Coordinated Privacy Disclosure, Final Report

Etihad Airways Android (com.mttnow.android.etihad)

Mobile Travel Technologies Ltd, developed with Ernst & Young, Abu Dhabi, UAE

SILENT · CASE CLOSED AND PUBLISHED ON THE STATED EMBARGO DATE, 25 SEPTEMBER 2026, SEVEN MESSAGES, ONE BOUNCE, ZERO REPLY OF ANY KIND

Target	Etihad Airways, the Android booking app for the UAE flag carrier
Package	com.mttnow.android.etihad, version 9.5.9
Operator	Mobile Travel Technologies Ltd (MTT), developed in partnership with Ernst & Young
Initial Disclosure	2026-06-27
Stated Embargo	2026-09-25, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, on the stated date
Regulators	Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	7, across 71 days: the first two addresses, security@etihad.ae and privacy@etihad.ae, either bounced or reported a full mailbox; dpo@etihad.ae, privacy@etihad.com, and dataprivacy@etihad.ae accepted the remaining messages.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Mobile Travel Technologies Ltd, the developer of the Etihad Airways Android app built in partnership with Ernst & Young, that the production binary embeds com.cyberfend.cyfsecurity, a Chinese-origin mobile security SDK, 46 compiled classes plus a native library, including a WebView monitoring service active in the same flow where passengers enter passport numbers and payment card details. China's National Intelligence Law Art. 7 obliges any Chinese organisation to cooperate with state intelligence work on request, and this practice is not disclosed anywhere in Etihad's privacy policy. This is the fourth consecutive travel-sector app in this audit series found to embed CyberfEnd, following trivago, the Amadeus-branded Merci client, and Air Canada.

A second finding names Quantum Metric, a US-based session-recording platform present as 621 compiled classes, active in the same booking and passport-entry flow. Session replay captures form-field interaction directly, meaning passport numbers, dates of birth, frequent-flyer credentials, and payment card details are all recorded and transmitted to US infrastructure as a matter of course, with Quantum Metric named nowhere as a data recipient in the app's privacy policy.

Five further findings cover the practical mechanics of a booking flow with weaker safeguards than its own subject matter warrants: Adobe Experience Platform Launch loads arbitrary tracking JavaScript from a CDN at runtime, meaning the actual tracking stack deployed to any given user session cannot be established from the binary alone; dual pre-consent SDK initialization starts Firebase Analytics before any consent screen, alongside a hardcoded Firebase API key and database URL; the UAE, where Etihad is incorporated, has no EU Commission adequacy decision, and the same binary additionally routes data to US infrastructure via Adobe Marketing Cloud; a development tunneling domain, localhost.run, is permitted cleartext traffic in the production network security configuration, indicating a development setting shipped unchanged; and the app requests READ_CALENDAR access to a user's entire device calendar with no documented feature requiring it, beyond the documented WRITE_CALENDAR use for saving bookings.

Seven messages were sent across 71 days. The first attempt, to security@etihad.ae, reported a permanently full mailbox; privacy@etihad.ae also failed outright. dpo@etihad.ae, privacy@etihad.com, and dataprivacy@etihad.ae accepted delivery for the remaining messages, cc'ing the Austrian DSB, Germany's BfDI, and CERT.at throughout. Not one reply, automated or human, was ever received on any address at any point. The embargo, stated directly to the target as 25 September 2026 in the original disclosure, elapses today. This report and the accompanying closure notice publish on that date.

Scope: Root-level static analysis of the production Etihad Airways Android application (com.mttnow.android.etihad, version 9.5.9), pulled from Google Play and reviewed on 27 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Etihad's, CyberfEnd's, Quantum Metric's, or Adobe's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Two correct to HIGH on their own computed bands: the CyberfEnd (CN) SDK's WebView monitoring capability active in the passport and payment entry flow, and Quantum Metric's session recording of the same passport, date-of-birth, frequent-flyer, and payment fields. Adobe Experience Platform Launch's runtime dynamic tag loading, dual pre-consent SDK initialization with a hardcoded Firebase key, and the UAE-to-US data transfer without an EU adequacy decision all correct to MEDIUM. A development tunnel domain left active in the production network security configuration corrects to MEDIUM. Undocumented calendar read access corrects to LOW. Seven messages were sent across 71 days, one address bouncing outright and one reporting a permanently full mailbox before three other addresses accepted delivery. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	A Chinese Security SDK Monitors the WebView Rendering Passport and Payment Entry
C2	HIGH	Quantum Metric Session Recording Captures Passport, Payment, and Frequent-Flyer Fields
C3	MEDIUM	Adobe Launch Loads Arbitrary Tracking JavaScript From a CDN at Runtime
C4	MEDIUM	Pre-Consent Firebase Initialization With a Hardcoded API Key
H1	MEDIUM	UAE and US Data Transfers With No EU Adequacy Decision
H2	MEDIUM	A Development Tunnel Domain Is Permitted Cleartext Traffic in Production
H3	LOW	Undocumented Full-Calendar Read Access

Subject & Operator Analysis

Etihad Airways is the flag carrier of the United Arab Emirates. The Android app is built by Mobile Travel Technologies Ltd (MTT) in partnership with Ernst & Young, confirmed by the compiled com.ey.* package structure present throughout the binary. A split_config.de.apk German-language locale package confirms EU residents are a targeted demographic, placing the app within GDPR Art. 3(2) scope.

Several genuine positives are worth naming. allowBackup is correctly set to false. The base network security configuration does not permit cleartext globally, only the single localhost.run exception noted above. PairIP app protection is implemented. The app has clearly had real security investment, the compliance layer around data flows and consent has not kept pace with the technical infrastructure.

Seven Messages, One Bounce, One Full Mailbox, Zero Reply

This case's correspondence record involved two address failures before a working channel was found. The first attempt, to security@etihad.ae, reported a permanently full mailbox on 27 June 2026 and remained unusable for the rest of the case. privacy@etihad.ae bounced outright on the same day. dpo@etihad.ae, privacy@etihad.com, and dataprivacy@etihad.ae accepted delivery for the remaining messages across the following 71 days, cc'ing the Austrian DSB, Germany's BfDI, and CERT.at throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: A Chinese Security SDK Monitors the WebView Rendering Passport and Payment Entry

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

com.cyberfend.cyfsecurity (CyberfEnd) is embedded as 46 compiled smali classes plus a native library, libcyfsecurity.so, including CYFWebViewService, a WebView monitoring service, and CCADialogActivity. WebView monitoring is active in the flow that renders passport verification and payment entry screens. CyberfEnd is a Chinese mobile security company; under China's National Intelligence Law Art. 7, any Chinese organisation must cooperate with state intelligence work on request. This is the fourth consecutive travel-sector app in this audit series found to embed the same SDK, after trivago, the Amadeus-branded Merci client, and Air Canada.

```
com.cyberfend.cyfsecurity.CYFWebViewService
com.cyberfend.cyfsecurity.CCADialogActivity
libcyfsecurity.so (native library), 46 compiled classes total
```

Impact: EU passengers entering passport numbers and payment card details in the booking flow have their session rendered inside a WebView actively monitored by a Chinese-origin security SDK, undisclosed in Etihad's privacy policy, with no informed consent obtained for that specific processing.

Fix: Remove CyberfEnd or restrict its monitoring scope away from the passport and payment entry views, and disclose the SDK and its origin in the privacy policy. No confirmation that this has occurred was ever received.

C2: Quantum Metric Session Recording Captures Passport, Payment, and Frequent-Flyer Fields

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7.

621 compiled Quantum Metric classes are present, active in the booking and passport-entry flow. Session recording captures passport number entry, date-of-birth input, frequent-flyer account credentials, and payment card details, transmitting this interaction data to US infrastructure. Quantum Metric is not named as a data recipient anywhere in Etihad's privacy policy.

```
com.quantummetric.* (621 compiled classes), session replay active in booking/passport
    flow
```

Impact: Travel-document and payment-card data entered by EU passengers is captured at the field level by a session-recording platform and sent to US infrastructure, with no technical safeguard preventing the capture of this data class and no disclosure of the recipient in the privacy policy.

Fix: Mask or exclude passport, date-of-birth, frequent-flyer, and payment fields from Quantum Metric session capture, and name the recipient in the privacy policy. No confirmation that this has occurred was ever received.

C3: Adobe Launch Loads Arbitrary Tracking JavaScript From a CDN at Runtime

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9.

A hardcoded Adobe Experience Platform Launch script URL is present in global_config_prod.json. Adobe Launch is a tag management system that loads arbitrary third-party tracking scripts from Adobe's CDN at runtime, meaning any tag configured in the associated Adobe property executes inside the app without being visible in the binary itself. The production APK additionally bundles a staging configuration exposing an internal infrastructure identifier.

```
adobeLaunchScript: https://assets.adobedtm.com/8aea536f4a27/6442c4906d25/launch-
    de32e47b5ddd.min.js
Staging identifier present in production build: etihad-adobe-aem-hosting
```

Impact: The tracking stack actually deployed to any given user session cannot be established from static analysis of the binary, since tags can be added or changed at any time through Adobe's console without an app update, which makes consent auditability structurally impossible from the outside.

Fix: Pin or version-lock the Adobe Launch configuration, remove the staging identifier from the production build, and document the current tag inventory for auditability. No confirmation that this has occurred was ever received.

C4: Pre-Consent Firebase Initialization With a Hardcoded API Key

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9.

AppOverridesInitProvider and FirebaseInitProvider both fire at app launch, initOrder=100, before any consent UI, with FirebaseInitProvider additionally directBootAware. Firebase Analytics begins collecting behavioural data before any consent dialog. A Firebase API key and Realtime Database URL are hardcoded in res/values/strings.xml.

```
google_api_key: AIzaSyCk0ot828CBgPCdVEaulyxQ9gSeMTvBbSA
firebase_database_url: https://etihad-oneapp.firebaseio.com
project_id: etihad-oneapp
```

Impact: Behavioural tracking begins before consent, and unauthenticated calls against the hardcoded key can exhaust project quotas, a real availability risk for a service passengers depend on for live bookings.

Fix: Defer Firebase initialization until after consent, and restrict the API key by package name and certificate fingerprint. No confirmation that this has occurred was ever received.

H1: UAE and US Data Transfers With No EU Adequacy Decision

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

Etihad Airways is incorporated in Abu Dhabi, UAE, for which the European Commission has issued no adequacy decision under GDPR Art. 45. The same binary embeds Adobe Marketing Cloud (1204 compiled classes), additionally routing EU user data to US infrastructure. No Art. 46 transfer mechanism is documented to users at the point of data collection.

Impact: EU passenger data reaches two jurisdictions with no adequacy decision, UAE and, via Adobe, the US, with no disclosed Art. 46 safeguard for either transfer.

Fix: Document the specific Art. 46 transfer mechanism relied on for both jurisdictions in the privacy policy. No confirmation that this has occurred was ever received.

H2: A Development Tunnel Domain Is Permitted Cleartext Traffic in Production

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3.

The production network security configuration permits cleartext traffic to localhost.run and all its subdomains, a public development-tunneling service. Its presence in a production APK distributed to millions of passengers indicates a development configuration was shipped unchanged. Any *.localhost.run subdomain receives unencrypted traffic from the app.

Impact: The base network security configuration otherwise blocks cleartext traffic, and this single exception is the kind of residual development artefact that, if a *.localhost.run subdomain is registered by an unrelated party, becomes a live cleartext-interception path against the production app.

Fix: Remove the localhost.run cleartext exception from the production network security configuration. No confirmation that this has occurred was ever received.

H3: Undocumented Full-Calendar Read Access

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

The app requests both READ_CALENDAR and WRITE_CALENDAR. Writing flight bookings to the calendar is a documented feature. Reading the calendar grants access to every event across every account on the device, personal appointments, medical entries, business meetings included, with no documented feature or data-minimisation assessment covering that read access.

Impact: Full-device calendar read access is present with no corresponding disclosed feature beyond the one-directional write already used for bookings.

Fix: Remove READ_CALENDAR unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

Article	Finding	Basis

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 9, 13(1)(e), 44–46	C1	Chinese-origin SDK with WebView monitoring active in passport and payment entry, undisclosed.
Art. 13(1)(e), 32	C2	Undisclosed session recording of passport, payment, and frequent-flyer fields to US infrastructure.
Art. 5(1)(a), 13, 32	C3	Runtime-loaded third-party tracking JavaScript breaking consent auditability.
Art. 7, 32	C4	Pre-consent behavioural tracking and a hard-coded, unrestricted API key.
Art. 45–46, 13(1)(f)	H1	UAE and US data transfers with no documented Art. 46 mechanism.
Art. 32	H2	Development tunnel domain permitted cleartext in production.
Art. 5(1)(c), 13	H3	Undocumented full-device calendar read access.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1 and C2 correct to HIGH on their own computed bands, matching the same CyberfEnd finding's computed band in the trivago, Amadeus Merci, and Air Canada reports; C3, C4, and H1–H2 correct to MEDIUM; H3 corrects to LOW. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: ETIHAD-2026-R1.