Coordinated Security & Privacy Disclosure, Final Report

Revolut for Android (com.revolut.revolut)

Licensed EU bank, largest app in the research series, one paragraph declaring six findings unfounded, a disclosure reclassified as a data subject access request

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE PARAGRAPH TWICE, THEN RECLASSIFIED AS A DSAR

Target	Revolut Bank UAB, Vilnius, Lithuania
Product audited	Revolut for Android, com.revolut.revolut v10.134
Disclosure reference	Case 12973-74394-83287
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase credentials, 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

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Revolut Android application, the largest app in this year's research series at 224MB, and identified six findings, two CRITICAL, four HIGH. The most significant, in RFI-IRFOS's assessment: Mesh Connect, 145,916 classes, the largest single third-party SDK identified in the entire 2026 audit series by a factor of 23, is integrated at the core banking data-model level, with named bidirectional mappings covering external card data, creditor details, beneficiary fields, and QR top-up data.

Firebase production credentials remain hardcoded and valid in every distributed copy of the app, notwithstanding Revolut's position that the referenced database has been deactivated. A dual biometric KYC stack, Onfido plus Fourthline plus two further NFC passport-reading libraries, gives the app four separate components capable of reading NFC chip data from passports.

Revolut's data protection function redirected the disclosure as out of scope within minutes of receipt. Its security function later declared, in an identical paragraph sent twice, that all findings were 'thoroughly assessed' and posed no active concern, without naming or technically rebutting any of six specific artifact-backed items. Revolut's final reply, on 4 September, characterized the entire disclosure as a data subject access request and stated it had no further information to provide. All six findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026 to Revolut's data protection team. Within minutes, Data Protection Support redirected the disclosure as out of scope for its function and pointed to a Responsible Disclosure form. Revolut Information Security later sent an identical paragraph, twice, on 21 July and 6 August, declaring all findings unfounded without naming, quoting, or technically addressing a single one of six specific artifact-backed items. On 4 September, Revolut's final reply reclassified the entire disclosure as 'your data subject access request dated 20 June' and stated it had no further information to provide.

ID	Severity	Title
C1	CRITICAL	Firebase production credentials hardcoded, live in every distributed copy
C2	CRITICAL	FOREGROUND_SERVICE_MEDIA_PROJECTION with no disclosed purpose
H1	HIGH	Mesh Connect: the largest third-party SDK in the 2026 research series, integrated at the core banking data-model level
H2	HIGH	Dual biometric KYC stack: four components capable of reading passport NFC chip data

ID	Severity	Title
H3	HIGH	QUERY_ALL_PACKAGES: full installed-app inventory, not disclosed
H4	HIGH	HIGH_SAMPLING_RATE_SENSORS and accelerometer capture during biometric login

Subject & Operator Analysis

Revolut Bank UAB (Vilnius, Lithuania) is a licensed EU bank offering multi-currency accounts, cards, and payment services, supervised for data protection by the Lithuanian Valstybine duomenu apsaugos inspekcija (VDAI).

Positive Observations

- No Chucker interceptor or FullStory session replay was identified, unlike several other financial applications in this year's audit series.
- cleartextTrafficPermitted is set to false.
- DETECT_SCREEN_RECORDING and DETECT_SCREEN_CAPTURE are both present, a positive defensive security practice RFI-IRFOS credits explicitly.

Findings

C1: Firebase production credentials hardcoded, live in every distributed copy

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

API key AIzaSyDiKkgOnh8Rhw_Fn0lePCYFHCzVeoK5hEg, Firebase App ID 1:641524086291:android:5bb8674918564983, database revolut-server.firebaseio.com, extracted from the production binary.

Revolut's position, stated in its 21 July and 6 August replies (identical paragraph, both instances): 'none of the identified items pose an active security vulnerability or data protection concern.' RFI-IRFOS's standing question, restated in every follow-up through 4 September: has this key been rotated as of today, yes or no? Revolut's own reply states the referenced database has been deactivated, but the key itself remains valid and extractable from every distributed copy of the app regardless of that database's status. No reply has confirmed the key's actual rotation state.

Impact: A live, publicly extractable key on a licensed bank's largest application enables probing and enumeration attacks regardless of one specific database's deactivation status.

Fix: Confirm the key's rotation status directly, and rotate and restrict any active replacement to the production certificate fingerprint.

C2: FOREGROUND_SERVICE_MEDIA_PROJECTION with no disclosed purpose

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 foreground media-projection service permission is declared. No screen-sharing or co-browsing SDK was identified in the binary that would explain this capability, distinguished from the two defensive permissions also present, DETECT_SCREEN_RECORDING and DETECT_SCREEN_CAPTURE, which RFI-IRFOS credits as positive security practice.

Not individually named in either of Revolut's two identical 'thoroughly assessed' replies. RFI-IRFOS's standing question, restated in every follow-up through 4 September: which shipped feature uses this permission, and where is that disclosed to users?

Impact: A media-projection capability with no identified corresponding feature or user-facing disclosure represents an undisclosed screen-capture-adjacent capability on a banking app.

Fix: Name the specific feature requiring FOREGROUND_SERVICE_MEDIA_PROJECTION, or remove the permission if unused.

H1: Mesh Connect: the largest third-party SDK in the 2026 research series, integrated at the core banking data-model level

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

145,916 Mesh Connect classes, roughly 23 times the size of the next-largest third-party SDK identified across the entire 2026 audit series, integrated with named bidirectional data-model mappings.

```
ExternalCardEntity      <-> com.meshconnect.link.ta1.h
CreditorEmbeddedEntity  <-> com.meshconnect.link.wca.a
BeneficiaryFieldsDto    <-> com.meshconnect.link.ma1.i
PayNowTopUpQrDto        <-> com.meshconnect.link.ib1.a
```

Not individually named in either of Revolut's two identical replies.

Impact: A US third-party SDK integrated at the core financial data-model level, covering card, creditor, and beneficiary data, with no confirmed Art. 44 transfer safeguard, represents a substantial, largely undocumented data-sharing surface.

Fix: Disclose Mesh Connect as a named Art. 28 sub-processor with its Art. 46 transfer mechanism, scoped to the specific data-model mappings identified.

H2: Dual biometric KYC stack: four components capable of reading passport NFC chip data

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

Onfido (4,058 classes, facial liveness and document capture) and Fourthline (5,777 classes, NFC passport chip reading), plus jMRTD (228 classes) and devnied (64 classes), two further NFC travel-document libraries.

Not individually named in either of Revolut's two identical replies. RFI-IRFOS's standing question, restated in every follow-up through 4 September: has an Art. 36 DPIA been conducted for this dual biometric stack, and by whom?

Impact: Four separate components capable of reading Art. 9 biometric passport data operate without a confirmed DPIA, on a platform combining two independently sufficient KYC vendors.

Fix: Confirm and publish the Art. 36 DPIA covering this data flow, and clarify why two independently complete KYC pipelines are both present.

H3: QUERY_ALL_PACKAGES: full installed-app inventory, not disclosed

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

QUERY_ALL_PACKAGES is declared, granting visibility into the device's full installed-application inventory, not disclosed in Revolut's privacy notice to RFI-IRFOS's knowledge.

Not individually named in either of Revolut's two identical replies.

Impact: A full installed-app inventory can support device fingerprinting or fraud-signal inference beyond what a banking app's stated purpose discloses.

Fix: Disclose the specific use case for QUERY_ALL_PACKAGES under Art. 13, or remove it if unused.

H4: HIGH_SAMPLING_RATE_SENSORS and accelerometer capture during biometric login

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

High-sampling-rate accelerometer data is captured during the login flow, named strings accelerometerFlow, accelerometerTimestamp, revolut_sso_login_biometric_prompt_biometric_sensor.

Not individually named in either of Revolut's two identical replies. RFI-IRFOS's standing question, restated in every follow-up through 4 September: is this data retained, transmitted to any third party, or used in behavioral-biometric profiling?

Impact: High-frequency motion-sensor data captured during login may constitute Art. 9(1) behavioral-biometric data depending on its retention and downstream use, neither of which Revolut has disclosed.

Fix: Disclose the retention period, transmission destination, and processing purpose for accelerometer data captured during login.

Revolut's Response, Recorded in Full

Within minutes of the original disclosure on 20 June 2026, Revolut's Data Protection Support team (Leo) replied: "It seems that your query is out of the scope of the data protection area. I'm afraid we are unable to support further on this matter. If you wish our technical teams to review you report, please find all the information about our Responsible Disclosure Program and report this issue with the form available here."

On 21 July and again on 6 August, Revolut Information Security sent the identical paragraph, in full: "Our Information Security and Data Protection teams, including Financial Crime and Mobile Security specialists, have comprehensively triaged, reviewed, and evaluated all the findings detailed in your submission. Following this formal internal assessment, we can confirm that none of the identified items pose an active security vulnerability or data protection concern for Revolut or our customers or partners. The permissions, configuration keys, and SDK integrations cited within your report operate strictly as intended and fully align with our security architecture and compliance frameworks... we now consider this case finalised and closed." Signed only "Revolut Information Security," no individual name given, sent word for word identical on both dates.

On 4 September 2026, Revolut's final reply, signed "Leo, Data Protection Support," stated in full: "We have no further information to provide in relation to your data subject access request dated 20 June. If you're not satisfied with our answer, you have the right to make a complaint at any time to your local data protection authority." RFI-IRFOS's original submission on 20 June was a security and GDPR findings disclosure covering six specific technical items, not a data subject access request, which by definition concerns one identified individual's own personal data rather than an app-wide design and configuration audit.

None of the six findings named in this report was individually addressed, quoted, or technically rebutted in any Revolut reply at any point across the 91 day correspondence.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Hardcoded, live production credential
C2	GDPR Art. 13, Art. 5(1)(b)	Undisclosed media-projection capability
H1	GDPR Art. 44, Art. 13(1)(e)(f)	Largest SDK in the research series, core financial data-model integration
H2	GDPR Art. 9(1), Art. 36	Dual biometric passport-reading stack, DPIA not confirmed
H3	GDPR Art. 5(1)(c), Art. 13	Undisclosed full installed-app inventory access
H4	GDPR Art. 9(1), Art. 13	Undisclosed behavioral-biometric-adjacent sensor capture

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent, case 12973-74394-83287 opened; 6 findings
2026-06-21	Data Protection Support (Leo): out of scope, redirects to Responsible Disclosure form
2026-06-26 / 06-29	Under-investigation acknowledgment; DPO states no visibility into the technical review
2026-07-21	Revolut Information Security: identical 'thoroughly assessed... finalised and closed' paragraph, first instance
2026-08-06	Same paragraph sent again, word for word, in reply to RFI-IRFOS's R2 restating six open questions
2026-08-15 / 08-24	Follow-ups restate all six findings by name; no further reply
2026-09-04	Final reply reclassifies the disclosure as a data subject access request, states no further information available
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Across 91 days, Revolut's data protection function redirected the disclosure within minutes, its security function sent the same one-paragraph blanket dismissal twice without naming any of six findings individually, and its final reply reclassified the entire matter as a data subject access request. No named individual beyond a single first name, Leo, appeared anywhere in the correspondence, and no finding received a specific, technical answer.

Residual Risk & Recommendations

- Confirm the Firebase key's actual rotation status directly, independent of the referenced database's deactivation.
- Name the specific feature requiring FOREGROUND_SERVICE_MEDIA_PROJECTION or remove the permission.
- Disclose Mesh Connect as a named Art. 28 sub-processor with its Art. 46 transfer mechanism.
- Publish the Art. 36 DPIA covering the dual biometric passport-reading KYC stack.
- Disclose the retention and processing purpose of accelerometer data captured during login.
- Route future security and regulatory disclosures to a function equipped to answer them technically, rather than reclassifying them as customer data requests.

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, 32, 36, 44. REF REVOLUT-2026-R1.