Coordinated Privacy Disclosure, Final Report

bank99 Android (at.bank99.meine.meine)

bank99 AG, Praterstraße 31, 1020 Wien, Austria

GENUINE FIRST REPLY, THEN SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO

Target	bank99, an Austrian online bank's Android app
Package	at.bank99.meine.meine
Operator	bank99 AG, Praterstraße 31, 1020 Wien, Austria
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	Austrian DSB, Austrian Financial Market Authority (FMA, banking supervisor), CERT.at
Total Outbound Messages	7, across 74 days, to datenschutz@bank99.at, cc'ing security@bank99.at, service@bank99.at, the Austrian DSB, and, from 4 August 2026, the FMA.
Inbound Replies	1 substantive reply, on 29 June 2026, from bank99's own Datenschutz team, confirming receipt and internal forwarding to relevant departments but declining to address any specific finding; 2 further replies, both automated redirects from the FMA's general public-inquiry desk, stating that this is not the correct FMA channel for this type of report. No technical answer to any of the three questions raised was ever received.

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 Seven Messages, One Genuine Reply, Two Wrong-Channel Redirects 5

4 Findings 6
- 4.1 F1: No Certificate Pinning at Any Layer on the Banking Login WebView 6
- 4.2 F2: Unsafe Content-Security-Policy on the Banking WebView 6
- 4.3 F3: Firebase API Key Hardcoded and Extractable 7
- 4.4 F4: Obfuscated Advertising-Attribution SDK, Alongside Pre-Consent Firebase Initialization, in a Banking App 7

5 Data Protection, Article by Article 8

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to bank99 AG that its Android app, a Cordova/WebView hybrid application, loads its remote banking login page (meine.bank99.at/banking/login.xhtml) into a WebView with no certificate pinning implemented at any layer: no network security configuration pin-set, no OkHttp CertificatePinner, and no Cordova SSL-pinning plugin. The login page relies entirely on default system TLS trust, meaning a compromised or misissued certificate authority in the device's trust store could intercept the entire banking session, including login credentials, in transit.

A second finding names the same WebView's Content-Security-Policy, which permits both unsafe-eval and unsafe-inline, materially weakening the WebView's own defenses against script injection even before the certificate-pinning gap is considered. A hardcoded Firebase API key and an obfuscated Adjust attribution SDK, initializing alongside a pre-consent Firebase bootstrap, round out the findings: advertising-attribution tracking with no documented legal basis or disclosed processor relationship, running inside an application whose sole purpose is banking services.

bank99's own Datenschutz team replied on 29 June 2026, four days after disclosure, confirming receipt and stating the findings had been forwarded internally for review, while declining to evaluate any specific finding or comment on the stated deadline. RFI-IRFOS acknowledged this the same day and set a written-response deadline of 9 July 2026 for the three specific technical questions raised, whether Adjust has a documented Art. 6 legal basis and processor disclosure, whether the Austrian DSB was notified under Art. 33, and whether an Art. 35 DPIA was conducted for banking-login and transaction data flowing through an unpinned WebView. That deadline, and every deadline since, passed without a technical answer. Two further replies, both from the Austrian FMA's general public-inquiry desk, arrived only to redirect RFI-IRFOS to a different, unrelated contact form, not to address the report as banking supervisor. Seven messages were sent across 74 days in total. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production bank99 Android application (at.bank99.meine.meine, version 1.0.39), as reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with bank99's backend infrastructure was performed.

Disposition

Four findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. A complete absence of certificate pinning on the app's banking login WebView, at every layer, reaches CRITICAL on the computed CVSS score alone. An unsafe Content-Security-Policy configuration on that same WebView, a hardcoded Firebase API key, and an undisclosed Adjust attribution SDK combined with pre-consent Firebase initialization all correct to MEDIUM. bank99's own Datenschutz team replied within four days confirming receipt and internal review, the only genuine engagement received; five further messages restating three specific technical questions across the following 70 days drew no further reply of any kind from bank99, and two automated redirects from the FMA's public-inquiry desk, stating the wrong channel had been used, instead of any answer from the banking supervisor itself.

ID	Severity	Title
F1	CRITICAL	No Certificate Pinning at Any Layer on the Banking Login WebView
F2	MEDIUM	Unsafe Content-Security-Policy on the Banking WebView
F3	MEDIUM	Firebase API Key Hardcoded and Extractable
F4	MEDIUM	Obfuscated Advertising-Attribution SDK, Alongside Pre-Consent Firebase Initialization, in a Banking App

Subject & Operator Analysis

bank99 is an Austrian online bank operated by bank99 AG, headquartered in Vienna, providing banking services via a Cordova/WebView hybrid Android app.

Seven Messages, One Genuine Reply, Two Wrong-Channel Redirects

This case's correspondence record includes a genuine, timely first reply, not silence from the outset. On 29 June 2026, four days after disclosure, bank99's own Datenschutz team confirmed receipt and stated the report had been forwarded internally for review, while explicitly declining to evaluate any specific finding or address the stated response deadline. RFI-IRFOS acknowledged this the same day and set a written-response deadline of 9 July 2026 for three specific technical questions. That deadline, and four further follow-up deadlines through 6 September 2026, all passed without any further reply from bank99. On 5 August 2026, two automated messages arrived from the Austrian FMA's general public-inquiry desk, cc'd from RFI-IRFOS's 4 August follow-up, stating only that consumer inquiries, complaints, and business-model questions must use a different, dedicated contact form, without addressing the report as the banking supervisor. Seven messages were sent in total across 74 days.

Findings

F1: No Certificate Pinning at Any Layer on the Banking Login WebView

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. This finding reaches CRITICAL on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

bank99's app loads its remote banking login page, meine.bank99.at/banking/login.xhtml, into a WebView with no certificate pinning at any layer: no network security configuration pin-set, no OkHttp CertificatePinner, and no Cordova SSL-pinning plugin. The login page relies entirely on default system TLS trust.

```
meine.bank99.at/banking/login.xhtml loaded into WebView
No NSC pin-set, no OkHttp CertificatePinner, no Cordova SSL-pinning plugin found
```

Impact: A compromised or misissued certificate authority present in the device's trust store, whether system, user-installed, or corporate MDM, could intercept the entire banking session, including login credentials and transaction data, in transit.

Fix: Implement certificate pinning on all layers handling the banking login and transaction WebView. No confirmation that this has occurred was ever received.

F2: Unsafe Content-Security-Policy on the Banking WebView

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 Content-Security-Policy governing the banking login WebView permits both unsafe-eval and unsafe-inline, materially weakening the WebView's own script-injection defenses independent of the certificate-pinning gap in F1.

Impact: Script-injection defenses on the banking WebView are weaker than a standard CSP configuration would provide, compounding the risk documented in F1 if an attacker achieves any injection foothold.

Fix: Remove unsafe-eval and unsafe-inline from the banking WebView's Content-Security-Policy. No confirmation that this has occurred was ever received.

F3: Firebase API Key Hardcoded and Extractable

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

A Firebase API key is hardcoded in plaintext in res/values/strings.xml, extractable from the production binary.

```
AIzaSyD8jtdT06oePLqFohurEF8yjmEopM5Jx_4
```

Impact: The key is trivially extractable, and depending on the security-rule configuration behind it, could enable unauthorized access or denial of service against legitimate users.

Fix: Restrict the Firebase API key by package name and SHA-1 certificate fingerprint. No confirmation that this has occurred was ever received.

F4: Obfuscated Advertising-Attribution SDK, Alongside Pre-Consent Firebase Initialization, in a Banking App

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.

The Adjust attribution SDK is present, obfuscated inside a generically named package, alongside FirebaseInitProvider auto-initializing before any user consent screen. No documented Art. 6 legal basis or processor disclosure for Adjust was located in bank99's privacy documentation.

Impact: Advertising-attribution tracking with no documented legal basis runs inside an application whose sole purpose is banking services, alongside analytics collection that begins before a user has consented to anything.

Fix: Document Adjust's legal basis and processor status under Art. 6(1) and Art. 28, and defer FirebaseInitProvider initialization until after consent. 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 and Austrian banking-supervision law, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32(1)(a)	F1	Complete absence of certificate pinning on banking login/transaction traffic.
Art. 32	F2	Weakened Content-Security-Policy on the same WebView.
Art. 32(1)(b)	F3	Hardcoded, trivially extractable Firebase API key.
Art. 6(1), Art. 7, Art. 13	F4	Undisclosed advertising-attribution SDK and pre-consent analytics init in a banking app.

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, F1 reaches CRITICAL on its computed CVSS v4.0 score alone, no editorial escalation applied; F2, F3, and F4 correct to MEDIUM to match their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: BANK99-2026-R1.