
- Telephone: +91-22-40238899

TERMS OF USE FOR "REPORT A SCAM"

Strategy India Fraud Reporting System
Website: www.strategyindia.com
Effective Date: 10 October 2025
Last Updated: 20 November 2025

1. ACCEPTANCE AND SCOPE

These Terms of Use (the "Terms") govern your submission of fraud reports through Strategy India's "Report A Scam" system (the "System"). By accessing the System, submitting a fraud report, or communicating with Strategy India regarding suspected MLM fraud, you agree to be bound by these Terms and the accompanying Privacy Policy.
If you disagree, do not submit a fraud report or use the System.

1.1 Definitions
"Strategy India" / "we" / "us" / "our" refers to Strategy India and its personnel.
"Reporter" / "you" / "your" refers to any individual submitting a fraud report (victim, informant, complainant, witness)
"Fraud Report" / "Report" refers to information, evidence, and materials you submit regarding suspected MLM fraud, pyramid schemes, or deceptive business operations.
"Alleged Fraudsters" refers to individuals or entities you believe are operating fraudulent schemes.

2. NATURE OF THE SYSTEM AND STRATEGY INDIA'S ROLE

2.1 Intelligence Gathering and Public Awareness
The System is designed to:

1. Collect intelligence on suspected MLM fraud and pyramid schemes operating in India.
2. Analyse reported schemes for viability, legality, and public risk.
3. Provide early warnings to the public via anonymised scam alerts and lists.
4. Facilitate law enforcement by sharing credible reports with investigating agencies.

2.2 What Strategy India Is NOT
Strategy India is not:

- A law enforcement agency (we do not conduct criminal investigations, make arrests, or prosecute offenders)
- A consumer court or tribunal (we do not adjudicate disputes, award compensation, or issue legally binding orders)
- A financial recovery service (we do not recover lost funds, negotiate settlements, or provide monetary assistance)
- A legal representation service (we do not serve as your attorney, and no attorney–client privilege exists)
- A regulatory body (we do not have statutory authority to shut down schemes, revoke licences, or impose penalties)

2.3 Advisory and Consultancy Capacity
Strategy India operates as a private consultancy providing:

- Fraud analysis and intelligence services
- Training and advisory services to law enforcement agencies
- Policy recommendations to government authorities
- Public education and awareness campaigns

Your use of the System is voluntary and does not guarantee any specific outcome.

3. ELIGIBILITY AND CAPACITY

3.1 Age and Legal Capacity

You must be:

- 18 years of age or older and possess legal capacity to enter binding agreements under the Indian Contract Act, 1872; or
- A parent or legal guardian submitting a report on behalf of a minor victim (under 18), in which case you represent and warrant that you have authority to act on the minor's behalf and provide consent for data processing

3.2 Truthfulness and Good Faith
You represent and warrant that:

- Information in your Fraud Report is true and accurate to the best of your knowledge and belief.
- You are submitting the Report in good faith (genuine belief of fraud, not for malicious, defamatory, competitive, or vindictive purposes)
- You have a lawful basis for providing evidence and third-party data (obtained legally, not through theft, hacking, or unauthorised access)
- You are not violating confidentiality agreements, non-disclosure obligations, or other legal duties by submitting the Report.

4. SUBMISSION PROCESS AND REQUIREMENTS

4.1 Method of Submission
Fraud Reports may be submitted via:

- Email: report@strategyindia.com with subject line "Fraud Report Submission"
- Web Form: [link to secure submission form, if applicable]
- Secure Upload Portal: [link to secure file transfer portal, if applicable]

4.2 Required Information
To enable effective analysis, your Report should include:
About the Alleged Fraudulent Scheme:

- Name of entity/operation (company name, website, trading name)
- Promoters, directors, founders, key stakeholders (names, photographs if available)
- Compensation plan structure (how payouts are calculated, recruitment requirements)
- Product/service offerings (or absence thereof; token products with no real value)
- Marketing claims and representations (income promises, lifestyle portrayals)
- Evidence of unsustainability or illegality (mathematical analysis showing payouts exceed revenue, pyramid structure diagrams)

About Your Involvement/Knowledge:

- Your relationship to the scheme (victim, ex-distributor, family member, concerned observer)
- How did you learn about the scheme
- Financial loss suffered (if applicable): amounts, dates, payment methods
- Attempts to recover funds or complaints filed elsewhere

Supporting Evidence:

- Contracts, enrolment agreements, compensation plan documents
- Screenshots of websites, social media, WhatsApp groups, and presentations
- Bank statements, payment receipts, transaction records
- Videos, audio recordings, photographs
- Communication records (emails, messages with promoters/uplines)

Your Contact Information:

- Name, email, telephone number (for follow-up questions or clarifications)
- Preferred confidentiality level (see Section 4.3 below)

4.3 Confidentiality Options
At the time of submission, indicate your preferred level of confidentiality:
Option 1- Fully Confidential (Default):

- Your identity is not disclosed to anyone except authorised Strategy India personnel.

- Identity may be shared with law enforcement only if legally compelled (court order, summons) or with your explicit consent.
- You will not be contacted by authorities unless you consent or the law requires it.

Option 2 – Identifiable to Authorities:

- Your identity and contact details are shared with law enforcement agencies investigating the reported scheme
- Authorities may contact you for witness statements, additional evidence, or clarification
- Identity remains protected from public disclosure and Alleged Fraudsters

Option 3 – Public (Not Recommended):

- You consent to your name being associated with the fraud report in public communications (rare; generally discouraged due to retaliation risk)
- Only select if you are comfortable with public identification (e.g., consumer advocate, media investigator with security measures)

Note: Strategy India generally defaults to Option 1 to maximise Reporter protection. Law enforcement agencies understand and respect the confidentiality of informants and whistleblowers.

5. ACCURACY AND FALSE REPORTING

5.1 Obligation of Truthfulness

You agree to provide information that is accurate, truthful, and complete to the best of your knowledge.

Mistakes versus Malice:

- Good-faith errors or inaccuracies due to incomplete information are understandable and do not constitute a breach.
- Knowingly false, fabricated, or maliciously misleading reports are strictly prohibited and may expose you to civil and criminal proceedings under the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and other applicable laws (including provisions on defamation and false accusations), in addition to any civil remedies available to Alleged Fraudsters for defamation or malicious prosecution.

5.2 Consequences of False Reporting

Submitting a knowingly false fraud report may result in:

Legal Liability:

- Defamation: Civil and criminal liability under applicable Indian law, including the Bharatiya Nyaya Sanhita, 2023 (in particular Section 356 on defamation), if false statements harm the reputation of Alleged Fraudsters.
- Criminal Penalties: Under the Whistleblower Protection Act, 2014, knowingly false complaints can result in a fine of up to ₹50,000 and/or imprisonment of up to 3 years
- Malicious Prosecution: If Alleged Fraudsters are wrongfully investigated/prosecuted based on your false report, you may face civil damages

System Access Termination:

- Strategy India may refuse future submissions from you
- Your identity may be disclosed to affected parties and law enforcement if false reporting is determined

No Liability for Strategy India:

- You indemnify and hold Strategy India harmless from any claims, damages, or legal actions arising from your false or defamatory reporting.

5.3 Verification and Due Diligence

Strategy India conducts its own due diligence and verification of Fraud Reports:

- We do not publish scam alerts or share with law enforcement based solely on a single, unverified submission.
- We cross-reference information, analyse compensation plans independently, and assess credibility.

- However, ultimate responsibility for the accuracy of the information you provide rests with you.

6. USE OF INFORMATION AND PUBLICATION

6.1 Law Enforcement Sharing
By submitting a Fraud Report, you authorise Strategy India to:

- Analyse the Report and supporting evidence.
- Share relevant information with law enforcement agencies (police, Economic Offences Wings, Enforcement Directorate, Central Bureau of Investigation, consumer protection authorities, regulators) as deemed appropriate for investigation and public protection.
- Coordinate with authorities on case developments, provide expert opinions, and testify as an expert witness if requested.

Limitations:

- We share only the information necessary and relevant to the investigation
- We request confidentiality protections for your identity (though ultimate control rests with authorities)
- We do not guarantee that authorities will investigate, prosecute, or take action

6.2 Public Alerts and Anonymisation
Strategy India may publish information about reported schemes in:

- Scam alert lists on www.strategyindia.com
- Case studies and research reports
- Media communications, blog posts, social media
- Training materials for law enforcement
- Policy submissions to the government

Anonymisation Commitment:

- Reporter identities are fully anonymised (no names, contact details, specific financial losses that could identify individuals)
- Victim information anonymised or aggregated (e.g., "dozens of victims lost amounts ranging from ₹50,000 to ₹5 lakh")
- Alleged Fraudster information may be published (including the names of promoters, companies, and websites) as necessary for public warning and accountability.

Purpose: Public alerts serve the public interest by preventing further victimisation and warning potential investors.

6.3 No Control Over Third-Party Use
Once published or shared with law enforcement:

- Information may be further disseminated (media coverage, court filings, regulatory reports)
- Strategy India cannot control how third parties use, quote, or republish information
- Alleged Fraudsters may attempt to identify sources (though we implement protections)

7. NO GUARANTEE OF OUTCOMES

7.1 Investigation and Enforcement
Strategy India does not guarantee that:

- Law enforcement will investigate your Fraud Report
- Alleged Fraudsters will be arrested, prosecuted, or convicted
- Fraudulent schemes will be shut down
- Court orders will be issued, or regulatory actions taken
- Assets will be seized or frozen

Reasons for Non-Investigation:

- Resource constraints of law enforcement agencies
- Jurisdictional issues (scheme operating from a foreign jurisdiction)

- Insufficient evidence for criminal prosecution
- Prioritisation of more severe or larger-scale frauds
- Legal technicalities or procedural hurdles

7.2 Financial Recovery
Strategy India does not guarantee and cannot assist with:
- Recovery of lost funds or investments
- Compensation from Alleged Fraudsters
- Refunds, settlements, or restitution

Recovery Avenues (Independent of Strategy India):
- Consumer Courts: File a complaint under the Consumer Protection Act, 2019
- Civil Litigation: File a civil suit for fraud, breach of contract, and unjust enrichment
- Criminal Proceedings: If prosecution is successful, the court may order restitution to victims (but no guarantee of recovery even if ordered)
- Insolvency Proceedings: If a fraudulent entity enters liquidation, creditors/victims may file claims (though recovery is often minimal)

7.3 Timing
Fraud investigations and prosecutions can take years. Strategy India cannot expedite law enforcement actions or court proceedings.

8. PROHIBITED CONDUCT

You agree not to:
Abuse the System:
- Submit spam, irrelevant, or trivial reports.
- Submit duplicate reports excessively (one submission per scheme is sufficient unless new evidence emerges)
- Use the System for purposes other than genuine fraud reporting (e.g., competitive sabotage, personal vendettas, harassment)

Violate Laws:

- Provide information obtained through illegal means (hacking, unauthorised computer access, theft, unlawful wiretapping, breach of computer systems).
- Violate privacy rights, defamation laws (including, where applicable, provisions on defamation under the Bharatiya Nyaya Sanhita, 2023), or intellectual property rights of third parties.
- Submit content that is obscene, pornographic, violent, or otherwise unlawful.

Misrepresent:
- Impersonate another person or entity.
- Falsely claim to represent a government agency, law enforcement, or regulatory body.
- Provide false contact information or fake identities (note: pseudonyms acceptable if contact method provided, but submission must be genuine)

Interfere:
- Attempt to gain unauthorised access to Strategy India's systems, databases, or confidential information.
- Introduce malware, viruses, or malicious code.
- Disrupt the System's operation or security.

9. INTELLECTUAL PROPERTY AND LICENCE

9.1 Your Content
You retain ownership of your Fraud Report and the evidence you submit. However, by submitting, you grant Strategy India a worldwide, non-exclusive, royalty-free, perpetual, irrevocable, sublicensable licence to:

- Use, reproduce, modify, adapt, publish, and distribute your Report and evidence for the purposes outlined in these Terms (fraud analysis, law enforcement sharing, public alerts, research, policy advocacy)
- Create derivative works (e.g., anonymised case studies, statistical reports) incorporating information from your Report.
- Sublicense to law enforcement agencies, legal advisors, and forensic experts as necessary for investigation and analysis

Rationale: This broad licence is necessary because fraud intelligence has long-term value, public alerts serve an ongoing purpose, and law enforcement coordination requires flexibility.

9.2 Strategy India's Content
All content on www.strategyindia.com and generated by Strategy India (analysis reports, scam alert lists, methodologies, trademarks) is the exclusive property of Strategy India and protected by copyright and intellectual property laws.

You may not:

- Reproduce, distribute, or commercially exploit Strategy India's fraud analysis, reports, or methodologies without written permission.
- Remove copyright, trademark, or proprietary notices.
- Use Strategy India's name, logo, or branding without authorisation.

Limited Use: You may share links to Strategy India's scam alerts and reference our public reports with proper attribution for non-commercial, informational purposes.

10. INDEMNIFICATION

You agree to indemnify, defend, and hold harmless Strategy India, its partners, employees, agents, and affiliates (collectively, "Indemnified Parties") from and against any claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees and litigation costs) arising from or related to:

i. Your Fraud Report: Claims by Alleged Fraudsters or third parties alleging defamation, false statements, privacy violations, or other harms based on information you provided
ii. Breach of These Terms: Your violation of any representation, warranty, or obligation herein (including false reporting, unlawful evidence collection, or misuse of the System)
iii. Third-Party Claims: Claims by other victims, informants, or parties affected by fraudulent schemes you reported, alleging that your report caused them harm (e.g., delayed recovery, reputational damage)
iv. Regulatory or Legal Actions: Fines, penalties, or sanctions imposed on Strategy India due to your provision of false, defamatory, or unlawfully obtained information
v. Malicious Prosecution and Related Claims: Without limiting the generality of the foregoing, you agree that the indemnity in this Section 10 covers any claims, notices, legal proceedings, or demands brought by Alleged Fraudsters or third parties alleging:
    - Defamation, loss of reputation, or commercial disparagement
    - Malicious prosecution, wrongful initiation of proceedings, or abuse of process
    - Any other civil or criminal liability said to arise from Strategy India's transmission of your report, your evidence, or Strategy India's public-interest communications that rely in whole or in part on your submissions.

Exception: Indemnification does not apply to claims arising solely from Strategy India's gross negligence, wilful misconduct, or breach of confidentiality obligations.
Defence Obligations:

- Strategy India will promptly notify you of claims subject to indemnification.
- You may assume control of defence (at your expense) with counsel reasonably acceptable to Strategy India.
- No settlement without Strategy India's prior written consent if it imposes obligations on or requires admission of liability by Strategy India.

11. LIMITATION OF LIABILITY

TO THE MAXIMUM EXTENT PERMITTED BY INDIAN LAW:

11.1 Disclaimer of Warranties

The System and all services are provided "AS IS" and "AS AVAILABLE" without warranties of any kind, express or implied, including:

- No guarantee of investigation, prosecution, or recovery (as stated in Section 7)
- No warranty of uninterrupted or error-free operation (System may experience downtime, technical issues, security incidents)
- No warranty of accuracy or completeness of Strategy India's fraud analysis or scam alerts (we rely on Reporter-provided information and our own research, but cannot guarantee absolute accuracy)
- No warranty of confidentiality (though we implement robust protections, no system is entirely immune to breaches)

11.2 Exclusion of Liability

Strategy India and Indemnified Parties shall not be liable for any direct, indirect, incidental, special, consequential, exemplary, or punitive damages arising from:

- Use of the System or submission of Fraud Reports
- Law enforcement actions or inactions (investigations, arrests, prosecutions, asset seizures, or lack thereof)
- Retaliation by Alleged Fraudsters against Reporters (though we take protective measures, we cannot guarantee Reporter safety)
- Data breaches or unauthorised access to Fraud Reports (despite security safeguards)
- Defamation or legal claims by Alleged Fraudsters against Reporters or Strategy India based on fraud reports
- Continued operation of fraudulent schemes despite reporting
- Loss of evidence, data corruption, or system failures
- Delays, errors, or omissions in analysis, reporting, or law enforcement coordination

Liability Cap: If, notwithstanding the foregoing, Strategy India is found liable, total aggregate liability shall not exceed ₹50,000 or the amount of any fees paid by you to Strategy India in connection with the System (which is typically ₹0, as the System is provided free of charge), whichever is lower.

11.3 Exceptions

The foregoing limitations do not apply to:

- Liability for gross negligence or wilful misconduct by Strategy India
- Fraud or fraudulent misrepresentation by Strategy India
- Liability that cannot be excluded under Indian law (e.g., specific data protection violations)

12. CONFIDENTIALITY OBLIGATIONS (MUTUAL)

12.1 Strategy India's Confidentiality Obligations

Strategy India agrees to:

- Maintain confidentiality of Reporter identities as outlined in the Privacy Policy and Section 4 of these Terms
- Implement security safeguards to protect Fraud Report data

- Limit access to authorised personnel on a need-to-know basis
- Not disclose Reporter identities publicly or to Alleged Fraudsters except as legally compelled or with Reporter consent

Duration: Confidentiality obligations survive indefinitely for Reporter identity information; five (5) years for other confidential information after case closure.

12.2 Reporter's Confidentiality Obligations
You agree to:

- Protect third-party privacy: Ensure that personal data of third parties (other victims, witnesses, non-involved individuals) included in evidence is necessary and relevant to fraud reporting; minimise exposure of unrelated personal details.
- Not disclose Strategy India's confidential information: If Strategy India shares confidential analysis, law enforcement coordination details, or operational information with you (e.g., case status updates), you agree not to disclose to third parties without consent.
- Respect law enforcement confidentiality: If authorities share sensitive investigative details with you, respect privacy and do not publicly disclose information that could compromise investigations

13. NO ATTORNEY–CLIENT OR FIDUCIARY RELATIONSHIP

Submitting a Fraud Report to Strategy India does not create:

- An attorney–client relationship (we are not your legal counsel; no legal privilege protects your communications)
- A fiduciary relationship (we do not owe fiduciary duties; our primary obligation is to the public interest in fraud prevention, not individual Reporter interests)
- An agency relationship (we do not act on your behalf in negotiations, litigation, or dealings with Alleged Fraudsters or authorities)

Legal Advice: Information provided by Strategy India (fraud analysis, guidance on reporting processes, and referrals to resources) is general in nature and not legal advice. Consult a licensed attorney for advice tailored to your situation.

14. FORCE MAJEURE

Strategy India is not liable for failure or delay in performing obligations under these Terms due to events beyond our reasonable control, including:

- Natural disasters, pandemics, and public health emergencies
- Government actions (lockdowns, internet shutdowns, emergency orders)
- Cyberattacks, data breaches by external actors (despite security measures)
- Labour strikes, civil unrest, terrorism, war
- Infrastructure failures (hosting provider outages, telecommunications disruptions)

Duration: Obligations suspended during a force majeure event; timelines extended by the period of delay. If the event continues for more than 90 days, either party may terminate the relationship (though existing Fraud Reports remain subject to Privacy Policy retention provisions).

15. DISPUTE RESOLUTION AND GOVERNING LAW

15.1 Governing Law
These Terms and any disputes arising from or related to your use of the System, submission of Fraud Reports, or relationship with Strategy India are governed by the laws of India, without regard to conflict of law principles.

15.2 Jurisdiction
Subject to the arbitration provisions below, the courts of Mumbai, Maharashtra, India, have exclusive jurisdiction over disputes.

15.3 Pre-Dispute Resolution
Before initiating formal proceedings, parties agree to:

Negotiation (15 days): Good-faith discussions between the Reporter and Strategy India senior management to resolve the dispute.

Mediation (optional, 30 days): If negotiation fails, parties may mutually agree to mediation under the rules of the Indian Council of Arbitration or other institution.

15.4 Arbitration
If informal resolution fails, disputes shall be resolved by binding arbitration under the Arbitration and Conciliation Act, 1996 (as amended):
Scope: All disputes except:

- Injunctive relief applications (may be sought from courts for urgency)
- Matters involving criminal conduct requiring judicial intervention

Nothing in this arbitration clause shall prevent Strategy India from approaching any court of competent jurisdiction for interim, conservatory, or injunctive relief, including to protect its confidential information, intellectual property, or reputation, pending the outcome of arbitration.

Arbitral Institution: Mumbai Centre for International Arbitration (MCIA); if no Agreement is reached within 15 days, MCIA.

Arbitrators: Single arbitrator for disputes involving claims less than ₹25 lakh; three arbitrators for higher-value disputes (each party appoints one, two party-appointed arbitrators appoint presiding arbitrator).
Seat: Mumbai, Maharashtra, India
Language: English

Confidentiality: Arbitration proceedings, submissions, and awards confidential (except as required for enforcement or by law).
Award: Final and binding; enforceable in any court of competent jurisdiction.
Costs: Each party bears its own costs unless the arbitrator allocates otherwise.
Class Action Waiver: All claims brought in individual capacity; no class, collective, or representative proceedings.

15.5 Limitation Period
Any claim arising from these Terms must be commenced within three (3) years from the date the cause of action accrues, or a shorter period as required under applicable limitation statutes.

16. GENERAL PROVISIONS

16.1 Entire Agreement
These Terms, together with the Privacy Policy, constitute the entire Agreement between you and Strategy India regarding the System and supersede all prior communications, proposals, or representations (oral or written).

16.2 Amendments
Strategy India may modify these Terms at any time:

- Updated "Last Updated" date at the top of Terms
- Material changes: prominent notice on "Report A Scam" page; email notification to Reporters with active contact information at least 14 days before the effective date (if feasible)
- Continued use after the effective date constitutes acceptance.

If you disagree with the modifications, cease using the System and contact us to withdraw your consent and request the deletion of your data (subject to legal retention exceptions).

16.3 Severability
If any provision is held invalid, illegal, or unenforceable, that provision shall be modified to the minimum extent necessary to make it enforceable, or severed if modification is not possible. The remaining provisions remain in full force.

16.4 Waiver
No waiver of any provision or breach constitutes waiver of any other provision or subsequent breach. Failure or delay in exercising any right or remedy does not constitute waiver.

16.5 Assignment
By Reporter: You may not assign or transfer these Terms or your obligations without Strategy India's prior written consent.
By Strategy India: Strategy India may assign these Terms or delegate performance to affiliates, successors, or assigns (including in connection with a merger, acquisition, or sale of assets), provided that confidentiality and data protection obligations remain binding on the assignee.

16.6 Survival
The following provisions survive termination or expiration of these Terms:

- Sections 5 (Accuracy and False Reporting), 6 (Use of Information and Publication), 9 (Intellectual Property and Licence), 10 (Indemnification), 11 (Limitation of Liability), 12 (Confidentiality Obligations), 13 (No Attorney–Client Relationship), 15 (Dispute Resolution and Governing Law), and 16 (General Provisions)

16.7 Notices
All notices under these Terms must be in writing and delivered to:
To Strategy India:
Level 17, Unit No. 1701–1704, Wing B & C
One BKC Centre, Plot No. C-66, G Block
Bandra Kurla Complex
Bandra East, Mumbai 400051
India
Email: info@strategyindia.com

Attention: Grievance Officer
To Reporter:
Email address provided in Fraud Report or contact information on file
Notices effective upon: email delivery confirmation or 24 hours after sending (whichever is earlier); courier signed receipt; registered post 5 business days after posting.

16.8 Language
These Terms are prepared in English. Any translation is for convenience only. In the event of conflict, the English version prevails.

16.9 Electronic Acceptance
You agree that your electronic submission of a Fraud Report (via email, web form, or other method) constitutes a binding legal obligation equivalent to a manual signature, pursuant to Section 10A of the Information Technology Act, 2000, and will be treated in accordance with applicable Indian evidence law on electronic records.

FORM-ADJACENT NOTICES

NOTICE 1: CRITICAL RISK WARNINGS

Before submitting this fraud report, you must understand and accept the following risks:
Legal Risks:

- Alleged fraudsters may sue you for defamation, even if your report is truthful.
- You may be required to testify in court proceedings and be cross-examined
- Legal defence can be costly; Strategy India does not fund it.

Retaliation Risks:

- Fraudsters may attempt to identify you despite confidentiality measures
- You may face harassment, threats, or intimidation
- Strategy India provides procedural protections, but cannot guarantee physical safety

Evidence Risks:

- Evidence obtained unlawfully (hacking, theft, unauthorised recording) exposes you to criminal liability
- You are responsible for the lawful collection of all materials submitted
- Intellectual property infringement in evidence may result in separate legal claims against you

No Guarantees:

- Reporting does not guarantee investigation, prosecution, or recovery of losses
- Law enforcement may decline to act, or investigations may conclude without charges
- You may remain involved in lengthy processes (investigations, trials) for years

Indemnification:

- You agree to defend and indemnify Strategy India from claims arising from your report
- If we are sued due to information you provided, you bear responsibility and costs
- This includes claims for defamation, privacy violations, unlawfully obtained evidence, or false reporting

Professional Advice Recommended:

- Consult a qualified attorney before submitting if you have concerns about legal exposure
- Consider reporting directly to the police or consumer protection authorities if you prefer government channels

NOTICE 2: EVIDENCE LEGALITY CERTIFICATION

By submitting evidence, you certify under penalty of perjury that:

i. All documents, recordings, screenshots, and materials were obtained lawfully
ii. No evidence was obtained through hacking, unauthorised computer access, theft, burglary, trespass, unlawful wiretapping, or breach of confidentiality agreements
iii. You have the legal right to disclose the information and evidence provided
iv. To the best of your knowledge, your submission violates no intellectual property rights (copyrights, trademarks, trade secrets), or such use qualifies as fair dealing/fair use for fraud reporting purposes.
v. You understand that unlawful evidence collection may expose you to civil and criminal liability under the Information Technology Act, 2000 (including provisions on unauthorised access and data breaches), the Bharatiya Nyaya Sanhita, 2023 (including offences

corresponding to theft and criminal trespass), the Telegraph Act, 1885 (unlawful interception), and other applicable laws.

vi. You agree to indemnify Strategy India from any claims arising from unlawfully obtained evidence you submitted

False Certification: Providing false certification may result in criminal prosecution and civil liability.

NOTICE 3: CONSENT AND ACKNOWLEDGEMENT

By submitting this fraud report, you confirm that you have read, understood, and agree to Strategy India's Privacy Policy and Terms of Use for the fraud reporting system.
You consent to Strategy India:

- Processing the information you provide to analyse suspected fraud
- Sharing relevant details with law enforcement agencies for investigation
- Publishing anonymised public alerts to warn others about the reported scheme
- Retaining your report as outlined in the Privacy Policy

You understand that:

- Your identity will be kept confidential unless legally compelled or with your explicit consent.
- Strategy India is not a law enforcement agency and cannot guarantee investigation, prosecution, or recovery of lost funds.
- Information you provide must be accurate and obtained lawfully.
- No attorney–client privilege or fiduciary relationship is created.

By clicking "Submit," you provide your free, specific, informed, and unconditional consent under the Digital Personal Data Protection Act, 2023.

NOTICE 4: FALSE REPORTING WARNING

WARNING: FALSE REPORTING

Knowingly submitting false, fabricated, or maliciously misleading fraud reports may result in:

- Defamation: Civil and criminal liability under applicable Indian law, including the Bharatiya Nyaya Sanhita, 2023 (in particular Section 356 on defamation), if false statements harm the reputation of Alleged Fraudsters.
- False accusations and bad-faith complaints: Criminal penalties may apply under applicable law, including, where relevant, the Whistleblower Protection Act, 2014, and may include fines of up to ₹50,000 and/or imprisonment of up to 3 years.
- Malicious prosecution: If Alleged Fraudsters are wrongfully investigated or prosecuted based on your knowingly false report, you may face civil damages under applicable law and common law principles.
- Termination of your ability to submit future reports
- Disclosure of your identity to affected parties and law enforcement

Only submit reports you genuinely believe, in good faith, involve fraudulent activity.

NOTICE 5: EVIDENCE AND THIRD-PARTY PRIVACY

EVIDENCE HANDLING

Ensure that all evidence (documents, screenshots, recordings) you submit was obtained lawfully and does not violate the privacy rights or confidentiality obligations owed to third parties.

You are responsible for:

- Lawful collection of materials (no hacking, theft, unauthorised access)
- Minimising the exposure of personal data of uninvolved individuals
- Accuracy of documents and representations

Strategy India is not liable for any unlawful collection of evidence or for any privacy violations.

This Privacy Policy and Terms of Use are effective as of 10 October 2025 and were last updated on 20 November 2025.

For questions or concerns, contact the Grievance Officer at info@strategyindia.com or +91-22-40238899.