



Public Transport Mobile Ticketing & Contactless Payment Security Audit 2026 Checklist

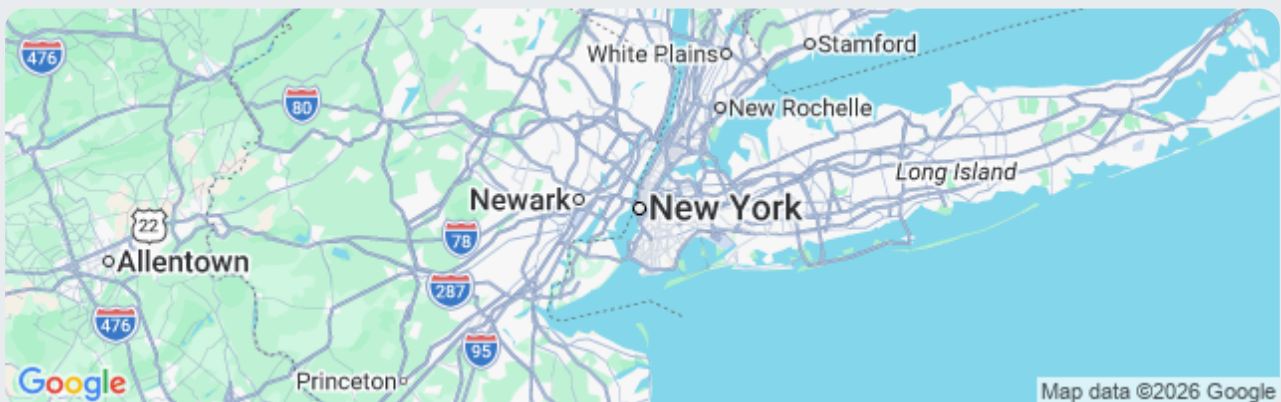
Hardware Integrity & Physical Security

Inspection of physical ticket vending machines (TVMs), card readers, and NFC terminals for tampering, hardware vulnerabilities, or unauthorized physical modifications.

Inspection Date

Terminal or Station ID

 [Set My Current Location](#)



Physical Tamper Seal Intact?

- ☐ Yes
- ☐ No
- ☐ N/A

Observed Physical Anomalies

- ☐ Broken Security Seals
- ☐ Unauthorized USB/Hardware Access
- ☐ Screen Damage/Tampering
- ☐ Loose Wiring/External Cables
- ☐ Skimming Device Detected

Detailed Description of Findings

Write something...

Evidence Photo (Tamper Evidence)

 Upload File

Inspector Verification

Encryption & Data Transmission Security

Verification of end-to-end encryption protocols (TLS/SSL), secure communication between readers and backend servers, and the integrity of wireless signal transmission.

Encryption Protocol Version

- ☐ TLS 1.2
- ☐ TLS 1.3
- ☐ AES-256
- ☐ Other/Legacy

Verified Secure Transmission Channels

- ☐ HTTPS/TLS
- ☐ Secure VPN Tunnel
- ☐ Encrypted Bluetooth (BLE)
- ☐ Secure NFC Protocol

Certificate Authority & Expiry Audit Notes

Write something...

Encryption Key Management Certificate Upload

 Upload File

Last Security Certificate Renewal Date

Enter date...

Bit Strength of Current Encryption Keys

Enter a number...

Software & Application Vulnerability Assessment

Audit of mobile app security patches, operating system compatibility, API security, and protection against unauthorized rooting or jailbreaking on passenger devices.

Mobile App Version Audit

- ☐ Current Version (Verified)
- ☐ Outdated Version (Action Required)
- ☐ Critical Vulnerability Detected

Security Protocols Verified

- ☐ API Authentication Check
- ☐ End-to-End Encryption (E2EE)
- ☐ Code Obfuscation Enabled
- ☐ SSL/TLS Certificate Validity
- ☐ Input Validation (SQLi/XSS Protection)

Identified Software Vulnerabilities

Write something...

Security Penetration Test Report

 Upload File

Last Security Patch Deployment Date

Enter date...

Lead Security Auditor Approval

Payment Gateway & Transaction Processing

Review of payment processor compliance, PCI-DSS standards adherence, transaction log accuracy, and the security of the settlement process between banks and transit authorities.

Audit Date

Enter date...

PCI-DSS Compliance Status

- ☐ Fully Compliant
- ☐ Partially Compliant
- ☐ Non-Compliant
- ☐ Under Review

Number of Failed Transactions Detected (Last 24h)

Enter a number...

Encryption Protocol Verification Details

Write something...

Payment Methods Tested

- ☐ Contactless Credit/Debit Card
- ☐ Mobile Wallet (Apple/Google Pay)
- ☐ Stored Value Transit Card
- ☐ QR Code Scanned Ticket

Transaction Log Sample Evidence

 Upload File

Auditor Authorization Signature

User Authentication & Access Control

Evaluation of passenger account login security, multi-factor authentication (MFA) for admin portals, and management of digital wallet/tokenization security.

Authentication Method Audited

- ☐ Biometric Authentication
- ☐ Multi-Factor Authentication (MFA)
- ☐ Password/PIN Entry
- ☐ Tokenized Digital Wallet

Verified Access Control Measures

- ☐ Role-Based Access Control (RBAC) Implementation
- ☐ Session Timeout Enforcement
- ☐ Device Fingerprinting
- ☐ Secure API Key Management

Admin Portal Access Review Notes

Write something...

Last Access Audit Completion Date

Enter date...

Evidence of Credential Encryption Audit

 Upload File

Auditor Verification Signature

Data Privacy & PII Protection

Assessment of Personally Identifiable Information (PII) handling, data anonymization during journey tracking, and compliance with 2026 global data protection regulations.

Data Compliance Framework Applied

☐ GDPR

☐ CCPA/CPRA

☐ Local/Regional Transit Regulation

☐ Other

Types of PII Collected

☐ Full Name

☐ Credit/Debit Card Details

☐ GPS/Location Data

☐ Email Address

☐ Device Identifiers

Data Anonymization Methodology

Write something...

Last Data Privacy Impact Assessment (DPIA) Date

Enter date...

Upload Privacy Policy Audit Report

 Upload File

Data Protection Officer (DPO) Verification

System Resilience & Offline Functionality

Testing of transaction processing during network outages, failover mechanisms, and the security of cached transaction data during connectivity drops.

Offline Transaction Mode Status

- ☐ Fully Operational
- ☐ Degraded Mode (Limited Offline Capability)
- ☐ System Failure (No Offline Processing)

Maximum Offline Transaction Limit

Enter a number...

Tested Offline Redundancy Features

- ☐ Local Data Caching
- ☐ Automatic Re-sync on Reconnection
- ☐ Battery Backup for Terminal Operation
- ☐ Secondary Communication Channel (e.g., 5G Failover)

Offline Sync Error Logs Summary

Write something...

System Stress Test Report

 Upload File

Last Successful Synchronization Date

Enter date...

Fraud Detection & Incident Response

Verification of real-time anomaly detection for fraudulent ticket usage, automated alerting for suspicious transaction patterns, and the efficiency of the security incident recovery plan.

Fraud Pattern Detected

- ☐ Duplicate Token/Card Usage
- ☐ Unusual Transaction Velocity
- ☐ Unauthorized API Access Attempt
- ☐ Physical Tampering Alert
- ☐ None Detected

Fraud Incident Description

Write something...

Incident Detection Date

Enter date...

Estimated Financial Impact

Enter a number...

Supporting Evidence/Logs

 Upload File

Security Auditor Verification

< Previous

> Next

👍 Finish

 Generate Sample Report