Coordinated Privacy Disclosure, Final Report

Priority Pass Android (com.prioritypass3)

Priority Pass Ltd, a subsidiary of Collinson Group, London, UK

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

Target	Priority Pass, an airport lounge-access membership platform
Package	com.prioritypass3, version 6.73.0
Operator	Priority Pass Ltd, a subsidiary of Collinson Group, London, UK
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	UK ICO (lead supervisory authority), Austrian DSB, Germany's BfDI, CERT.at
Total Outbound Messages	5, across 77 days, to security@prioritypass.com; privacy@prioritypass.com and dpo@prioritypass.com both hard-bounced from the first send onward.
Inbound Replies	0. No reply, automated or human, was ever received.

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 Priority Pass Ltd that its Android app runs three session-recording platforms, Heap, ContentSquare, and Datadog RUM, simultaneously before any consent signal, on an app whose primary screens display payment card details, lounge membership credentials, and travel history. Heap's autocapture module initializes at the earliest possible ContentProvider priority, and ContentSquare, the largest single session-recording SDK found in this build at 404 classes, adds heatmaps, session replay, and user-journey analysis. Every tap on a payment card screen and every rendered lounge-access QR code is within the capture scope of at least one of these platforms before the user has consented to anything. This computes to HIGH/8.7 under CVSS v4.0.

A second HIGH finding: ACCESS_BACKGROUND_LOCATION, the most invasive location permission Android offers, tracks the device's precise GPS continuously, including when the app is closed and the screen is off. Combined with LocusLabs, an airport indoor-mapping SDK, Priority Pass can construct a continuous record of a user's movement through terminal, gate, lounge, and departure, even after the app has been closed, with no documented legal basis in the privacy policy.

A third finding, MEDIUM: AppDynamics, Cisco's enterprise Application Performance Monitoring agent, instruments network calls, UI performance, and error traces, potentially including authentication request headers and timing data, and routes this telemetry to Cisco's US infrastructure with no Art. 13(1)(e) disclosure naming it as a processor. A fourth finding, LOW: SYSTEM_ALERT_WINDOW allows the app to draw a persistent overlay over every other application on the device, including banking apps and lock screens, with no documented functional need in a lounge-access app. A fifth, purely informational finding: the production APK contains com.example.googlemapapp.permission.MAPS_RECEIVE, a permission string copied verbatim from Google's own Maps SDK tutorial and never replaced with the app's real package name. It is functionally inert and carries no computed CVSS severity, but its presence in a build distributed to millions of users is worth naming as a build-rigor signal. Genuine positives are worth naming: no cleartext traffic override exists, HTTPS is enforced throughout, allowBackup is correctly set to false, biometric authentication is used properly, Braintree is a well-established payment processor, and no passport-scanning SDKs were found.

Five messages were sent across 77 days, to security@prioritypass.com; privacy@prioritypass.com and dpo@prioritypass.com both hard-bounced from the first send onward. The UK ICO, as lead supervisory authority, along with the Austrian DSB and Germany's BfDI, were copied throughout. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, stated directly to the target in the initial disclosure, elapses today. This report and the accompanying closure notice publish on the stated date.

Scope: Root-level static analysis of the production Priority Pass Android application (com.prioritypass3, version 6.73.0), pulled from Google Play and reviewed on 27 June 2026. No account was created and no interaction with Heap's, ContentSquare's, Datadog's, or AppDynamics's backend infrastructure was performed.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Three simultaneous pre-consent session-recording platforms active on payment and membership-credential screens, and continuous background location tracking combined with indoor airport positioning, both correct to HIGH. An undisclosed Cisco enterprise telemetry agent corrects to MEDIUM. A system-wide overlay permission corrects to LOW. A left-over tutorial-placeholder permission string is functionally inert and carries no computed severity. Five messages were sent across 77 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	Three Simultaneous Session-Recording Platforms Active on Payment and Membership Screens
C3	HIGH	Continuous Background Location Combined With Indoor Airport Positioning
H1	MEDIUM	Undisclosed Cisco Enterprise Telemetry Agent
C2	LOW	System-Wide Overlay Capability
H2	LOW	Leftover Tutorial-Placeholder Permission String

Subject & Operator Analysis

Priority Pass Ltd, a subsidiary of Collinson Group, London, UK, operates one of the largest airport lounge-access membership platforms. The UK ICO is the competent lead supervisory authority for Priority Pass's EU operations.

Genuine positives are worth naming. No cleartext traffic override exists; HTTPS is enforced throughout. allowBackup is correctly set to false. USE_BIOMETRIC is used for authentication, not identification. Braintree, the payment processor, is well-established and follows secure patterns. No passport-scanning SDKs were found. The core transport and payment-authe ntication posture is sound; the pre-consent session-recording and location-tracking layer is where the gaps in this report sit.

Five Messages, Zero Reply

All five messages in this case's correspondence record were sent to security@prioritypass.com across 77 days; privacy@prioritypass.com and dpo@prioritypass.com both hard-bounced from the first send onward. The UK ICO, Austrian DSB, and Germany's BfDI were copied throughout. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Three Simultaneous Session-Recording Platforms Active on Payment and Membership Screens

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.

Heap (autocapture, initOrder=1, the earliest possible ContentProvider priority), ContentSquare (404 classes, the largest session-recording SDK in this build, heatmaps and session replay), and Datadog RUM all initialize before any consent UI is shown, on an app whose primary screens display payment card details, lounge membership credentials, and travel history.

```
HeapViewAutocaptureContentProvider -> initOrder=1
HeapCoreContentProvider -> initOrder=2
DdRumContentProvider (Datadog RUM) -> fires on attach
FirebaseInitProvider -> initOrder=100, directBootAware=true
google_api_key: AIzaSyAFGhZrg1RhVyMJ7UUerNd96pXGELaQrGM
```

Impact: Every tap on a payment card screen, every lounge-access QR code displayed, and every membership credential rendered is within capture scope for at least one of three recording platforms, before the user has consented to anything, and none of the three is disclosed as a named data processor.

Fix: Gate all three session-recording platforms behind a consent mechanism before any capture begins. No confirmation that this has occurred was ever received.

C3: Continuous Background Location Combined With Indoor Airport Positioning

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.

ACCESS_BACKGROUND_LOCATION tracks the device's precise GPS continuously, including when the app is not in use and the screen is off. Combined with LocusLabs, an airport indoor-mapping SDK, the app can construct a continuous record of a user's movement through terminal, gate, lounge, and departure, even after the app is closed.

Impact: A detailed, continuous movement record through airport facilities is built with no documented legal basis, using the most invasive location permission Android offers.

Fix: Document the specific Art. 6 legal basis for background location processing and complete a DPIA covering the LocusLabs indoor-positioning component specifically. No confirmation that this has occurred was ever received.

H1: Undisclosed Cisco Enterprise Telemetry Agent

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.

AppDynamics (com.appdynamics.eumagent), Cisco's enterprise Application Performance Monitoring platform, instruments network calls, UI performance, and error traces, potentially including request headers, response codes, and timing data for authentication flows, routed to Cisco's US infrastructure.

Impact: Performance telemetry from a payment- and credential-handling app reaches Cisco's US infrastructure with no Art. 13(1)(e) disclosure naming it as a processor.

Fix: Name AppDynamics as a data processor in the privacy policy and document the applicable Art. 28 processor agreement. No confirmation that this has occurred was ever received.

C2: System-Wide Overlay Capability

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.

SYSTEM_ALERT_WINDOW allows the app to draw a persistent overlay over every other application on the device, including banking apps, password managers, and lock screens, the mechanism used in overlay-phishing and clickjacking attacks. No documented functional requirement exists in a lounge-access app.

Impact: A lounge-membership app carries the technical capability to draw arbitrary UI over any other app on the device, with no disclosed purpose.

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

H2: Leftover Tutorial-Placeholder Permission String

LOW, INFORMATIONAL, functionally inert, no exploitable technical impact, CVSS not applicable.

com.example.googlemapapp.permission.MAPS_RECEIVE is present in the production APK, a permission string copied verbatim from Google's Maps SDK getting-started tutorial, where com.example.googlemapapp is the placeholder package name developers are meant to replace. This confirms the declaration was copied from tutorial code without modification.

Impact: The finding itself is functionally inert and carries no exploitable technical impact. It is reported as a build-rigor signal: its presence in a production app distributed to millions of users suggests other configuration artifacts may have been similarly overlooked, a pattern worth naming even where CVSS does not apply.

Fix: Remove the leftover tutorial permission string. 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. 6, Art. 7, Art. 13, Art. 32	C1	Three simultaneous session-recording platforms active on payment and membership screens.
Art. 5(1)(c), Art. 6, Art. 13	C3	Continuous background location combined with indoor airport positioning.
Art. 13, Art. 44	H1	Undisclosed Cisco enterprise telemetry agent.
Art. 5(1)(c), Art. 13	C2	System-wide overlay capability.
Art. 25	H2	Leftover tutorial-placeholder permission string, privacy by design.

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 C3 correct to HIGH, H1 corrects to MEDIUM, and C2 and H2 correct to LOW, all on their own computed bands, with no escalation applied. H2 is a functionally inert build-quality artifact, reported for its own sake, not a real vulnerability; CVSS does not meaningfully apply to it. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: PRIORITYPASS-2026.