Coordinated Security & Privacy Disclosure, Final Report

Badoo (com.badoo.mobile)

Dating platform, Bumble Inc., government identity document processing at scale

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, EIGHT WRITTEN NOTICES, ZERO REPLIES OF ANY KIND

Target	Bumble Inc., Austin, Texas, US (NASDAQ: BMBL)
Product audited	Badoo for Android, com.badoo.mobile, v5.471.0
Disclosure reference	REF BADOO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Veriff NFC passport biometric, CVSS v4.0 8.7 High) / C1, C3 transport security score 8.6 High

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Badoo Android application and identified seven findings, four CRITICAL, three HIGH. The most significant concern government identity documents and biometric data: Badoo integrates Au10tix for passport and national ID document processing and Veriff for NFC biometric passport-chip reading, both transmitted with zero certificate pinning anywhere in the application.

Au10tix, the identity-verification vendor Badoo relies on, had its own authentication tokens exposed for approximately seven months in 2020, an incident that granted access to customer facial scans and identity documents at the vendor level. Badoo's own transport security compounds this: no network_security_config.xml exists anywhere in the binary, meaning every document upload, every NFC passport read, and every private message is transmitted with no certificate pinning at all.

Eight written notices were sent to security@badoo.com and security@bumble.com over 91 days. None produced a reply of any kind. Two addresses used in the original notice, privacy@badoo.com and casework@ico.org.uk, hard-bounced on the first attempt. All seven findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026 to security@badoo.com and security@bumble.com, bcc Austrian DSB and CERT.at. Two originally-targeted addresses, privacy@badoo.com and casework@ico.org.uk, hard-bounced on first attempt and were dropped from every subsequent send. Seven further written notices followed through 12 September 2026. None produced a reply of any kind, not an acknowledgment, not a dispute, not a bounce explaining the silence.

ID	Severity	Title
C1	CRITICAL	Au10tix government identity document processing with zero certificate pinning
C2	CRITICAL	Veriff plus NFC passport chip reading: biometric extraction on a dating platform
C3	CRITICAL	No network_security_config.xml anywhere in the application
C4	CRITICAL	Firebase API key and database URL hardcoded in production APK
H1	HIGH	Sierra: a third-party AI customer-service agent processes identity-verification disputes
H2	HIGH	The most aggressive permission set in this research series

ID	Severity	Title
H3	HIGH	Four simultaneous ad networks monetize an identity-verified user base

Subject & Operator Analysis

Bumble Inc. (NASDAQ: BMBL, Austin, Texas) operates Badoo alongside its flagship Bumble app. Badoo's identity-verification requirements, processing government passports, national IDs, and NFC biometric chip data, place it in a materially different risk category from most consumer dating apps: a breach here would expose not just dating preferences but government-issued identity documents themselves.

Findings

C1: Au10tix government identity document processing with zero certificate pinning

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

Au10tix processes government identity documents, passports, national IDs, and proof of address, inside Badoo. Au10tix's own authentication tokens were exposed for approximately seven months in 2020, granting access to customer facial scans and identity documents at the vendor level. Badoo ships no network_security_config.xml.

No response was received naming this finding. Passport and national ID uploads on Badoo transit with no certificate pinning, meaning a network position attacker on a compromised network could intercept the same class of document data that was already exposed once, at the vendor level, in 2020.

Impact: Government identity documents uploaded to Badoo travel through a vendor with a documented prior credential-exposure incident, over a connection with no certificate pinning.

Fix: Implement certificate pinning for all Au10tix document-upload traffic and obtain written confirmation from Au10tix of current security controls following its 2020 incident.

C2: Veriff plus NFC passport chip reading: biometric extraction on a dating platform

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

Veriff, combined with NFC reading of the biometric chip embedded in modern passports (ICAO 9303), extracts the machine-readable zone, biographical data, and the chip's own stored facial image.

No response was received naming this finding. This is direct extraction of the passport chip's own biometric facial image, GDPR Art. 9(1) special category and Art. 4(14) biometric data, processed on a consumer dating application rather than a context where such verification depth is typically expected.

Impact: The biometric facial image stored in a user's passport chip is extracted and processed by a dating app's identity-verification flow.

Fix: Publish the specific Art. 9(2)(a) consent flow and Art. 35 DPIA covering NFC passport-chip biometric extraction specifically, separate from general identity-verification consent.

C3: No network_security_config.xml anywhere in the application

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

Zero certificate pinning across the entire application, confirmed by the complete absence of any network_security_config.xml file in the binary.

No response was received naming this finding. Every document upload, every NFC passport read, every AI customer-service conversation, and every private message is transmitted with no certificate pinning at all, not a partial or misconfigured implementation but a total absence.

Impact: All application traffic, including the identity-document and biometric flows named in C1 and C2, is susceptible to MITM interception on a compromised network.

Fix: Implement certificate pinning application-wide with primary and backup pins on a rotation schedule.

C4: Firebase API key and database URL hardcoded in production APK

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

A Firebase API key and database URL are hardcoded in the shipped production binary.

No response was received naming this finding.

Impact: The exposed key enables FCM token enumeration and probing against Badoo's backend independent of the app's own access controls.

Fix: Rotate the key, restrict it to the production certificate fingerprint, and enable Firebase App Check.

H1: Sierra: a third-party AI customer-service agent processes identity-verification disputes

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2

Sierra, a third-party AI customer-service agent, processes user support conversations, including disputes about passport-verification rejections.

No response was received naming this finding. Passport-rejection disputes routed through a third-party AI processor mean identity-document content and the specifics of a verification failure are shared outside Badoo's own systems, with no confirmed Art. 28 processor agreement scope specific to this data category.

Impact: Sensitive identity-verification dispute content, potentially including details of the underlying document, is processed by a third-party AI agent.

Fix: Confirm and publish the Art. 28 processor agreement scope with Sierra specific to identity-verification dispute content, and exclude document images from any AI-processed conversation where possible.

H2: The most aggressive permission set in this research series

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

DISABLE_KEYGUARD, FOREGROUND_SERVICE_CAMERA, and DOWNLOAD_WITHOUT_NOTIFICATION are all declared, none defensible for a dating application's disclosed core function.

No response was received naming this finding. DISABLE_KEYGUARD in particular grants the capability to bypass the device lock screen, a capability with no stated purpose in Badoo's own functionality.

Impact: A permission set exceeding what a dating application's stated purpose requires, including lock-screen bypass capability.

Fix: Remove DISABLE_KEYGUARD, FOREGROUND_SERVICE_CAMERA, and DOWNLOAD_WITHOUT_NOTIFICATION unless a specific, documented, user-facing feature requires each individually.

H3: Four simultaneous ad networks monetize an identity-verified user base

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, Meta Audience Network, Amazon Publisher Services, and Braze are all integrated simultaneously.

No response was received naming this finding. Behavioral signals from a user base whose identity has been verified via government documents flow to four independent commercial ad networks simultaneously.

Impact: Behavioral data from identity-verified users reaches four independent commercial advertising ecosystems simultaneously.

Fix: Consolidate ad network integrations and assess whether identity-verified status itself is being used, directly or indirectly, as an ad-targeting signal.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 9(1), Art. 32, Art. 5(1)(f)	Government ID document processing via a vendor with a prior credential-exposure incident, no cert pinning
C2	GDPR Art. 9(1), Art. 4(14), Art. 25	Biometric passport-chip facial image extraction
C3	GDPR Art. 32(1)(a)	No certificate pinning anywhere in the application
C4	GDPR Art. 32	Exposed backend credential
H1	GDPR Art. 5(1)(b), Art. 13, Art. 28	Third-party AI processing of identity-verification dispute content
H2	GDPR Art. 25	Disproportionate permission set including lock-screen bypass capability
H3	GDPR Art. 5(1)(c)	Behavioral monetization of an identity-verified user base

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@badoo.com/security@bumble.com, bcc DSB/CERT.at; privacy@badoo.com and case-work@ico.org.uk hard-bounce and are dropped
2026-06-28 / 07-03	Follow-ups, no reply
2026-08-01	42-day follow-up, no reply
2026-08-05 / 08-15 / 08-25	Continued follow-ups, no reply
2026-09-04	63-day follow-up, no reply
2026-09-12	84-day follow-up restates all seven findings and three questions, deadline 19 September 2026
2026-09-19	Embargo closes; this report publishes

Eight written notices across 91 days produced no reply of any kind. All seven findings, including government identity document processing over unpinned connections, stand exactly as originally reported.

Residual Risk & Recommendations

- Implement certificate pinning application-wide, prioritizing the Au10tix and Veriff document/biometric traffic paths.
- Confirm Au10tix's current security posture in writing following its 2020 incident.
- Publish the Art. 9(2)(a) consent flow and Art. 35 DPIA for NFC passport-chip biometric extraction specifically.
- Confirm the Art. 28 processor scope with Sierra for identity-dispute conversations.
- Remove DISABLE_KEYGUARD, FOREGROUND_SERVICE_CAMERA, and DOWNLOAD_WITHOUT_NOTIFICATION absent a specific documented purpose for each.
- Rotate the exposed Firebase credential.

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. 4, 5, 9, 13, 25,

28, 32. REF BADOO-2026-R1.