# Coordinated Privacy Disclosure, Final Report

## Air Canada Android (com.aircanada.mobile)

Air Canada, Montreal, Canada (TSX: AC)

**REPEATED BOUNCES, ONE WORKING ADDRESS FOUND LATE, ZERO REPLY OF ANY KIND · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE**

| | |
|---|---|
| **Target** | Air Canada, an airline booking, check-in, and boarding Android app |
| **Package** | com.aircanada.mobile |
| **Operator** | Air Canada, Montreal, Canada (TSX: AC) |
| **Initial Disclosure** | 2026-06-27 |
| **Original Embargo** | 2026-09-25 (90 days from disclosure, as stated in the original notice) |
| **Report Published** | 2026-09-25, on the original embargo date |
| **Regulators** | Austrian DSB, CNIL (France, EU passenger data), German BfDI, CERT.at |
| **Total Outbound Messages** | 4, across 77 days: an initial attempt to privacy@aircanada.com , security@aircanada.com, and dpo@aircanada.com bounced repeatedly across ten separate delivery-failure notifications through 30 June and again through 20 July 2026; a working address, privacy_vieprivee@aircanada.ca, was located and used for the final two 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 Air Canada that its Android app implements JMRTD (166 classes) with APDULevelEACTACapable, Extended Access Control Terminal Authentication, the specific ICAO 9303 protocol required exclusively to access Data Group 3 (ten-print fingerprints) and Data Group 4 (iris scans) from EU biometric passport chips. Basic Access Control and Password Authenticated Connection Establishment, the mechanisms most travel apps use, only reach Data Groups 1 and 2, name and document data; EAC-TA goes further, and its presence indicates the app is built to extract biometric data beyond standard passport reading. A supporting stack, BouncyCastle post-quantum cryptography, EJBCA certificate management, and a JPEG2000 decoder for the specific image format biometric passport photos use, confirms this is a functioning capability, not dead code.

A second finding names a device-level surveillance layer running on the same device that processes this passport data, not a single tracking flow: LexisNexis ThreatMetrix (37 classes) device fingerprinting and MobileShield (21 classes) are both active, meaning server-side linkage between passport biometric processing and device fingerprinting occurs on the same device, a data protection impact assessment trigger under Art. 35(3)(b). A third finding, CyberfEnd, an obfuscated SDK, is present here as the third consecutive travel-sector app in this audit series found to contain it, following trivago and a package originally attributed to Amadeus, suggesting a shared upstream vendor across otherwise unrelated travel apps.

Four messages were sent across 77 days. The initial disclosure to privacy@aircanada.com, security@aircanada.com, and dpo@aircanada.com bounced repeatedly, generating ten separate delivery-failure notifications between 27 June and 20 July 2026. A working address, privacy_vieprivee@aircanada.ca, was located and used for the final two messages, on 29 August and 12 September 2026. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, set at first contact, elapses today, 25 September 2026, and this report publishes on that date.

**Scope:** Root-level static analysis of the production Air Canada Android application (com.aircanada.mobile), as reviewed on 27 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Air Canada's, LexisNexis's, or Kochava-family backend infrastructure was performed.

### Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. The presence of Extended Access Control Terminal Authentication, the ICAO 9303 protocol required exclusively to extract fingerprints and iris scans from EU biometric passport chips, reaches HIGH on the computed CVSS score alone. Device-fingerprinting software running on the same device that handles passport biometric data, a shared obfuscated SDK also found in two other travel-sector apps in this audit series, undocumented network and connectivity permissions, and a hardcoded Firebase key all correct to MEDIUM. Four messages were sent across 77 days, the majority bouncing before a working address was found. Not one reply of any kind was ever received.

| ID | Severity | Title |
|---|---|---|
| C1 | HIGH | Extended Access Control Terminal Authentication: the Specific Protocol Required to Extract Fingerprints and Iris Scans From EU Biometric Passports |
| H1 | MEDIUM | Device Fingerprinting Software Active on the Same Device Handling Passport Biometric Data |
| H2 | MEDIUM | A Shared, Obfuscated SDK Also Found in Two Other Travel-Sector Apps in This Audit Series |
| H3 | MEDIUM | Undocumented Network and Connectivity Modification Permissions |
| M1 | MEDIUM | Firebase API Key Hardcoded and Extractable |

## Subject & Operator Analysis

Air Canada is a major international airline headquartered in Montreal, Canada, whose Android app handles booking, check-in, boarding passes, and biometric passport scanning for international travel.

## Ten Bounces, One Working Address Found Late, Zero Reply

This case's correspondence record involved extensive delivery failure before any working channel was found. The initial disclosure to privacy@aircanada.com, security@aircanada.com, and dpo@aircanada.com generated ten separate bounce or delivery-delay notifications between 27 June and 20 July 2026, across three separate follow-up attempts. A working address, privacy_vieprivee@aircanada.ca, Air Canada's Canadian French-language privacy contact, was located and used for the final two messages, on 29 August and 12 September 2026, cc'ing CNIL and the German BfDI. Not one reply, automated or human, was ever received on any address at any point across the full 77 days of outreach.

## Findings

### C1: Extended Access Control Terminal Authentication: the Specific Protocol Required to Extract Fingerprints and Iris Scans From EU Biometric Passports

**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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.**

JMRTD (166 classes) implements APDULevelEACTACapable, Extended Access Control Terminal Authentication, the ICAO 9303 protocol required exclusively to access Data Group 3 (ten-print fingerprints) and Data Group 4 (iris scans) from EU biometric passport chips. Basic Access Control and PACE, the mechanisms most travel apps use, only reach Data Groups 1 and 2 (name, document number, and similar). A full supporting stack, BouncyCastle post-quantum cryptography, EJBCA CVC certificate management, net.sf.scuba smart-card NFC, and a JPEG2000 decoder for biometric passport photos, plus a dedicated OARO module (475 classes: biometric, document-scanner, NFC-passport-reader, and onboarding components), confirms this is a functioning capability.

```
JMRTD (166 classes): APDULevelEACTACapable (Extended Access Control Terminal
    Authentication)
BouncyCastle post-quantum crypto, EJBCA CVC cert management, net.sf.scuba (smart-card
    NFC), jj2000 (JPEG2000 decoder)
OARO (475 classes): bio + documentscanner + nfcpassportreader + onboarding
```

**Impact:** The app contains the specific technology needed to extract fingerprints and iris scans from an EU biometric passport chip, beyond the basic passport-reading most travel apps use, in a consumer airline booking application.

**Fix:** Document the specific purpose requiring EAC-TA-level access, restrict it to a confirmed, disclosed use case, or remove it if the app does not actually need biometric Data Group 3/4 access. No confirmation that this has occurred was ever received.

### H1: Device Fingerprinting Software Active on the Same Device Handling Passport Biometric Data

**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.**

LexisNexis ThreatMetrix (37 classes) and MobileShield (21 classes) are both active on the same device where passport biometric processing occurs, meaning server-side linkage between the two is architecturally possible, an Art. 35(3)(b) DPIA-triggering combination.

```
LexisNexis ThreatMetrix (37 classes)
MobileShield (21 classes)
```

**Impact:** Device-fingerprinting data and biometric passport data are both processed on the same device, creating a potential linkage between a user's device identity and their biometric passport data.

**Fix:** Document whether ThreatMetrix and MobileShield outputs are ever linked to passport-processing data, and conduct an Art. 35 DPIA if so. No confirmation that this has occurred was ever received.

### H2: A Shared, Obfuscated SDK Also Found in Two Other Travel-Sector Apps in This Audit Series

**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.**

CyberfEnd is present in this binary, confirmed as the third consecutive travel-sector app in this audit series found to contain the same obfuscated SDK, following trivago and a package originally, and since corrected, attributed to Amadeus, suggesting a shared upstream vendor or build pipeline across otherwise unrelated travel-industry apps.

**Impact:** An obfuscated SDK's presence across three unrelated travel-industry apps suggests a shared vendor whose data-processing role has not been independently established for any of them.

**Fix:** Identify and document CyberfEnd's function and data-processing role. No confirmation that this has occurred was ever received.

### H3: Undocumented Network and Connectivity Modification Permissions

**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.**

WRITE_SETTINGS, CHANGE_NETWORK_STATE, and CHANGE_WIFI_STATE are all declared with no documented feature located that requires them.

```
android.permission.WRITE_SETTINGS
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_STATE
```

**Impact:** The app can modify system settings and network/WiFi state with no documented feature justifying that capability in an airline booking app.

**Fix:** Document the specific feature requiring each permission, or remove unused ones. No confirmation that this has occurred was ever received.

### M1: Firebase API Key Hardcoded and Extractable

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

A Firebase API key is hardcoded and extractable from the production binary, project aircanada-app.

```
AIzaSyBJgQEakXrAEcX9Fbb47RRXL0uO3TP-OsQ (Firebase project: aircanada-app)
```

**Impact:** The key is trivially extractable, and depending on the security-rule configuration behind it, could enable unauthorized access or denial of service against legitimate users.

**Fix:** Restrict the Firebase API key by package name and SHA-1 certificate fingerprint. No confirmation that this has occurred was ever received.

## 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, Art. 35(3)(b) | C1 | The specific technical capability required to extract biometric passport data beyond standard reading. |
| Art. 35(3)(b) | H1 | Device fingerprinting active on the same device as biometric passport processing. |
| Art. 13(1)(e) | H2 | An unidentified, obfuscated SDK shared across multiple travel-sector apps. |
| Art. 5(1)(c), Art. 13(1)(c) | H3 | Undocumented network and system-settings modification permissions. |
| Art. 32 | M1 | Hardcoded, trivially extractable Firebase API key. |

**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 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; H1, H2, H3, and M1 correct to MEDIUM to match their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: AIRCANADA-2026-R1.