Digital Fraud Prevention Policy

Internal
V1.0 Updated 23/12/25

1. Purpose

Establish guidelines, procedures, and responsibilities for preventing, detecting, investigating, and responding to digital fraud within TLC Digitech Pvt Ltd (hereinafter referred to as "the Company"). Digital fraud poses significant risks to financial stability, reputation, and data security. This policy aims to foster a culture of vigilance and integrity to mitigate these threats.

2. Scope

This policy applies to:

- All employees
- All devices and communication channels capable of receiving telephone / video calls or voice messages on behalf of the Company

3. Types of Digital Fraud

Fraud Type	Description	Typical Goals
Digital Arrest Scam	Fraudsters impersonate law enforcement officials (e.g., CBI, ED, Police, Customs, TRAI) via video/audio calls, claiming the victim is involved in a serious crime (money laundering, parcel with drugs, etc.). Victims are threatened with immediate arrest and kept on continuous calls ("digital arrest") while coerced into transferring money, revealing banking details, or granting remote access.	Extort large sums of money, steal banking credentials, drain accounts, or install remote-access malware.
Identity Theft	Stealing and misusing personal identifiable information (e.g., Aadhaar, PAN, passport, bank details, login credentials, biometric data) to impersonate legitimate individuals.	Open fraudulent accounts, obtain credit/loans, bypass KYC, commit tax fraud, or access victim services.
Phishing / Smishing / Vishing	Fraudulent emails, SMS/WhatsApp messages, or voice calls that trick users into revealing credentials, OTPs, clicking	Steal login credentials, OTPs, session tokens, or infect

Fraud Type	Description	Typical Goals
	malicious links, or installing malware. (Digital Arrest scams often begin with vishing and escalate to video calls.)	devices with malware for further compromise.
Synthetic & Fake Accounts	Creating accounts using entirely fabricated, stolen, or AI-generated identities (fake names, documents, selfies, liveness videos).	Abuse referral/promotional programs, money laundering, KYC bypass, bonus hunting, or platform manipulation.
Account Takeover (ATO)	Gaining unauthorized control of legitimate user or employee accounts through credential stuffing, phishing, session hijacking, SIM swapping, or social engineering.	Perform fraudulent transactions, steal funds/rewards, extract personal data, or damage reputation.
Data Manipulation & Digital Forgery	Altering digital transactions, forging documents, e-signatures, screenshots, or system records using editing tools or deepfake technology.	Approve fake loans, modify transaction amounts, falsify KYC documents, or divert payments.
Payment & UPI/Card Fraud	Unauthorized transactions using stolen card details, UPI IDs, remote-access apps (AnyDesk, TeamViewer), QR code manipulation, or payment gateway exploits.	Direct money transfers, purchase goods/services, or launder money.
Social Engineering & Impersonation	Psychological manipulation of employees, customers, or vendors using urgency, authority, fear, or trust to bypass security controls.	Gain access to systems, approve fraudulent requests, disclose credentials, or transfer funds.
Refund & Chargeback Abuse	Filing false refund/return claims, claiming non-delivery, colluding with merchants, or exploiting chargeback processes.	Obtain free goods/services or recover money after receiving products (friendly fraud).

Fraud Type	Description	Typical Goals
Platform & API Abuse	Bot-driven attacks, credential testing, scraping, excessive API calls, rate-limit bypass, or exploitation of logic vulnerabilities.	Mass account creation, inventory hoarding, price scraping, denial-of-inventory, or service disruption.

4. Policy Statement

All personnel are expected to:

- Conduct business with honesty and integrity in all digital interactions.
- Protect confidential data and digital assets from unauthorized access or misuse.
- Report any suspected digital fraud immediately without fear of retaliation.

5. Prevention Measures

5.1 Device and Network Security

- All devices (company-issued or personal) used for Company access must be password-protected with strong, unique passwords (at least 8 characters, including uppercase/lowercase letters, numbers, and symbols).
- Install and regularly update antivirus/anti-malware software, firewalls, and security patches.
- Access Company systems only through secure, private networks; avoid public Wi-Fi for sensitive activities.
- Enable disk encryption and use password management tools provided by the Company.
- Lock devices when unattended and report lost or stolen devices immediately to IT.

5.2 Email and Communication Safety

- Be cautious with emails: Do not open attachments or click links from unknown or suspicious sources.
- Verify sender legitimacy by checking email addresses, grammar, and content for inconsistencies (e.g. urgent requests for sensitive information).

- Avoid responding to phishing attempts

5.3 Password and Access Management

- Change passwords every three months and last 3 passwords cannot be same across accounts.
- Use multi-factor authentication (MFA) wherever available.
- Share credentials only when necessary and through secure channels

5.4 Data Transfer and Handling

- Transfer confidential data only over secure networks and to authorized recipients.
- Encrypt sensitive files before sharing and verify recipient security protocols.
- Refrain from downloading unauthorized software or accessing suspicious websites.

5.5 Controls

- Mandatory multi-factor authentication (MFA) with hardware keys or authenticator apps (SMS-based OTP prohibited for high-risk actions).
- Device binding and trusted-device management for all customer and employee logins.
- Real-time transaction and behaviour monitoring using UEBA (User and Entity Behavior Analytics).
- Regular red-team exercises and phishing simulations.

5.6 Preventive Controls by Fraud Type

Fraud Type	**Key Preventive Controls**
Digital Arrest Scam	Company-wide awareness campaigns. Immediate escalation protocol: any employee or customer receiving such a call must disconnect and report instantly. - Block known scam numbers and domains at gateway level. “Safe-word” or out-of-band verification process for any urgent law-enforcement-related communication claiming to involve the Company.
Identity Theft	Liveness detection, biometric deduplication, Aadhaar/PAN masking, OCR + human review for high-value actions.

Fraud Type	Key Preventive Controls
Phishing / Smishing / Vishing	Email/SMS domain whitelisting, link scanning sandbox, anti-spoofing (DMARC, SPF, DKIM), employee awareness drills.
Synthetic & Fake Accounts	AI-powered document verification, selfie-liveness checks, cross-database identity linkage, velocity checks on sign-ups.
Account Takeover (ATO)	Session binding, anomaly detection (impossible travel, new device fingerprint), automatic logout on suspicious behaviour.
Data Manipulation & Digital Forgery	End-to-end encryption, digital signature validation (Aadhaar e-Sign, DSC), tamper-evident audit logs, screenshot detection.
Payment & UPI/Card Fraud	Virtual card numbers, transaction limits, remote-access app blocking on company devices.
Social Engineering & Impersonation	Out-of-band confirmation for high-risk actions, “no urgency” policy, executive impersonation alerts.
Refund & Chargeback Abuse	Refund only to original payment method, delivery proof requirements, chargeback representment team.
Platform & API Abuse	CAPTCHA/bot detection (reCAPTCHA Enterprise), rate limiting, API key rotation, behavioural bot management.

6. **Detection of Digital Fraud**

The Company will monitor for red flags indicative of digital fraud or identity theft. Relevant red flags, adapted from regulatory guidelines, include:

Category	Examples
Alerts from Credit Agencies	Fraud alerts, credit freezes, address discrepancies, or unusual inquiry patterns.
Suspicious Documents	Forged IDs, altered applications, or inconsistencies between presented info and records.

Category	Examples
Suspicious Personal Information	Invalid SSNs, mismatched addresses, or use of deceased individuals' data.
Suspicious Account Activity	Sudden changes in activity (e.g., address updates followed by large transactions), returned mail, or unauthorized charges.
Notices from Other Sources	Reports from customers, law enforcement, or data breach notifications.

In addition to the above, the Fraud Detection team shall actively monitor for the following indicators specific to the fraud types:

- Sudden spike in accounts registered from the same IP/range or device fingerprint.
- Multiple failed login attempts followed by successful login from a new location (credential stuffing).
- OTP requests without corresponding login attempt.
- Use of known phishing kits or malicious URLs/domains.
- Mismatched geolocation between account registration, KYC, and transactions.
- High-velocity refund or cashback claims from newly created accounts.

8. **Instructions to Follow**

- **Do not stay on the call** – politely disconnect immediately.
- **Do not transfer money, share OTPs, bank details, or allow remote access** under any circumstances.
- Forward any suspicious call recordings, screenshots, or video call details to **techescalations@tlcgroup.com** immediately.

9. Training and Awareness

- All new hires will receive training during onboarding.
- Annual refresher training will cover fraud recognition, prevention best practices, and reporting procedures.

- Specialized training for high-risk roles (e.g., IT, finance) will include simulations of phishing attacks and red flag scenarios.
- Modules on **Digital Arrest / Courier Scam / Law Enforcement Impersonation/ UPI, Refund and chargeback fraud trends**. Real-life case studies and red-flag audio/video clips shared during training sessions.
- Recognition of synthetic identity and forged document red flags.
- Social engineering scenarios involving impersonation of Chairman / Leadership Team, law enforcement, or bank officials.
