Coordinated Security & Privacy Disclosure, Final Report

PayPal for Android (com.paypal.android.p2pmobile)

PSD2 payment app, one substantive reply in ten weeks, a manifest fact misstated, the single most exposed finding left unmentioned

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ONE REPLY, ONE FALSE CLAIM, ONE FINDING LEFT OUT

Target	PayPal, Inc., San Jose, California, US
Product audited	PayPal for Android, com.paypal.android.p2pmobile
Disclosure reference	REF PAYPAL-2026-R1 / PP-ESC-127612042574605418
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Chucker interceptor / C3 Firebase, CVSS v4.0 9.3)

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Positive Observations 4

4 Findings 4

4.1 C1: Chucker HTTP interceptor active in the production PSD2 payment binary . 5

4.2 C2: Four independent Art. 9 biometric SDKs, none named as a data processor, never addressed in any reply 6

4.3 C3: Hardcoded Firebase credential in the production APK 7

4.4 H1: RECORD_AUDIO declared with no corresponding feature, and misstated as absent in PayPal's own reply 8

4.5 H2: AD_ID plus a behavioral-biometrics fraud engine instrumenting payment flows, two vendors left unaddressed 8

5 Data Protection, Article by Article 9

6 Disclosure Timeline & Outcome 10

7 Residual Risk & Recommendations 11

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production PayPal Android application, a 155MB base package plus a dedicated 1.3MB split_facialcapture.apk, 246,953 smali classes across 42 DEX files, and identified five findings, three CRITICAL, two HIGH. The most significant, in RFI-IRFOS's assessment: four independent Art. 9 biometric SDKs, FaceTec, MiTek MiSnap, MicroBlink BlinkID, and Daon DMDS, totaling 4,269 smali classes, none named individually as an Art. 28 sub-processor in PayPal's published privacy documentation.

Separately, the Chucker HTTP interceptor, 246 smali classes, is active in the production PSD2 payment binary, capturing and persisting all HTTP request and response bodies to an on-device SQLite database with a system notification. A hardcoded Firebase credential was also extracted verbatim from the production binary.

PayPal's Global Customer Complaints & Advocacy team sent one substantive reply on 12 July, signed by JJ Thompson, addressing Chucker, Firebase, advertising data sharing, and microphone access. That reply stated the app 'does not request the Android audio-recording permission required for microphone functionality', a claim contradicted by RFI-IRFOS's own static extraction of android.permission.RECORD_AUDIO from the production manifest. The same reply did not mention FaceTec, MiSnap, BlinkID, or Daon once, the report's four-biometric-SDK finding and, in RFI-IRFOS's assessment, its most legally exposed. Six subsequent written requests for correction or clarification, addressed to the reply's own named escalation contact, received no further response of any kind.

Scope: Static analysis of the publicly downloaded production PayPal Android APK, on an authorized test device, only. No PayPal account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to security@paypal.com and dpo@paypal.com, both auto-rejected by a monitored but unmonitored noreply@paypal.com mailbox on every subsequent round. A resend reached dpo@ and privacy@ directly on 28 June. On 12 July, PayPal's Global Customer Complaints & Advocacy team, under ticket PP-ESC-127612042574605418, sent the only substantive reply this case ever received: a six-paragraph review addressing Chucker, Firebase, advertising sharing, and microphone access, that misstated a manifest fact and never once named the report's most legally exposed finding. Six further written notices asking for correction received no further reply of any kind.

ID	Severity	Title
C1	CRITICAL	Chucker HTTP interceptor active in the production PSD2 payment binary
C2	CRITICAL	Four independent Art. 9 biometric SDKs, none named as a data processor, never addressed in any reply
C3	CRITICAL	Hardcoded Firebase credential in the production APK

ID	Severity	Title
H1	HIGH	RECORD_AUDIO declared with no corresponding feature, and misstated as absent in PayPal's own reply
H2	HIGH	AD_ID plus a behavioral-biometrics fraud engine instrumenting payment flows, two vendors left unaddressed

Subject & Operator Analysis

PayPal, Inc. (San Jose, California) operates a PSD2-licensed EU payment service through PayPal (Europe) S.a.r.l. et Cie, S.C.A., processing financial transaction data for a global user base.

Positive Observations

- The strongest network security configuration in RFI-IRFOS's audit series to date: TrustKit certificate pinning on paypal.com and paypalobjects.com with 6 SHA-256 backup pins each, enforcePinning="true", cleartextTrafficPermitted="false", and a live violation report-URI.
- io.didomi.sdk consent management is present.
- PayPal's Global Customer Complaints & Advocacy team, under JJ Thompson, produced the only reply in this case addressing multiple named findings directly, rather than a generic acknowledgment or bug-bounty redirect.

Findings

C1: Chucker HTTP interceptor active in the production PSD2 payment binary

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

com.chuckerteam.chucker, 246 smali classes, captures all HTTP request and response bodies and persists them to an on-device SQLite database with a persistent system notification.

PayPal's 12 July reply, verbatim: "Our investigation confirmed that Chucker is a development tool used only in internal debug versions of the application for testing purposes. The production version of the PayPal app used by customers does not include the functional Chucker implementation and cannot use Chucker to inspect, capture, or store network traffic... Chucker can only operate when an internal developer setting is enabled. This setting is disabled by default." RFI-IRFOS's finding is limited to the SDK's compiled presence, confirmed via static analysis of the publicly downloaded production APK; PayPal's reply is a claim about a runtime developer-setting gate that RFI-IRFOS's static analysis cannot itself confirm or refute, and no supporting evidence (a build-variant manifest diff, the specific gating flag, or an independent confirmation) accompanied the claim.

Impact: If PayPal's runtime gate is accurate and correctly enforced in every distributed build, exposure is limited to the compiled SDK's continued presence in the production binary. If the gate can be enabled by any actor with device access, financial transaction traffic on a licensed EU payment app becomes locally interceptable and persisted in plaintext.

Fix: Remove the Chucker dependency from the production build variant entirely rather than gating it at runtime, and publish the specific build configuration confirming its exclusion.

C2: Four independent Art. 9 biometric SDKs, none named as a data processor, never addressed in any reply

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

4,269 combined smali classes across four independent US biometric vendors, delivered via a dedicated split_facialcapture.apk and the main binary.

```
FaceTec Inc.       1,152 classes  facial liveness / 3D map
MiTek MiSnap       1,185 classes  document + facial match
MicroBlink BlinkID 1,747 classes  document scan + biometric extraction
Daon DMDS            185 classes  biometric authentication
```

None of these four vendors was mentioned once in PayPal's 12 July reply, which addressed Chucker, Firebase, advertising data sharing, and microphone access but not this finding. RFI-IRFOS's follow-up of 13 July stated, verbatim: "your letter addresses chucker, firebase, ad targeting and the microphone. it does not mention facetec, misnap, blinkid or daon once. that's not an oversight in a six-paragraph 'thorough review' – that's the single most legally exposed finding in the report, and it was the one left out." No PayPal reply since 12 July has addressed this finding by name.

Impact: Four independent Art. 9 biometric processing pipelines operate without a confirmed, publicly named Art. 28 sub-processor disclosure, on a payment app with a global EU user base.

Fix: Name all four vendors individually as Art. 28 sub-processors in the applicable privacy documentation, publish the Art. 46 transfer mechanism for each, and confirm which of the four are active for EU-region accounts specifically.

C3: Hardcoded Firebase credential in the production APK

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

A complete Firebase project configuration extracted verbatim from the production binary.

```
google_app_id:          1:735175912799:android:d6e02a642ea140a6271aea
firebase_database_url:  api-project-735175912799.firebaseio.com
project_id:             api-project-735175912799
```

PayPal's 12 July reply, verbatim: "these configuration values are not considered secret credentials and do not provide privileged access to customer information or PayPal systems." RFI-IRFOS's standing position, applied identically across every case in this research series: a publicly extractable Firebase key is a finding regardless of whether it is classified as a secret, because the burden of demonstrating its security-rules configuration rests with the operator under Art. 5(2), not with an outside researcher who cannot see the backend rules from a downloaded APK alone.

Impact: A publicly extractable Firebase key on a global payment platform enables, at minimum, quota-exhaustion and enumeration exposure whose actual severity depends on backend security rules PayPal has not disclosed.

Fix: Publish the Firestore/Storage security rules for this project, confirm App Check enforcement, or rotate and restrict the key to the production certificate fingerprint.

H1: RECORD_AUDIO declared with no corresponding feature, and misstated as absent in PayPal's own reply

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

android.permission.RECORD_AUDIO is declared in the production AndroidManifest.xml, extracted via apktool, with no corresponding audio, voice, or accessibility feature identified in the app's UI or smali.

PayPal's 12 July reply, verbatim: "Our review found no active PayPal feature that requires microphone access. The relevant code is not in use, and the application does not request the Android audio-recording permission required for microphone functionality." This is a factual claim RFI-IRFOS's own static extraction directly contradicts: a permission is either declared in the application manifest or it is not, independent of whether any feature currently exercises it. This specific discrepancy was raised in RFI-IRFOS's 13 July reply and restated in every subsequent follow-up through 4 September; no version string, build hash, or manifest excerpt was ever provided by PayPal to reconcile it.

Impact: An unexplained, unaddressed factual discrepancy between PayPal's own written review and a directly reproducible static-analysis fact undermines confidence in the review's other conclusions, independent of the permission's actual runtime use.

Fix: Either produce the manifest excerpt or build variant showing RECORD_AUDIO's absence, or correct the 12 July statement and confirm the permission's actual purpose.

H2: AD_ID plus a behavioral-biometrics fraud engine instrumenting payment flows, two vendors left unaddressed

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

AD_ID is declared alongside Adobe Marketing Cloud, Amplitude, and TransUnion iovation (62 smali classes, behavioral-biometrics fraud scoring) instrumenting payment flows.

PayPal's 12 July reply, verbatim: "PayPal does not share financial transaction data with advertising, attribution, or marketing vendors... Some transaction-related information may be processed by Datadog, which is used internally by PayPal for application monitoring, performance, and reliability purposes." Datadog is a name PayPal introduced that does not appear in RFI-IRFOS's own finding; the reply addressed only that one vendor under this finding and did not mention Adobe Marketing Cloud or Amplitude, the two vendors RFI-IRFOS had actually named.

Impact: Two named third-party vendors instrumenting payment-adjacent data flows remain unaddressed in PayPal's only substantive reply, which instead responded regarding a vendor RFI-IRFOS had not raised under this finding.

Fix: Confirm, per named vendor (Adobe Marketing Cloud, Amplitude, TransUnion iovation), what payment-flow data each receives and under what Art. 6 legal basis.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(a); PSD2 Art. 95; RTS 2018/389 Art. 22	Debug interceptor compiled into production payment binary
C2	GDPR Art. 9(1), Art. 9(2)(a), Art. 13(1)(e), Art. 28(1), Art. 46	Four undisclosed biometric sub-processors, never addressed
H1	GDPR Art. 5(1)(c)	Undisclosed permission, factually misstated as absent
H2	GDPR Art. 5(1)(b), Art. 6	Payment-flow instrumentation, two named vendors unaddressed
C3	GDPR Art. 32	Hardcoded, publicly extractable credential

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to security@paypal.com + dpo@paypal.com; noreply@paypal.com auto-replies begin on every round thereafter
2026-06-27	6-day follow-up, cc press@paypal.com added
2026-06-28	Delivery-fix resend to dpo@/privacy@, cc lux-dpo@/achriss@paypal.com, bcc CNPD Luxembourg (bounced), DSB, CERT.at
2026-07-12	PayPal's only substantive reply, JJ Thompson, Global Customer Complaints & Advocacy, ticket PP-ESC-127612042574605418, names escalation contact headofcomplaints@paypal.com
2026-07-13	RFI-IRFOS rebuttal: manifest-fact discrepancy on RECORD_AUDIO, C2 omission, escalates to headofcomplaints@paypal.com
2026-07-27 / 08-09 / 08-18 / 08-31 / 09-04	Five further written requests for correction or clarification; zero further response of any kind from PayPal, including from the named escalation contact
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Across roughly ten weeks and three parallel delivery threads, PayPal sent exactly one substantive human reply. That reply named and addressed four of the report's findings, but stated a factual claim about RECORD_AUDIO contradicted by RFI-IRFOS's own static extraction, and did not mention the four-biometric-SDK finding at all. Six subsequent written requests for correction, including to the reply's own named escalation contact, received no further response of any kind.

Residual Risk & Recommendations

- Reconcile the RECORD_AUDIO discrepancy: either produce the build evidence for its absence or correct the 12 July statement.
- Name FaceTec, MiTek MiSnap, MicroBlink BlinkID, and Daon DMDS individually as Art. 28 sub-processors with their respective Art. 46 transfer mechanisms.
- Publish the Firebase project's security-rules configuration or rotate and restrict the key.
- Remove the Chucker dependency from the production build variant entirely, and publish the build configuration confirming its exclusion.
- Confirm what payment-flow data Adobe Marketing Cloud and Amplitude specifically receive, and under what legal basis.

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 Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 9, 13, 25, 28, 32, 46; PSD2 Art. 95. REF PAYPAL-2026-R1.