Coordinated Privacy Disclosure, Final Report

Coin Master Android (com.moonactive.coinmaster)

Moon Active Ltd, 100M+ installs

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, EIGHT MESSAGES, ZERO REPLY OF ANY KIND

Target	Coin Master, a slot-machine-mechanic mobile game
Package	com.moonactive.coinmaster, 100M+ installs
Operator	Moon Active Ltd
Initial Disclosure	2026-06-24
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Austrian DSB, Germany's BfDI, UK ICO, EDPS
Total Outbound Messages	8, across 65 days, all to privacy@moonactive.com and dpo@moonactive.com; a separate BCC copy to the UK ICO bounced on the first send, the primary target addresses accepted every message.
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 24 June 2026, RFI-IRFOS disclosed to Moon Active that its Coin Master Android app, installed over 100 million times, reads the device address book of its own users to obtain the names of people who have never installed the app, never seen its privacy policy, and never given any form of consent. Three dedicated first-party libraries (MoonActive.NativeContacts.dll, MoonActive.NativeContacts.Android.dll, MoonActive.ContactsConnect.dll) and a smali-level AddressBookManager.load() method exist for exactly this purpose. A second finding compounds this: the app also requests the Facebook user_friends OAuth scope through a FriendFinderDialog component, meaning a user's device contacts and their Facebook friends list are combined into a complete social graph, spanning people who never interacted with Moon Active on either channel.

A third finding concerns the app's own declared child-protection architecture, present but disconnected. Coin Master ships both an AppLovin MAX age-restriction interface and a dedicated MoonActive.AgeVerification.dll library, yet across 9,801 compiled smali files, setIsAgeRestrictedUser() is called with true zero times. The app uses explicit slot-machine, jackpot, and casino mechanics, and its own child-protection wiring exists in the binary without ever being connected to the part that matters. RFI-IRFOS holds this finding at HIGH under an explicit blast-radius escalation beyond its own computed CVSS band, given the install base and the specific combination of gambling-adjacent mechanics with unconditional behavioral ad profiling of any user, including minors.

Two further findings cover pre-consent tracking, applovin, Facebook, and Google Ads SDKs are each registered as Android ContentProviders with explicit initOrder values, one of them 101, meaning device and advertising identifiers reach three ad networks before any consent dialog is shown, and three BOOT_COMPLETED receivers fire this same sequence on device reboot even if the app is never opened, and two hardcoded Firebase API keys in the production binary, which RFI-IRFOS did not test against production systems but names as a credential-exposure and attack-surface finding regardless.

Eight messages were sent across 65 days, all to privacy@moonactive.com and dpo@moonactive.com, with the Austrian DSB, Germany's BfDI, the UK ICO, and the EDPS copied on various rounds. Not one reply, automated or human, was ever received from Moon Active on any address at any point. The embargo, stated directly to the target as 19 September 2026 in the original disclosure, elapsed six days before this report and closure notice publish.

Scope: Root-level static analysis of the production Coin Master Android application (com.moonactive.coinmaster), pulled from Google Play and reviewed on 24 June 2026. No account was created, no backend was accessed, and none of the three named credential-exposure attack vectors in H1 were tested against production systems.

Disposition

Five findings were disclosed on 24 June 2026, re-scored under CVSS v4.0. Two, the non-user contact data extraction and the dual-channel Facebook/contacts social graph extraction, reach HIGH on their own computed CVSS scores. A third, the declared-but-never-activated AppLovin age restriction flag in a slot-machine-mechanic game, computes to MEDIUM on CVSS alone but is held at HIGH under an explicit RFI-IRFOS blast-radius escalation given the finding concerns behavioral ad profiling of minors at 100M+ install scale. Pre-consent SDK initialization and hardcoded Firebase keys both correct to MEDIUM. Eight messages were sent across 65 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	HIGH	The App Reads Contacts of People Who Have Never Installed It
C2	HIGH	Declared Age-Restriction Interface, Zero Activations, in a Slot-Machine-Mechanic Game
C3	MEDIUM	Ad SDKs Initialize and Reboot-Triggered Receivers Fire Before Any Consent Screen
H2	HIGH	Facebook Friend Finder Combines With Contact Data Into a Complete Social Graph
H1	MEDIUM	Hardcoded Firebase API Keys in the Production Binary

Subject & Operator Analysis

Coin Master is a mobile slot-machine-mechanic game published by Moon Active Ltd, installed over 100 million times. Three supervisory authorities, the Austrian DSB, Germany's BfDI, and the UK ICO, have jurisdiction over their respective user populations.

Several genuine positives are worth naming. The network security configuration restricts cleartext traffic to localhost only, with no wildcard cleartext exception and no production HTTP endpoints. There is no PRC routing of any kind, no WeChat SDK, no Pangle, no ByteDance, no Chinese CDN dependency. Both MoonActive.AgeVerification.dll and Unity.Usercentrics.dll, a consent management platform, are present in the binary, meaning the architectural intent to build a compliant consent and age-verification flow exists. C2 and C3 are wiring problems on top of that existing architecture, not the absence of one.

Eight Messages, Zero Reply

All eight messages in this case's correspondence record were delivered successfully to privacy@moonactive.com and dpo@moonactive.com across 65 days, cc'ing the Austrian DSB, Germany's BfDI, and the EDPS on later rounds. A single separate BCC copy of the initial disclosure to the UK ICO's casework address bounced due to an organizational mail-flow rule, unrelated to Moon Active's own mail infrastructure. Not one reply, automated or human, was ever received from Moon Active on any address at any point.

Findings

C1: The App Reads Contacts of People Who Have Never Installed It

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.

READ_CONTACTS is declared, backed by three dedicated first-party libraries (MoonActive.NativeContacts.dll, MoonActive.NativeContacts.Android.dll, MoonActive.ContactsConnect.dll) and a smali-level AddressBookManager.load() method that reads contact names directly from the device address book. The people whose names appear in a user's contact list have never interacted with Moon Active, never seen its privacy policy, and never given consent of any kind.

```
<uses-permission android:name="android.permission.READ_CONTACTS"/>
MoonActive.NativeContacts.dll, MoonActive.NativeContacts.Android.dll, MoonActive.
    ContactsConnect.dll
smali/com/androidnative/features/common/AddressBookManager.smali: .method public load
    ()V
```

Impact: Personal data of non-users, people who have never installed Coin Master, is systematically processed at scale with no Art. 6(1) legal basis, since these individuals cannot themselves have consented to anything.

Fix: Establish a documented legal basis for the contacts use case or remove READ_CONTACTS entirely. No confirmation that this has occurred was ever received.

C2: Declared Age-Restriction Interface, Zero Activations, in a Slot-Machine-Mechanic Game

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.

The app ships 1,330 AppLovin MAX smali files including a fully declared age-restriction interface, plus a dedicated MoonActive.AgeVerification.dll library. Across 9,801 compiled smali files, setIsAgeRestrictedUser() is called with true zero times. Coin Master uses explicit slot-machine mechanics, 743 references to spin, jackpot, slot, casino, gamble, wager, and loot appear across the smali. Behavioral ad profiling runs unconditionally for every user, including minors. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the affected population is unconditional across all 100M+ installs, and the finding combines undisclosed behavioral ad profiling of minors with explicit gambling-adjacent mechanics.

```
smali/.../MaxAdapterParameters.smali: isAgeRestrictedUser()
MoonActive.AgeVerification.dll, MoonActive.AgeVerification.Android.dll (present,
    unused)
setIsAgeRestrictedUser(true): 0 invocations across 9,801 smali files
```

Impact: A child-protection mechanism that the developer's own binary shows was built, and never connected, means behavioral advertising profiling runs on minors playing a game with explicit slot-machine and casino mechanics, with no technical control preventing it.

Fix: Wire the existing age-verification result to setIsAgeRestrictedUser(true) before AppLovin initializes. No confirmation that this has occurred was ever received.

C3: Ad SDKs Initialize and Reboot-Triggered Receivers Fire Before Any Consent Screen

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.

AppLovin (initOrder=101), Facebook, and Google Ads are each registered as ContentProviders that fire at app startup, before Application.onCreate and before any consent UI. Three BOOT_COMPLETED receivers additionally fire this sequence on device reboot, meaning a user who installs the app and reboots their device without ever opening it still triggers the same ad-SDK initialization chain.

```
<provider android:name="com.applovin.sdk.AppLovinInitProvider" android:initOrder
    ="101"/>
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider" android:
    initOrder="100"/>
BOOT_COMPLETED receivers: 3
```

Impact: Device and advertising identifiers reach three ad networks before any consent dialog is shown, and the explicit initOrder value documents this as a deliberate sequencing decision, not an unreviewed SDK default.

Fix: Gate all ContentProvider ad-SDK initializers behind the existing Usercentrics consent flow. No confirmation that this has occurred was ever received.

H2: Facebook Friend Finder Combines With Contact Data Into a Complete Social Graph

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.

A FriendFinderDialog component requests the Facebook user_friends OAuth scope, reading the user's Facebook friends list. Combined with C1's device-contacts extraction, the app builds a complete social graph across two separate channels, spanning people who never interacted with Moon Active on either one.

```
smali/com/facebook/gamingservices/FriendFinderDialog.smali: "FRIEND_FINDER"
smali/com/facebook/AuthenticationTokenClaims.smali: "user_friends" OAuth scope
```

Impact: Two independent channels, device contacts and Facebook friends, each individually require their own legal basis, and combined they produce a social graph of the user and their entire network, including people who never installed the app or connected a Facebook account to it.

Fix: Remove the Facebook friends OAuth scope or establish a documented legal basis for social-graph construction covering both the user and their non-user contacts. No confirmation that this has occurred was ever received.

H1: Hardcoded Firebase API Keys in the Production Binary

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

Two Firebase API keys are hardcoded in res/values/strings.xml and confirmed via smali extraction. Three exploitation vectors are named without having been tested against production systems: security-rules misconfiguration enabling unauthenticated data access, FCM push spoofing against the full install base, and unreviewed remote-config changes that bypass Google Play review.

```
google_api_key: AIzaSyC-YLm2eZTWBgWsB0wZG9P8cLc34sOdw40
AIzaSyCTleR-Pz5mog10TgffQouT_Seh8_sAtmg
mobilesdk_app_id: 1:934677175563:android:5ea22968cd92563283d60e
```

Impact: None of the three named vectors were tested against production, but the credential exposure itself, combined with a 100M+ install base, is a real attack surface if Firebase security rules are ever misconfigured.

Fix: Restrict both keys by package name and 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. 5(1)(a), Art. 6(1), Art. 13	C1	Non-user contact data processed with no legal basis.
Art. 5(1)(b), Art. 6(1)(a), ePrivacy Art. 5(3)	C2	Declared-but-unwired age-restriction mechanism in a gambling-adjacent app.
Art. 7, Art. 5(1)(a), Art. 13, ePrivacy Art. 5(3)	C3	Ad SDK initialization before any consent UI, including on device reboot.
Art. 32, OWASP Mobile M1	H1	Hardcoded, unrestricted Firebase API keys.

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 corrects to HIGH on its own computed band, and C2 is held at HIGH under an explicit, stated blast-radius escalation beyond its computed MEDIUM band. C3 and H1 correct to MEDIUM on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: COM.MOONACTIVE.COINMASTER.