Coordinated Privacy Disclosure, Final Report

Freecash (com.freecash.app2)

Almedia GmbH, Potsdamer Str. 125, 10783 Berlin, Germany

FAST TO ACKNOWLEDGE, SILENT ON SUBSTANCE · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 96 DAYS AFTER DISCLOSURE, FOUR FORWARDING CONFIRMATIONS, ZERO TECHNICAL ANSWER

Target	Freecash, a Get-Paid-To (GPT) rewards platform with 10M+ downloads, users earn coins for completing offers and convert them to PayPal, bank transfer, or cryptocurrency payouts
Package	com.freecash.app2
Operator	Almedia GmbH, Potsdamer Str. 125, 10783 Berlin, Germany
Initial Disclosure	2026-06-20
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-24, five days after the embargo, an internal publishing gap, not a change in terms
Regulators in CC	Austrian DSB. Competent supervisory authority for the operator is the Berliner Beauftragte für Datenschutz und Informationsfre iheit (BlnBDI)
Total Outbound Messages	6, across 96 days
Inbound Replies	4, all from support@freecash.com, each a generic forwarding confirmation naming no finding. Zero replies of any kind since 7 August 2026, 48 days of total silence including through two follow-up deadlines.

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

Contents

1 Executive Summary 4

2 Subject & Operator Analysis 5

3 Architecture & Data Flow 6

4 Findings 6

4.1 C1: Firebase API Key Hardcoded in a Production App That Processes Real-Money Payouts . . . 6

4.2 C2: PACKAGE_USAGE_STATS Combined With Confirmed adjoe and CleverTap Queries: Full Device App-Ecosystem Surveillance . . . 7

4.3 H1: All Four Android Privacy Sandbox Advertising Permissions Declared Simultaneously . . . 8

4.4 H2: Fyber FairBid and Tapjoy, a Dual Offer-Wall Stack, the Largest Ad Mediation Footprint in This Audit Series . . . 9

4.5 H3: Four Independent Marketing and Analytics Platforms Running Simultaneously 10

4.6 H4: Dormant Braze Geofence Module Present, No Location Permission Currently Declared . . . 10

4.7 H5: Minimum SDK 21 (Android 5.0 Lollipop, 2014) Permits Financial Payouts on a Decade of Unpatched Devices . . . 11

4.8 H6: Trusted Web Activity Architecture Plus a Native Adjust Bridge: Dual Web and Native Tracking Per Offer Completion . . . 11

5 Impact Analysis 12

6 Fast to Acknowledge, Silent on Substance: Four Replies, Zero Findings Named, Then 48 Days of Nothing 12

7 Data Protection, Article by Article 13

Executive Summary

On 20 June 2026, RFI-IRFOS disclosed to Almedia GmbH that its rewards platform, Freecash, combines a hardcoded Firebase API key with the Android permission android.permission.PACKAGE_USAGE_STATS, confirmed in bytecode to be actively queried by both the adjoe Playtime SDK and CleverTap, meaning Freecash and its SDK partners can build a behavioral profile spanning the user's entire device, not just their activity inside Freecash, on a platform whose users complete tasks in exchange for real-money PayPal, bank, and cryptocurrency payouts.

Freecash's support team responded the same day the disclosure was sent, faster than nearly every other target in this year's audit series, and three named support staff (Tamsen, Brett, Mara) each separately confirmed, over the following seven weeks, that the report had been forwarded to the development team. Not one of those four replies engaged a single specific finding, named a remediation step, or answered a direct question. On 18 August 2026, after 57 days of forwarding confirmations, RFI-IRFOS posed three specific yes-or-no questions about the two CRITICAL findings directly to Almedia GmbH, with a deadline of 25 August. That deadline passed without any reply. The same three questions were repeated on 5 September 2026 with a new deadline of 7 September. That deadline also passed without reply. As of publication, 48 days have elapsed since Freecash's last message of any kind.

Scope: Root-level static analysis of the production Freecash Android application (com.freecash.app2, version 1.195, versionCode 195, 20,297 smali classes), covering the AndroidManifest, resource strings, and decompiled dex/smali, as pulled and reviewed on 20 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Freecash's or Almedia GmbH's backend infrastructure was performed. The public build has been re-pulled and hash-compared on a weekly cadence throughout the embargo period; no findings below required revision as a result.

Disposition

Eight findings were disclosed on 20 June 2026, later re-scored under CVSS v4.0: one finding independently reaches CRITICAL on the computed CVSS score alone, without any editorial escalation (PACKAGE_USAGE_STATS combined with confirmed adjoe and CleverTap device-wide usage-stats queries, functioning as full device app-ecosystem surveillance on a platform that also processes real-money payouts). One finding is corrected down to MEDIUM (a hardcoded Firebase key, availability-only exposure). Four findings correct down to MEDIUM from an original HIGH label. Two findings, a dormant geofence module and a 2014-era minimum OS version, are classified OBSERVATIONAL, real and worth recording but not demonstrated technical attack paths on their own. Freecash's support team replied four times, faster than nearly every other target in this year's audit series, but every reply was an identical, content-free forwarding confirmation. Three specific yes-or-no questions about the two CRITICAL findings, posed on 18 August 2026 with a deadline of 25 August, then repeated on 5 September with a deadline of 7 September, received no answer of any kind, not even a fifth forwarding confirmation. This report closes and publishes the case on the terms disclosed from the first message.

ID	Severity	Title
C1	MEDIUM	Firebase API Key Hardcoded in a Production App That Processes Real-Money Payouts
C2	CRITICAL	PACKAGE_USAGE_STATS Combined With Confirmed adjoe and CleverTap Queries: Full Device App-Ecosystem Surveillance
H1	MEDIUM	All Four Android Privacy Sandbox Advertising Permissions Declared Simultaneously
H2	MEDIUM	Fyber FairBid and Tapjoy, a Dual Offer-Wall Stack, the Largest Ad Mediation Footprint in This Audit Series
H3	MEDIUM	Four Independent Marketing and Analytics Platforms Running Simultaneously
H4	OBSERVATIONAL	Dormant Braze Geofence Module Present, No Location Permission Currently Declared
H5	OBSERVATIONAL	Minimum SDK 21 (Android 5.0 Lollipop, 2014) Permits Financial Payouts on a Decade of Unpatched Devices
H6	MEDIUM	Trusted Web Activity Architecture Plus a Native Adjust Bridge: Dual Web and Native Tracking Per Offer Completion

Subject & Operator Analysis

Freecash (com.freecash.app2) is a Get-Paid-To rewards platform with over 10 million downloads, operated by Almedia GmbH of Berlin, Germany. Users complete offers, app installs, surveys, game sessions, video views, in exchange for virtual coins convertible to PayPal, bank transfer, or cryptocurrency payouts. The app is a Trusted Web Activity wrapper around app.freecash.com.

A genuine positive is worth naming plainly: Freecash's support team responded the same day RFI-IRFOS's disclosure was sent, and continued to reply, by name, across seven weeks, faster and more consistently than the large majority of the more than two hundred companies contacted in this year's campaign. The certificate-pinning configuration for the production offer-wall backend (adjoe.zone, 5 SHA-256 pins) and a current compileSdk (35) are also genuine positives. None of this, however, produced a single sentence of technical engagement with any of the eight findings across four separate replies.

Architecture & Data Flow

Freecash's business model requires that user actions generate advertising value, and the SDK architecture reflects this directly: all four Android Privacy Sandbox advertising permissions (H1), two independent offer-wall platforms (H2), four independent marketing and analytics platforms (H3), and, underneath all of it, PACKAGE_USAGE_STATS combined with confirmed adjoe and CleverTap device-wide usage queries (C2), the single finding in this report that reaches CRITICAL on CVSS v4.0 alone. A hardcoded Firebase key (C1) sits at the operation al-security layer beneath a platform that also processes real-money payouts.

Findings

C1: Firebase API Key Hardcoded in a Production App That Processes Real-Money Payouts

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

The Firebase API key and App ID are hardcoded in res/values/strings.xml and extractable from the public APK in under 60 seconds by anyone. Firebase keys are not secrets by design, so the finding is availability, not confidentiality: a party holding the key can exhaust the project's Firebase quota. On a platform where users store wallet balances and link PayPal accounts, an availability failure in the backing infrastructure carries direct financial consequences for users mid-payout.

```
res/values/strings.xml
google_api_key:  AIzaSyAEEEydtKNVcH6muebvwKwbSaOg3QRGjHk
google_app_id:   1:772342929499:android:4a7764a26b53cf2f94877e
Firebase modules active: Analytics, Crashlytics, Messaging, Installations
```

Impact: Quota exhaustion or credential abuse can disrupt backend availability for a platform whose core function is processing real-money payouts, a service context where downtime has a direct financial cost to users.

Fix: Rotate the exposed key, apply Firebase App Check and key restrictions, and route database access through an authenticated backend layer. As of 5 September 2026, RFI-IRFOS asked directly whether the key had been rotated since 22 June 2026; no answer was ever received.

C2: PACKAGE_USAGE_STATS Combined With Confirmed adjoe and CleverTap Queries: Full Device App-Ecosystem Surveillance

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N, 9.2. This finding reaches CRITICAL on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

The manifest declares android.permission.PACKAGE_USAGE_STATS, one of Android's most invasive protected permissions, grantable only through a manual system-settings flow. Static analysis confirms active use: five distinct smali classes across the adjoe Playtime SDK call UsageStatsManager/queryUsageStats to monitor which partner game apps a user opens and for how long, and a separate CleverTap class independently reads the same device-wide usage-stats data. Neither is scoped to Freecash's own app; UsageStatsManager exposes the complete device app-usage history, every app opened, how long, how frequently, to both vendors. On a platform whose commercial model is selling user attention and behavioral data to advertisers, this device-wide visibility, not Freecash-specific analytics, is the core commercial asset.

```
AndroidManifest.xml: android.permission.PACKAGE_USAGE_STATS

io/adjoe/sdk/internal/P0.smali      -- adjoe Playtime: monitors game session duration
io/adjoe/sdk/internal/H.smali       -- adjoe internal usage stats handler
io/adjoe/sdk/internal/s0.smali      -- adjoe usage tracking
io/adjoe/sdk/internal/T.smali       -- adjoe usage stats transmitter
com/clevertap/android/sdk/q$d.smali -- CleverTap: reads device usage stats
```

Impact: Two independent third parties can each construct a profile of every app installed and used on a person's device, banking, health, dating, and messaging apps included, entirely outside the scope of what Freecash itself needs to operate, on a platform whose users are financially incentivized to keep the app installed and engaged.

Fix: Document a specific Art. 6(1) legal basis for PACKAGE_USAGE_STATS distinct from prize administration, disclose the device-wide scope of adjoe's and CleverTap's access before the permission is requested, and consider whether Art. 35 DPIA obligations are triggered. Asked directly on 18 August and again on 5 September 2026 whether a documented DPIA exists for this combination; no answer was ever received.

H1: All Four Android Privacy Sandbox Advertising Permissions Declared Simultaneously

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

The manifest declares ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_CUSTOM_AUDIENCE, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_AD_ID together, each a distinct advertising pipeline: interest-category profiling, on-device remarketing auctions, OS-level conversion tracking, and the cross-app advertising identifier. Combined with PACKAGE_USAGE_STATS (C2) and the ad-mediation and marketing stacks below (H2, H3), the cumulative profiling scope is proportionate to a full advertising exchange, not a rewards app.

```
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
```

Impact: A user's interest profile, remarketing eligibility, and cross-app identity are all simultaneously exposed to the advertising ecosystem through four independent, OS-level pipelines, each requiring its own disclosed legal basis.

Fix: Document an individual Art. 6(1) legal basis and Art. 13(1)(c) disclosure for each of the four Privacy Sandbox pipelines separately. No confirmation that this has occurred was ever received.

H2: Fyber FairBid and Tapjoy, a Dual Offer-Wall Stack, the Largest Ad Mediation Footprint 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:L/SI:N/SA:N, 6.9.

Fyber FairBid (3,146 smali classes, the largest single SDK in this audit series) and Tapjoy (585 classes), both owned by Digital Turbine, run as two independent, parallel offer-wall platforms. Each completed offer generates a conversion event tracked across at least Fyber, Adjust, and the Privacy Sandbox Attribution API. Digital Turbine is US-headquartered; no Art. 44-49 transfer mechanism for EU offer-completion data is disclosed at the app level.

```
com/fyber/fairbid/          -- core mediation, 3,146 classes
com/fyber/fairbid/ads/ofw/   -- offer wall module
com/tapjoy/                  -- second, independent offer wall, 585 classes
```

Impact: Every completed offer generates a multiply-tracked conversion event routed to a US-headquartered ad-mediation operator with no disclosed transfer mechanism for EU user data.

Fix: Name Fyber FairBid, Tapjoy, and Digital Turbine individually as data recipients with a stated Art. 44-49 transfer mechanism in the privacy documentation. No confirmation that this has occurred was ever received.

H3: Four Independent Marketing and Analytics Platforms Running Simultaneously

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

Braze (875 classes, US), CleverTap (223 classes, India), Adjust (331 classes, Germany-registered but routes to US), and Amplitude (3 classes, US) all run in parallel. Adjust's WebView JavaScript bridge generates attribution events directly inside the offer-completion flow; Braze ships a full HTML/JS in-app-message bridge and, separately, a dormant geofencing module (H4). Four independent CRM/analytics platforms for a rewards app is a data-minimization question the app's own architecture does not answer.

SDK	Classes	Data flows to
Braze	875	US (Braze Inc., NYC)
CleverTap	223	India (CleverTap, Mumbai)
Adjust	331	Germany-registered, routes to US
Amplitude	3	US (Amplitude Inc., SF)

Impact: The same offer-completion event is independently captured and transmitted by four separate marketing and analytics vendors across three jurisdictions, none individually named with a stated legal basis in the privacy documentation.

Fix: Name each of the four platforms individually with its specific data flow destination and legal basis under Art. 13(1)(e) and Art. 44-49. No confirmation that this has occurred was ever received.

H4: Dormant Braze Geofence Module Present, No Location Permission Currently Declared

OBSERVATIONAL — not independently CVSS-scored; ACCESS_FINE_LOCATION is not currently declared, so this is latent infrastructure, not an active data flow.

com/braze/models/BrazeGeofence.smali is present in the production binary. The current manifest does not declare ACCESS_FINE_LOCATION, so geofencing is dormant today. Braze geofencing can be enabled from the Braze dashboard without a new app release, and the location permission could be added in a future update to activate this existing infrastructure immediately, an undisclosed latent capability worth naming even though it is not active now.

Impact: A location-tracking capability already exists in the shipped binary and could be switched on server-side at any time, without users seeing a new permission-request flow tied to a visible app update.

Fix: Disclose the presence of dormant geofencing infrastructure and commit to a permission-change notice if it is ever activated. No confirmation that this has occurred was ever received.

H5: Minimum SDK 21 (Android 5.0 Lollipop, 2014) Permits Financial Payouts on a Decade of Unpatched Devices

OBSERVATIONAL — not independently CVSS-scored; a platform-fragmentation exposure, not a specific demonstrated vulnerability in the app itself.

minSdk 21 allows Freecash to process real-money PayPal, bank, and cryptocurrency payouts and store wallet balances on Android 5.0 Lollipop devices from 2014, more than a decade without security patches. This is a general platform-security posture question, not a specific exploited flaw, and is recorded here as a real, transparency-relevant gap, not a scored technical attack path.

Impact: Financial transaction data and wallet credentials are processed on a device population that, by construction, includes phones with over a decade of unpatched operating-system vulnerabilities.

Fix: Raise minSdk to a currently-supported Android baseline for the financial-transaction code path specifically, even if the general app retains broader compatibility. No confirmation that this has occurred was ever received.

H6: Trusted Web Activity Architecture Plus a Native Adjust Bridge: Dual Web and Native Tracking Per Offer Completion

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.

Freecash's core experience runs as a Trusted Web Activity rendering app.freecash.com inside a Chrome Custom Tab. Survey responses and offer completions therefore happen inside a WebView, subject to standard web tracking, while the Adjust JavaScript bridge (assets/adjust.js) simultaneously injects native attribution events into that same WebView context. Every offer completion is tracked twice, once at the web layer and once at the native SDK layer, neither disclosed individually.

```
android:manageSpaceActivity="com.google.androidbrowserhelper.trusted.
    ManageDataLauncherActivity"
baseUrl / launchUrl: https://app.freecash.com
assets/adjust.js, adjust_config.js, adjust_event.js -- native bridge inside the
    WebView
```

Impact: The cumulative behavioral profile generated per offer completion, combining web-layer and native-layer tracking of the identical user action, exceeds what either tracking system alone would suggest is collected.

Fix: Disclose the dual-layer tracking architecture explicitly and document the combined data collection scope for a single offer-completion event. No confirmation that this has occurred was ever received.

Impact Analysis

C2 does not sit beside the advertising-stack findings (H1-H3), it sits underneath them as their enabling layer: H1 through H3 describe how Freecash and its partners monetize behavior inside the app, and C2 shows that the same partners can see behavior on the rest of the user's device too, unscoped to Freecash. On a platform where completing tasks earns real money, this device-wide visibility is not incidental to the business model, it is a structural part of it.

Fast to Acknowledge, Silent on Substance: Four Replies, Zero Findings Named, Then 48 Days of Nothing

This case's correspondence record is a distinct pattern from most others in this campaign: Freecash replied quickly and by name, four times across seven weeks (Sophie, Tamsen, Brett, Mara), each confirming the report had been forwarded to the development team, and none engaging a single specific finding. On 18 August 2026, after 57 days of forwarding confirmations, RFI-IRFOS posed three direct yes-or-no questions about the two CRITICAL findings to Almedia GmbH, with a deadline of 25 August 2026. That deadline passed unanswered. The same three questions were repeated on 5 September 2026 with a new deadline of 7 September. That deadline also passed unanswered. As of this publication, 48 days have elapsed since Freecash's last message of any kind, not even a fifth forwarding confirmation.

THE THREE QUESTIONS, POSED TWICE, NEVER ANSWERED

1. On what Art. 6(1) GDPR legal basis is PACKAGE_USAGE_STATS processed, and is it disclosed to users before the permission request that it captures usage of other apps on the device. Yes or no.
2. Has the Firebase key (AIzaSyAEEEydtKNVcH6muebvwKwbSaOg3QRGjHk) been rotated since 22 June 2026. Yes or no.
3. Does a documented Art. 35 GDPR Data Protection Impact Assessment exist for the combination of device-wide usage tracking, four marketing platforms, and real-money payouts. Yes or no, and if yes, with what date.

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. 32(1)(b)	C1	Hardcoded Firebase credential, availability risk on a platform processing real-money payouts.
Art. 5(1)(b), Art. 6(1), Art. 35	C2	Device-wide app-usage surveillance via PACKAGE_USAGE_STATS, confirmed active by two independent SDKs, no documented legal basis or DPIA received.
Art. 6(1), Art. 13(1)(c)	H1	Four simultaneous ad-targeting permission pipelines, no individually disclosed legal basis.
Art. 13(1)(e), Art. 44-49	H2	Dual offer-wall stack, undisclosed transfer mechanism to a US-headquartered operator.
Art. 13(1)(e), Art. 44-49, Art. 5(1)(c)	H3	Four independent marketing platforms, no individually disclosed legal basis or transfer mechanism.

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, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, C2 reaches CRITICAL on its computed CVSS v4.0 score alone, with no editorial escalation applied or needed; C1, H1, H2, H3, and H6 are corrected down to MEDIUM to match their own computed bands; H4 and H5 are classified OBSERVATIONAL because they are real, transparency-relevant findings without a demonstrated technical attack path to score. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: FREECASH-2026-R1.