Coordinated Privacy Disclosure, Final Report

Sparda-Banking-App Android (de.sparda.banking.app)

Atruvia AG (formerly Fiducia & GAD), shared infrastructure across 118 German cooperative banks, ~30M customers

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE STATED EMBARGO DATE, SEVEN MESSAGES, ONE GENERIC ACKNOWLEDGMENT, ZERO SUBSTANTIVE REPLY

Target	Sparda-Banking-App, built by Atruvia AG for the German cooperative banking sector
Package	de.sparda.banking.app, version 9.0.0
Operator	Atruvia AG, shared infrastructure across 118 cooperative banks (Volksbanken, Raiffeisenbanken, Sparda-Banken), approximately 30 million customers
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-25, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, on the stated date
Regulators	BfDI (lead SA), BSI CERT-Bund, Austrian DSB, CERT.at, EDPS, Baden-Württemberg LfDI
Total Outbound Messages	7, across 48 days, to postfach@atruvia.de, datenschutz@atruvia.de, and named Atruvia staff; the original addresses at sparda.de all bounced outright.
Inbound Replies	1 generic acknowledgment from an Atruvia staff member on 2026-07-01, stating the matter was under review, addressing none of the four findings by name. No further reply of any kind was ever received.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Atruvia AG, the shared technology provider behind the Sparda-Banking-App and the wider German cooperative banking sector, that its Android banking app has no certificate pinning at any layer, no network security configuration file, an OkHttp CertificatePinner class present but with zero configured pins across all three DEX archives, and no custom pinning plugin. The app's own TrustManager validates correctly, but without app-side pinning, a compromised or fraudulently issued CA certificate can intercept the entire banking session. This is the single most severe finding in this report, computing to CRITICAL on its own CVSS band before any editorial adjustment.

A second finding names LexisNexis ThreatMetrix BehavioSec, a behavioral biometrics SDK that captures keystroke dynamics, swipe gestures, and sensor data through JavaScript injection into the app's full-screen banking WebView, transmitting this data via HTTP POST to LexisNexis servers in Georgia, USA. All four TMX modules load via Java ServiceLoader on every app start. Static analysis found zero references to OneTrust, the app's own consent management platform, anywhere in the relevant integration packages: the behavioral profiling runs independently of consent status entirely. Keystroke and swipe-gesture dynamics are biometric data under Art. 4(14) GDPR and EDPB Guidelines 01/2023, and the US transfer requires Art. 46 safeguards that RFI-IRFOS found no evidence of.

Two further findings round out the disclosure: the AD_ID permission is actively read, with AppsFlyer's SDK explicitly calling setAdvertisingIdWithGps(true), and a shared string linking AppsFlyer and Adobe Experience Platform indicates the two SDKs share a joint data profile, on a banking application; and a hardcoded Firebase API key alongside a FirebaseInitProvider that initializes before any consent dialog. Genuine positives are worth naming: the app integrates established security SDKs (Encap/Thales, Giesecke+Devrient for NFC, Auth0, Data Theorem, Dynatrace), its TrustManager validates correctly, and its SDK targeting shows active technical-debt reduction. OneTrust is present and correctly integrated as infrastructure, the specific failure is that it and ThreatMetrix BehavioSec are simply not connected, an architectural decision at the Atruvia level, not an individual developer's implementation error.

Seven messages were sent across 48 days, to postfach@atruvia.de, datenschutz@atruvia.de, and named Atruvia staff, after the original sparda.de addresses all bounced outright. A single reply arrived on 1 July, a generic acknowledgment stating the security of Atruvia's applications was a top priority and that the matter was under review; it did not name a single one of the four findings, and no further reply of any kind followed it across six subsequent messages and 48 additional days. The 90-day embargo, stated directly to the target in the initial disclosure, elapses today. This report and the accompanying closure notice publish on the stated date. The Adobe Launch configuration embedded in the APK lists 118 distinct bank IDs, meaning a fix at the Atruvia level protects millions of customers across the entire cooperative banking network at once.

Scope: Root-level static analysis of the production Sparda-Banking-App Android application (de.sparda.banking.app, version 9.0.0, SHA-256 63fd9c2988b38bc6c8574161c0bd6e7bb02fa02b8582d3a05699b6e0d74bea86), pulled from Google Play and reviewed on 25 June 2026, including full decompilation of all three DEX archives and manual smali-level analysis. No account was created and no interaction with LexisNexis's, AppsFlyer's, Adobe's, or Firebase's backend infrastructure was performed.

Disposition

Four findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. The absence of certificate pinning at any layer of a banking application reaches CRITICAL/9.1 on its own computed band without escalation. Behavioral biometric data collection with no consent gate, transmitted to a US third party, reaches HIGH/8.7 on its own computed band. Advertising-ID and attribution SDK use, and a hardcoded, pre-consent Firebase key, both correct to MEDIUM. Seven messages were sent across 48 days. One generic acknowledgment was received on the seventh day, stating the matter was under review; it named none of the four findings and no further reply of any kind followed it.

ID	Severity	Title
F1	CRITICAL	No Certificate Pinning at Any Layer of a Banking Application
F2	HIGH	Behavioral Biometric Data Collected With No Consent Gate, Transmitted to the US
F3	MEDIUM	Advertising ID and Attribution SDK Use on a Banking Application
F5	MEDIUM	Hardcoded Firebase Key With Pre-Consent Initialization

Subject & Operator Analysis

The Sparda-Banking-App is built and maintained by Atruvia AG (formerly Fiducia & GAD IT AG) for the entire German cooperative banking sector. The Adobe Launch configuration embedded in the APK lists 118 distinct bank IDs, meaning the app's shared infrastructure spans Volksbanken, Raiffeisenbanken, and Sparda-Banken, approximately 30 million customers, and a fix at the Atruvia level protects all of them at once. The Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) is the lead supervisory authority for a finding of this scale.

Genuine positives are worth naming. The app integrates established security SDKs, Encap Security/Thales and Giesecke+Devrient for NFC, Auth0, Data Theorem App Secure, and Dynatrace. Its TrustManager validates certificates correctly at the code level. targetSdk 36 and minSdk 29 show active technical-debt reduction. OneTrust is present and correctly integrated as consent-management infrastructure, the specific gap named in F2 is that ThreatMetrix BehavioSec simply is not wired into it, an architectural decision at the Atruvia level, not an individual developer's oversight.

Seven Messages, One Generic Acknowledgment, Zero Substantive Reply

The original addresses at sparda.de, datenschutz@sparda.de, presse@sparda.de, and info@sparda.de, all bounced outright on the first attempt. postfach@atruvia.de, datenschutz @atruvia.de, and named Atruvia staff accepted delivery for the remaining messages, copying the BfDI, BSI CERT-Bund, the Austrian DSB, CERT.at, the EDPS, and Baden-Württemberg's LfDI throughout. A single reply arrived on 1 July 2026 from an Atruvia staff member, stating that the security of Atruvia's applications and the protection of its customers were of the highest priority and that the matter was under review. It named none of the four findings specifically. No further reply of any kind followed it across the subsequent six messages and 48 additional days.

Findings

F1: No Certificate Pinning at Any Layer of a Banking Application

CRITICAL, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.1.

No network security configuration file is present. OkHttp's CertificatePinner class is present in the binary but configured with zero SHA-256 pins across all three DEX archives. No Cordova plugin or custom pinner supplies pinning either. The app's own TrustManager validates certificates correctly, but with no app-side pinning, a compromised or fraudulently issued CA certificate can intercept the entire banking session.

```
network_security_config.xml: not present
OkHttp CertificatePinner class: present, 0 configured pins across 3 DEX archives
Benchmark: Deutsche Bank uses TrustKit with 3 pins including backup
```

Impact: A single compromised or fraudulently issued certificate authority, a real and documented threat category, can intercept banking traffic for an app used across 118 banks and approximately 30 million customers with no app-level defense in place.

Fix: Implement certificate pinning (TrustKit or equivalent) with at least one primary and one backup pin per domain. No confirmation that this has occurred was ever received.

F2: Behavioral Biometric Data Collected With No Consent Gate, Transmitted to the US

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.

LexisNexis ThreatMetrix BehavioSec loads all four modules via Java ServiceLoader on every app start, capturing keystroke and touch dynamics, accelerometer and gyroscope data, inside the app's full-screen banking WebView, which is the banking interface itself, not a hidden iframe. Data is transmitted via HTTP POST to LexisNexis servers in Alpharetta, Georgia. Static analysis found zero references to OneTrust, the app's own consent management platform, anywhere in the relevant integration packages.

```
TMXBehavioSecInitializer, TMXSensorsInitializer, TMXAuthenticationInitializer,
    TMXDeviceSecurityHealthInit
TMXWebView: fill_parent x fill_parent (the banking interface itself)
zero OneTrust references in integration packages JlPcMZIbV/, JFVNSLdBT/
```

Impact: Keystroke and swipe-gesture dynamics are biometric data under Art. 4(14) GDPR, collected and transmitted to a US processor with no consent gate and no documented Art. 46 transfer safeguard, on a banking application shared across 118 institutions.

Fix: Wire ThreatMetrix BehavioSec initialization into the existing OneTrust CMP status, and document the Art. 46 transfer mechanism covering LexisNexis. No confirmation that this has occurred was ever received.

F3: Advertising ID and Attribution SDK Use on a Banking Application

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.

AD_ID is declared and actively read. AppsFlyer's SDK explicitly calls setAdvertisingIdWithGps(true). ACCESS_ADSERVICES_ATTRIBUTION is additionally declared. A shared string (android_adobe_mobile) links AppsFlyer and Adobe Experience Platform, indicating the two SDKs share a joint data profile.

```
AFe1fSDK.smali: setAdvertisingIdWithGps(true)
ACCESS_ADSERVICES_ATTRIBUTION declared
Shared identifier: android_adobe_mobile (AppsFlyer <-> Adobe)
```

Impact: Advertising attribution infrastructure with GPS-augmented device identification, shared across two marketing platforms, is present in a banking application where users would not expect advertising-attribution tracking.

Fix: Remove advertising-attribution SDKs from the banking app, or document a specific, disclosed purpose for their presence. No confirmation that this has occurred was ever received.

F5: Hardcoded Firebase Key With Pre-Consent Initialization

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.

A Firebase API key is hardcoded in res/values/strings.xml. FirebaseInitProvider is declared with initOrder=100, initializing before any consent dialog.

```
google_api_key: AIzaSyBq9Maj6BYTimDgoqv8ESMV4mvvhjPvVyM
FirebaseInitProvider: initOrder=100
```

Impact: An extractable key enables quota-exhaustion denial of service and data access if Firebase security rules are weak, and pre-consent initialization means tracking infrastructure activates before any consent mechanism runs.

Fix: Restrict the key by package name and certificate fingerprint, enforce App Check, and confirm deny-by-default rules; gate initialization behind 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, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32	F1	No certificate pinning at any layer of a banking application.
Art. 9, Art. 44, Art. 46	F2	Behavioral biometric data collected with no consent gate, US transfer.
Art. 6, Art. 7	F3	Advertising-ID and attribution SDK use on a banking application.
Art. 32	F5	Hardcoded Firebase key with pre-consent initialization.

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 corrects to CRITICAL and F2 corrects to HIGH, both on their own computed bands. F3 and F5 correct to MEDIUM on their own computed

bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF #S-2026-031-A.