Security & Privacy Disclosure, Final Report

Truecaller: Trusted Caller ID for Android (com.truecaller)

A phonebook upload counter next to a store claim, a general unreachable-code reply that names no finding, and three questions that stay open.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 20 NOVEMBER 2026. ONE GENERAL REPLY OF 18 SEPTEMBER 2026 AND AUTOMATED TICKETS ONLY, NO ITEMISED ANSWER.

Target	True Software Scandinavia AB (Truecaller)
Versions Audited	26.32.7 / 2632007 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	10: 1 Critical, 2 High, 4 Medium, 1 Low, 2 observations (C2, H3, H4, M2 reassessed, M3 and M4 observations)
Status	GENERAL REPLY 18 SEPTEMBER 2026, NO ITEMISED REPLY AS OF 21 NOVEMBER 2026. Automated ticket only after the notice of 15 November 2026
SHA-256 (base APK)	`c8ac7ae6e684d5c9625412d5e0f417db335d3b5f27e4a7b818d8619f6d3e9406`

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 7

5 Engagement Summary and Response Pattern Analysis 8

6 Findings 10
- 6.1 C1: Phonebook upload counter next to a store claim of no upload 10
- 6.2 C2: A noneu hostname pattern on OTP verification and telephony hosts 12
- 6.3 H1: Huawei and Mintegral components registered in the manifest 13
- 6.4 H2: Five providers start SDKs before consent and subscription checks 14
- 6.5 H3: Exported account-state provider with a normal-level permission 15
- 6.6 H4: AI Call Scanner analyses the voice of a call counterparty 16
- 6.7 M1: Firebase and Google API key hardcoded in strings.xml 17
- 6.8 M2: Cleartext allowed for two TCPay domains, no pinning 18
- 6.9 M3: Notification listener service registered 19
- 6.10 M4: Family Protection Admin and Member services 20

7 Impact Analysis 20

8 The Complete Chain 21

9 Inference Data, Bystanders and Control 22

10 Consumer Protection & Platform Disclosures 22

11 Data Protection: Article by Article 23

12 Regulatory & Legal Landscape 23

13 Indicators of Compromise & Reproducible Evidence 24

14 Disclosure Timeline & Outcome 24

15 What Truecaller Got Right 25

16 Residual Risk & Recommendations 26

Executive Summary

Truecaller: Trusted Caller ID is a caller identification, spam blocking and dialer application that Google Play lists with more than one billion downloads. It is published by True Software Scandinavia AB. On 22 August 2026 RFI-IRFOS sent ten scored findings, one unscored note on the permission surface and three questions from a root level code analysis of version 26.32.7 under REF TRUECALLER-2026-R1.

The lead finding is in the app's own telemetry. An event schema named AppUgcUpload counts the contacts in the phonebook, the contacts identified for upload and the contacts actually uploaded, with an upload type of Initial and a code path named tagsPhonebookForcedUpload. The Play listing says that Truecaller does not upload the phonebook. The people counted are the contacts of every installer, who never saw a Truecaller screen. Further findings cover five providers that start advertising and analytics SDKs before any consent screen and on the devices of paying Premium subscribers, Huawei and Mintegral components in the manifest, a hostname pattern marked "-noneu" on the verification flow that partner apps embed, an exported provider with a weak permission, and a voice classifier for the other party on a call.

Truecaller answered once, on 18 September 2026. The reply concludes that no personal data breach occurred, describes unreachable code in builds in general terms, states that the release process was strengthened, declines to share compliance documents including any impact assessment, and points to a security.txt programme. It names no finding and no component. The notice did not allege a breach, and manifest-registered components are instantiated by the operating system. RFI-IRFOS asked for an itemised reply by number or a written statement of declining on 18 September, on 17 October and on 15 November 2026. None has arrived. The only message after the follow-up of 15 November 2026 is an automated ticket confirmation (ticket 6460053).

This report separates what the package shows from what only the operator can say. The package shows that the pipeline, the hosts and the features are built. It does not show that they run for EEA users. Three questions carry that open part: the legal basis for non-user contacts, the Article 46 safeguard for EEA phone verification, and a DPIA for the voice classifier. Compared with the notice, four severities are lower here and two items are recorded as observations.

Scope: Root level code analysis of the Google Play release 26.32.7 (versionCode 2632007) as an XAPK from a mirror, matched to the mirror's published hash: resources decoded without sources, the dex string pool and the Avro schema strings searched by byte offset. The live Play listing was read on 21 and 22 August 2026. No Truecaller server was contacted, no account was created, the Firebase key was not tested and no runtime instrumentation was used. No control flow analysis was performed. Where one would be needed the finding says UNVERIFIED.

ID	Severity	Title
C1	CRITICAL	Phonebook upload counter next to a store claim of no upload
C2	MEDIUM	A noneu hostname pattern on OTP verification and telephony hosts
H1	HIGH	Huawei and Mintegral components registered in the manifest
H2	HIGH	Five providers start SDKs before consent and subscription checks
H3	MEDIUM	Exported account-state provider with a normal-level permission
H4	MEDIUM	AI Call Scanner analyses the voice of a call counterparty
M1	MEDIUM	Firebase and Google API key hardcoded in strings.xml
M2	LOW	Cleartext allowed for two TCPay domains, no pinning
M3	INFO	Notification listener service registered
M4	INFO	Family Protection Admin and Member services

ID	Sent 22 Aug	This report	Basis

Finding Status at a Glance

The table shows the severity sent in the first notice of 22 August 2026 next to the severity in this report. Six labels differ. C2, H3, H4 and M2 are lower because the evidence supports a lower band, and M3 and M4 are recorded as observations. No label changed because of a statement by Truecaller. The notice also carried an eleventh item, L1 (listed in the notes as LOW or INFO), the size of the permission and exported-component surface (93 permissions, 56 exported components), which was noted for completeness and never scored. It is described under Architecture.

ID	Sent 22 Aug	This report	Basis
C1	CRITICAL	CRITICAL	CVSS 5.9, raised by blast-radius escalation. Upload pipeline confirmed in the string pool, execution for EEA devices not observed.
C2	CRITICAL	MEDIUM	CVSS 6.3. Routing logic of the -noneu hosts is unverified.
H1	HIGH	HIGH	CVSS 6.3, raised by blast-radius escalation. Manifest-registered, data reach not shown.
H2	HIGH	HIGH	CVSS 6.9, raised by blast-radius escalation. Manifest-registered providers, data transmission not observed.
H3	HIGH	MEDIUM	CVSS 4.8. Content returned by the provider was not examined.
H4	HIGH	MEDIUM	CVSS 2.1, raised one band by blast-radius escalation. Legal basis question for non-user voices.
M1	MEDIUM	MEDIUM	CVSS 6.3. Key exposure, rules not examined.
M2	MEDIUM	LOW	CVSS 2.3. Cleartext limited to two asset domains.
M3	MEDIUM	INFO	Capability only, scope not established.
M4	MEDIUM	INFO	Disclosed opt-in feature, no adverse finding asserted.

Subject & Operator Analysis

Truecaller: Trusted Caller ID (package com.truecaller) is a caller identification, spam blocking and dialer application. The copyright string in res/values/strings.xml (settings_about_copyright_title) reads ”Copyright © True Software Scandinavia AB. All rights reserved.” The Google Play listing shows the developer Truecaller, more than 1 billion downloads, ratings of 4.3 to 4.4 stars from 29.2 million reviews, the category rank 7 in top grossing communication, an update on 14 August 2026, in-app purchases and ads, and the content rating ”Parental Guidance Recommended, Users Interact, In-App Purchases”. The Data Safety label says that the app may share Device or other IDs with third parties and may collect Location, Personal info and 9 other types, that data is encrypted in transit, that deletion can be requested and that an independent security review exists. These values were captured on 21 and 22 August 2026.

True Software Scandinavia AB is confirmed as the operator by the binary and by the APKMirror developer categorisation. The name indicates a Swedish company. The registered address and the data protection officer were not found in the binary and were not verified live, and both are UNVERIFIED. The lead supervisory authority would be the Swedish Integritetsskyddsmyndigheten (IMY) if the main establishment is in Sweden. That is an inference and was not confirmed against a registry.

Item	Value
Package	com.truecaller
Version	26.32.7 (versionCode 2632007)
XAPK SHA-256	b2d6994237ba302f48bc54b537ebf01e9a99812edcf9ae4f1a7f047eb385b210
base.apk SHA-256	c8ac7ae6e684d5c9625412d5e0f417db335d3b5f27e4a7b818d8619f6d3e9406
Signing certificate SHA-1	0ac1169ae6cead75264c725febd8e8d941f25e31 (per APKPure verification)
Size	XAPK 91,734,140 bytes, base.apk 75,227,310 bytes
Code base	9 dex files (classes.dex to classes9.dex) plus assets/audience_network.dex
Source of the package	APKPure mirror. The XAPK hash matches the hash that the mirror publishes. The app was not installed on the audit device
Support contact	support@truecaller.com (confirmed in strings.xml and the only address confirmed for the notice)
Data Protection Officer	Not found. UNVERIFIED

Architecture & Data Flow

The analysis decoded resources only (apktool without sources) and searched the dex string pool and the Avro schema strings by byte offset. No smali pass and no control flow analysis was run, and where such a pass would be needed the finding says UNVERIFIED. The decompile intermediates were deleted during the session to free disk space, and the reference copies of AndroidManifest.xml, strings.xml and network_security_config.xml are kept in the case archive.

Layer	Observed	Source
Phonebook and call data	READ_CONTACTS, WRITE_CONTACTS, READ_CALL_LOG, WRITE_CALL_LOG, call screening service, AppUgcUpload schema and sync methods	Manifest, classes7.dex
Dialer role	set_as_default_caller_id_app_in_setting and set_as_default_phone_app_in_setting strings, CALL_PHONE, ANSWER_PHONE_CALLS, PROCESS_OUTGOING_CALLS, MANAGE_OWN_CALLS	strings.xml, Manifest
Spam pipeline	AppBlockingAction schema, reportSpam, SpamReportColors, inReportSpamList, inTopSpammerList	Dex string pool
Voice features	AI Call Scanner, Custom Voice, call recording	strings.xml, dex
Third-party SDK surface	OTP verification SDK for partner apps, 12 or more ad and attribution SDKs, Huawei and Mintegral components	Manifest, dex
Backends	-noneu hosts, privacy-policy-eu, tc-images-eu bucket, Firebase project truecallerapis	String pool, strings.xml
Consent	IAB TCF v2 and Google UMP stack	Dex
Family features	Family Protection Admin and Member services	Dex
Surface size	93 uses-permission declarations (including RECORD_AUDIO, CAMERA, ACCESS_FINE_LOCATION, ACTIVITY_RECOGNITION, BLUETOOTH_SCAN, USE_BIOMETRIC, AD_ID, READ_SMS, WRITE_SMS, SEND_SMS) and 56 exported components. This matches the feature breadth of dialer, SMS, VoIP, call recording, payments, family safety and ads, and is not rated on its own	Manifest

Engagement Summary and Response Pattern Analysis

The notice went on 22 August 2026 at 14:19 UTC to support@truecaller.com with the Datenschutzbehörde and the European Data Protection Supervisor in copy. Truecaller's ticket system answered within 20 seconds with ticket 6022352 and a standard intake text that asks for screenshots and the phone number of the account. One substantive message came from Truecaller on 18 September 2026 at 08:33 UTC, 27 days after the notice, signed with a first name, from the same support address. It is the only message of substance in the thread. The table sets each statement of that reply against what it addresses and what it leaves open.

Statement of 18 Sep 2026	What it addresses	What it leaves open
″No evidence of a personal data breach″	Whether personal data was compromised by unauthorised access or disclosure.	The notice did not allege a breach. It concerned lawful basis (C1), transfer safeguards (C2), consent timing (H2) and special-category processing (H4).
Code can be present in a build but ″not reachable at runtime″, built from shared libraries and generated schema classes	A general distinction between presence, reachability and processing, which is a fair distinction.	No finding is named and no class, provider or file is said to be unreachable. Manifest-registered items (H1 components, the five H2 providers, the H3 provider) are instantiated by the operating system. M2 is a configuration file and M1 is a resource. Only the dex-string-only items can be unreachable.
Dead-code elimination strengthened and a verification step added to the release process	A change to the build that is aimed at the kind of code reported.	The weekly comparison of shipped builds is the test of this statement. The case folder holds no recorded result of such a comparison.
Where features that process personal data are activated in the EEA, GDPR obligations are met, including DPIAs and transfer assessments	A general assurance with a condition (″where activated″).	It does not say whether AppUgcUpload, the -noneu routing or AI Call Scanner are activated in the EEA. The three questions of the notice ask exactly that.
Internal compliance documentation, including any DPIA, will not be shared	The operator's choice not to disclose documents.	Question 3 (a DPIA for AI Call Scanner) therefore remains open on the record.

Statement of 18 Sep 2026	What it addresses	What it leaves open
Findings may be submitted through the security.txt programme for ”recognition or compensation”	A redirect to a separate channel.	The disclosure here follows ISO/IEC 29147 and a fixed timetable. The thread contains no submission through that channel.

RFI-IRFOS answered on 18 September 2026 at 10:07 UTC and named two patterns, a response that answers a question not asked and runtime language applied to manifest-registered findings. It restated the three questions unchanged, noted the refusal to share a DPIA without dispute, and asked for an itemised reply to C1, C2, H1 to H4 and M1 to M4 by number or a written statement of declining. A follow-up of 17 October 2026 repeated the three questions and the open items, and a third follow-up of 15 November 2026 repeated them five days before the publication date. No message from Truecaller beyond an automated ticket confirmation is in the thread as of 21 November 2026. This report does not claim that the reply is wrong on every point. It records that none of the ten items was addressed by its number.

Findings

C1: Phonebook upload counter next to a store claim of no upload

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 (CVSS-B), editorial severity CRITICAL

classes7.dex contains an Avro event schema named AppUgcUpload (namespace com.truecaller.tracking.events, documented purpose "Event logged on pre installs") with the fields contactsInPhonebook, contactsIdentified, contactsUploaded and includeNames, an upload type of Normal, Initial or TagReset, and a result of Proceeded, Disabled or Skipped. The same string pool holds the names .syncContactByUri(, SyncContactsResult(createdContactIds= and tagsPhonebookForcedUpload. The Google Play listing states: "Truecaller does not upload your phonebook & does not make your phonebook public or searchable." A mirror copy of the same text reads: "Truecaller does not upload your phonebook to make it public or searchable." The two wordings differ in what they exclude, and the binary shows an instrumented upload pipeline with a counter for contacts actually uploaded. What the pipeline sends for an EEA installer (numbers only, or numbers with names), and whether the Initial upload runs before or after any consent screen, was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.9 to CRITICAL because the pipeline sits in an app that Google Play lists with more than 1 billion downloads, and the people whose names and numbers are counted for upload are the contacts of every installer, who never saw a Truecaller consent screen and have no relationship with the operator.

```
{"name":"result","type":"string","doc":"The result of the upload (Proceeded|Disabled|
    Skipped)"},
{"name":"type","type":"string","doc":"The type of the upload (Normal|Initial|TagReset)
    "},
{"name":"installerPackageName","type":"string","doc":"The app package name - used to
    check if app wa
    s installed from play store"},
{"name":"buildName","type":"string","doc":"..."},
{"name":"contactsInPhonebook","type":"int","doc":"The number of contacts in phonebook
    "},
{"name":"contactsIdentified","type":"int","doc":"The number of contacts identified for
     the upload"},
{"name":"contactsUploaded","type":"int","doc":"The number of contacts actually
    uploaded"},
{"name":"includeNames","type":"boolean","doc":"True if enhanced search is eligible and
     name upload i
    s granted"}
```

```
.syncContactByUri(
%SyncContactsResult(createdContactIds=
tagsPhonebookForcedUpload
```

The sentence of the schema doc, "Event logged on pre installs", suggests that the event is logged on devices where the app ships preinstalled. The internal label UGC (user-generated

content) suggests that the operator treats the installer's phonebook as content that the installer contributes.

The evidence is the schema, the field documentation and the method names in the string pool. No control flow pass and no runtime capture was performed. What is therefore not established: whether the upload runs for EEA devices today, whether names are sent (the includeNames flag is gated by an enhanced search eligibility), whether the Initial upload precedes a consent screen, and what the tagsPhonebookForcedUpload path forces. Truecaller's reply of 18 September 2026 does not say that AppUgcUpload or the sync methods are unreachable. It describes unreachable code in general terms and names no component.

The same app declares READ_CONTACTS, WRITE_CONTACTS, READ_CALL_LOG and WRITE_CALL_LOG and registers a call screening service (TruecallerCallScreeningService, BIND_SCREENING_SERVICE), so the upload pipeline sits in an app that already holds the address book and the call history.

Impact: The people affected are the contacts of Truecaller users, a group that by construction did not install the app. Their names and numbers are counted for upload from someone else's phone. An Article 14 notice cannot reach them through any Truecaller screen.

Fix: Answer in writing which legal basis under Article 6(1) covers uploaded contacts who are not Truecaller users, how Article 14 is met toward them, what the includeNames flag and the tagsPhonebookForcedUpload path do for EEA devices, and align the store listing wording with the pipeline in the build.

C2: A noneu hostname pattern on OTP verification and telephony hosts

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as CRITICAL on 22 August 2026, reassessed in this report

Literal hostnames in the string pool encode an EU and non-EU distinction into production backend names, including sdk-otp-verification-noneu.truecaller.com for the embedded OTP verification SDK that third-party apps use for phone verification. The company also maintains a separate privacy-policy-eu URL and an EU-labelled storage bucket (tc-images-eu). This shows that the operator built infrastructure around an EU and non-EU residency distinction, which is necessary but not sufficient for Articles 44 and 46. The package does not show which requests route to the -noneu hosts for an EEA phone number, or whether an -eu counterpart exists and is used instead. The finding is therefore recorded as the open routing question it is. It was disclosed as CRITICAL on 22 August 2026 and is reassessed in this report to the band that the evidence supports, because the routing logic is unverified, not because of any statement by Truecaller.

```
https://sdk-otp-verification-noneu.truecaller.com/v2/otp/client/installation/
https://sdk-otp-verification-noneu.truecaller.com/v3/otp/installation/
https://cloud-telephony-noneu.truecallerstatic.com
https://testing-ads-router-noneu.truecaller.net
https://testing-leadgen-noneu.truecaller.net
```

```
https://privacy.truecaller.com/privacy-policy
https://privacy.truecaller.com/privacy-policy-eu
https://storage.googleapis.com/tc-images-eu/myview/...
messenger-dev-se1.truecaller.com
```

The SDK case is the sharpest. An EEA end user of a third-party app that embeds the Truecaller SDK for phone verification never opens the Truecaller app and never sees Truecaller's privacy policy, yet the phone number of that person is processed through this endpoint family. Question 2 of the notice asks whether that number routes through the -noneu host and under which Article 46 safeguard. The question was asked on 22 August, 12 September, 18 September and 17 October 2026 and has not been answered.

Impact: The people affected are users of any third-party app that offers Truecaller SDK verification. They consented to that app's terms and not to Truecaller's.

Fix: State in writing which host serves EEA verification traffic and which Article 46 mechanism covers any transfer, and link the SDK flow to the EU privacy policy.

H1: Huawei and Mintegral components registered in the manifest

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), editorial severity HIGH

These components are manifest-registered, not only present in the dex: the Huawei push receiver (PushMsgReceiver), the HMS message service, the Huawei push provider, the AAID InitProvider (initOrder 500), the AGConnect initialisation provider, and Mintegral components (MBComponentLifecycleProvider, MBCommonActivity, a NetWorkChangeReceiver). Class descriptors for ByteDance Pangle, Yandex Mobile Ads, VK myTarget and the Tencent WeChat SDK sit in the dex string pool, and their activation state is UNVERIFIED. The mediation waterfall is completed by AppLovin, AppsFlyer (with its OAID module), Facebook Audience Network, InMobi, ironSource, Moloco, Unity Ads, Vungle and tech.crackle.cracklertbsdk. Whether call, contact or location content reaches these SDKs is not established. Ad SDKs usually receive advertising identifiers and ad context. The finding is the presence of this set inside this permission profile. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the app holds the address book, call log, SMS and location of more than 1 billion downloads and wires in components of a PRC-based ad vendor and of Huawei, with the ad vendor the subject of independent security research in 2022.

```
<receiver android:directBootAware="true" android:exported="true" android:name="com.
    huawei.hms.suppor
    t.api.push.PushMsgReceiver" android:permission="com.truecaller.permission.
    PROCESS_PUSH_MSG">
<service android:directBootAware="true" android:exported="true" android:name="com.
    huawei.hms.support
    .api.push.service.HmsMsgService" android:process=":pushservice"/>
<provider android:authorities="com.truecaller.aaidinitprovider" android:exported="
    false" android:ini
    tOrder="500" android:name="com.huawei.hms.aaid.InitProvider"/>
<provider android:authorities="com.truecaller.AGCInitializeProvider" android:exported
    ="false" androi
    d:name="com.huawei.agconnect.core.provider.AGConnectInitializeProvider"/>
<provider android:authorities="com.truecaller.mbcomponentlifcycleprovider" android:
    exported="false"
    android:name="com.mbridge.msdk.config.component.status.
    MBComponentLifecycleProvider"/>
<activity android:name="com.mbridge.msdk.activity.MBCommonActivity" .../>
```

```
Lcom/bytedance/sdk/openadsdk/...
Lcom/bytedance/pangle/plugin/Plugin;
Lcom/yandex/mobile/ads/banner/BannerAdView;
Lcom/my/target/ads/MyTargetView...
com.tencent.mm.opensdk.openapi.WXAPIFactory
```

The findings notes cite Snyk's 2022 report on Mintegral ("SourMint") on undisclosed click injection and clipboard and URL collection, and PRC National Intelligence Law Article 7 for the Chinese vendors. Both are public references that the notes carry and that are not re-verified in this report. The point is that two components of Chinese origin are wired into the

manifest, not that call content is shown to flow to them.

Impact: The people affected are every user of the app and, through the address book, the contacts of every user. The ad identifiers and device context that ad SDKs commonly receive link a person to a device.

Fix: Name each ad and push SDK that runs on EEA devices with its operating entity and transfer mechanism, remove SDKs that are not needed, and document the gating of the Huawei components on devices without Huawei services.

H2: Five providers start SDKs before consent and subscription checks

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 (CVSS-B), editorial severity HIGH

The manifest declares five providers that the operating system instantiates when the app process starts, before any Activity can render: FirebaseInitProvider (initOrder 100, directBootAware), MobileAdsInitProvider (100), VungleProvider (102), the Huawei AAID InitProvider (500) and FreshchatInitProvider. A real IAB TCF v2 and Google User Messaging Platform consent stack is present in the binary (TCStringDecoder, AdsConsentManager, IABTCF_gdprApplies, IABTCF_TCString, user-messaging-platform 3.2.0). It governs ad personalisation state once the SDKs run and does not decide whether these providers are instantiated. A Premium subscriber's device runs the same initialisation, because Play Billing cannot intercept provider start. Whether personal data is transmitted onward by an initialised SDK for a given user was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the initialisation runs on every launch of an app with more than 1 billion downloads, including on the devices of paying subscribers who bought the ad-free experience.

```
<provider android:authorities="com.truecaller.firebasesdkprovider" android:
    directBootAware="true" an
    droid:exported="false" android:initOrder="100" android:name="com.google.firebase.
    provider.Fireba
    seInitProvider"/>
<provider android:authorities="com.truecaller.mobileadsinitprovider" android:exported
    ="false" androi
    d:initOrder="100" android:name="com.google.android.gms.ads.MobileAdsInitProvider
    "/>
<provider android:authorities="com.truecaller.vungle-provider" android:exported="false
    " android:init
    Order="102" android:name="com.vungle.ads.VungleProvider"/>
<provider android:authorities="com.truecaller.aaidinitprovider" android:exported="
    false" android:ini
    tOrder="500" android:name="com.huawei.hms.aaid.InitProvider"/>
<provider android:authorities="com.truecaller.freshchat.initprovider" android:enabled
    ="true" android
    :exported="false" android:multiprocess="true" android:name="com.freshchat.consumer
    .sdk.provider.
    FreshchatInitProvider"/>
```

Truecaller's reply of 18 September 2026 describes unreachable code in application builds. A ContentProvider declared in the manifest is not unreachable code. The operating system instantiates it at process start. This is documented platform behaviour and is the reason the

point was raised in the follow-up of 18 September 2026 without being answered.

The Play Billing integration for Premium is confirmed in the dex (BillingClient, com.android.vending.billing). Premium's stated benefit is an ad-free experience. The initialisation sequence above does not depend on subscription state.

Impact: The people affected include paying Premium subscribers. They pay for an ad-free experience and their device still starts the same advertising, analytics and support SDKs at launch as the device of a user of the ad-supported app.

Fix: Defer initialisation of advertising and analytics SDKs until consent state is known and subscription state is checked, using on-demand initialisation instead of manifest providers.

H3: Exported account-state provider with a normal-level permission

---

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 22 August 2026, reassessed in this report

The provider with the authorities com.truecaller.TcAccountStateProvider and com.truecaller.TcInfoContentProvider is exported and its read permission com.truecaller.permission.sdk.internal.read_account_state has protectionLevel normal. Android grants a normal permission to any app that declares it, with no prompt and no signature match. The sibling internal SDK permissions in the same manifest (SDK_ACTION_HANDLER, PROCESS_PUSH_MSG, PUSH_PROVIDER) use protectionLevel signature. Some cross-app exposure is by design, because the provider belongs to the Truecaller SDK surface for partner apps. The content that the provider returns was not examined, so the rating reflects the weaker permission level and not a demonstrated read of personal data. It was disclosed as HIGH and is reassessed in this report for that reason.

```
<permission android:name="com.truecaller.permission.sdk.internal.read_account_state"
    android:protect
    ionLevel="normal"/>
<provider android:authorities="com.truecaller.TcAccountStateProvider;com.truecaller.
    TcInfoContentPro
    vider" android:exported="true" android:name="com.truecaller.sdk.utils.
    TcInfoContentProvider" and
    roid:readPermission="com.truecaller.permission.sdk.internal.read_account_state"/>
```

Not tested: the columns and values the provider returns, and whether they identify the account holder. No second app was built and no query was run.

Impact: Any other app on the same phone can declare one line in its manifest and query the account-state provider without the user seeing a permission dialog.

Fix: Raise the read permission to signature level or a signature-or-allowlist scheme for partner apps, and document what the provider returns.

H4: AI Call Scanner analyses the voice of a call counterparty

LOW, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), editorial severity MEDIUM, disclosed as HIGH on 22 August 2026, re-assessed in this report

The store listing says: ”AI Call Scanner can analyze whether a voice may be human or AI synthesized during a call.” The binary confirms a settings-exposed feature (AICallScanner, showAICallScannerButton, CallsSettings$AiCallScannerOptions$ShowScannerButton). Separately, a Custom Voice feature records the device owner’s voice for an assistant persona, with its own terms page and the instruction ”Tap the microphone button to record, then read the text clearly and naturally and tap again when you’re done.” The counterparty on a call analysed by AI Call Scanner is very often not a Truecaller user and sees nothing of this processing. Whether classification runs on the device or on a server, what is retained, and the legal basis for a non-user’s voice are not shown by the package. A search for on-device audio feature markers (AudioClassifier, .tflite, mfcc, spectrogram, feature_vector, audio_feature) returned no hits, which is a string-pool negative and not a bytecode-verified negative. Disclosed as HIGH, this finding is a legal basis and impact assessment question more than a technical flaw. CVSS gives it a LOW band. RFI-IRFOS blast-radius escalation: raised from LOW/2.1 to MEDIUM because the voices analysed belong to call counterparties who have no account, no notice and no way to object, and the voice is potentially biometric data.

```
AICallScanner
showAICallScannerButton
Lcom/truecaller/settings/impl/ui/calls/
    CallsSettings$AiCallScannerOptions$ShowScannerButton;
```

```
CallAssistantCustomVoiceMicrophoneInstructions: "Tap the microphone button to record,
    then read the
    text clearly and naturally and tap again when you're done."
https://storage.googleapis.com/public-hznp758ywfi3oz4w1wpdyqxhn1jrf3pa/assets/custom-
    voice-terms.htm
    l
```

RECORD_AUDIO is tied in the string pool to conventional features (VoIP calling, voicemail greeting recording, call recording troubleshooting) and to these two features. The existence of a dedicated terms page for Custom Voice shows that the operator treats the feature as legally distinct.

Impact: The people affected are the people on the other end of a call. They are chosen by nobody and informed by nobody, and for Custom Voice the owner’s own voice sample is the input to a synthetic voice model.

Fix: Answer question 3 of the notice in writing, state whether the classification runs on the device, state the retention of any audio or derived value, and state the legal basis for analysing a non-user’s voice.

M1: Firebase and Google API key hardcoded in strings.xml

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B)

The values below ship in every copy of version 26.32.7. A Firebase API key in a client is expected and is not a secret by Google's design. The notice described five abuse vectors that follow from key, database URL and sender ID: quota and billing exhaustion, replay of an unrestricted key against other Google APIs on the same project, project and IAM enumeration, FCM token enumeration for targeted phishing, and unauthenticated Realtime Database read if the rules are misconfigured. The key was not tested against any server and the Security Rules were not examined.

```
<string name="firebase_database_url">https://truecallerapis.firebaseio.com</string>
<string name="gcm_defaultSenderId">22378802832</string>
<string name="google_api_key">AIzaSyB-U1NIB36__pxbjuXECXX28S8PK6l672g</string>
<string name="google_app_id">1:22378802832:android:d040f8b97ff358e8</string>
```

Impact: The exposure is availability and abuse of the operator's own Firebase project. Push token enumeration would target Truecaller's own users with phishing if it were possible.

Fix: Restrict the key by package name and signing certificate, confirm deny-by-default Security Rules on the Realtime Database, and enforce App Check on the project.

M2: Cleartext allowed for two TCPay domains, no pinning

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), disclosed as MEDIUM on 22 August 2026, reassessed in this report

network_security_config.xml permits cleartext for assets.api.tcpay.in, assets.tcpay.in and 127.0.0.1 (includeSubdomains true) and declares no pin-set. The two named external domains belong to TCPay, the payments product of the India market (TcpayPromo and TCPAY_ONBOARDING strings are confirmed in the dex). Asset domains typically serve static images. The configuration opens a cleartext path that a network attacker could use to tamper with content, and the absence of pinning leaves every other connection on system CA trust alone. It was disclosed as MEDIUM and is reassessed to the band of its vector because the affected content is static assets.

```
<network-security-config>
    <debug-overrides>
        <trust-anchors><certificates src="user" /></trust-anchors>
    </debug-overrides>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">assets.api.tcpay.in</domain>
        <domain includeSubdomains="true">assets.tcpay.in</domain>
        <domain includeSubdomains="true">127.0.0.1</domain>
    </domain-config>
</network-security-config>
```

Impact: The practical exposure is limited to content loaded from the two asset domains and to the general reliance on system trust for everything else.

Fix: Remove the cleartext exception, serve the assets over HTTPS, and add pinning for the core API hosts.

M3: Notification listener service registered

INFO, no CVSS v4.0 score assigned, disclosed as MEDIUM on 22 August 2026, recorded as an observation

NotificationHandlerService is registered with BIND_NOTIFICATION_LISTENER_SERVICE. Once the owner grants the separate Notification Access permission, the service can observe notifications of every app, which is enough to derive who messages whom and when without reading content. A separately named OTPCopierService suggests OTP autofill as the primary use, a conventional feature. What is retained or derived from other notifications is UNVERIFIED. The item is recorded as an observation because a capability alone does not meet the standard for a scored finding.

```
<service android:exported="false" android:name="com.truecaller.notifications.
    NotificationHandlerServ
    ice" android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter><action android:name="android.service.notification.
    NotificationListenerService"/>
    </intent-filter>
</service>
```

Impact: A grant of Notification Access to a caller identification app is broader than OTP autofill by construction.

Fix: State what the notification service reads, keeps and derives, and limit it to OTP notifications.

M4: Family Protection Admin and Member services

INFO, no CVSS v4.0 score assigned, disclosed as MEDIUM on 22 August 2026, recorded as an observation

The package contains truecaller.familyprotectionconfig.admin.v1.AdminService and truecaller.familyprotectionconfig.member.v1.MemberService, with local data source methods for auto-reject sources, protection level and block patterns. The feature is store-advertised and opt-in (”Remotely end suspicious or fraud calls”, ”Manage spam block lists for your family”, ”Check battery level and activity status”). No adverse finding is asserted for the feature or its purpose. It is recorded as the binary-confirmed instance of operator-side or admin-side push of device behaviour.

```
truecaller.familyprotectionconfig.admin.v1.AdminService
truecaller.familyprotectionconfig.member.v1.MemberService
FamilyProtectionConfigLocalDataSource.getAutoRejectSources
FamilyProtectionConfigLocalDataSource.getProtectionLevelFlow
FamilyProtectionConfigLocalDataSource.getAllBlockPatterns
```

Impact: The family members who are linked as Member receive configuration from an Admin account. A household can include children, and the rating of the app does not speak to them.

Fix: Document what the Admin account can see and change on a Member device and how a Member is told.

Impact Analysis

Three groups of people are affected, and only one of them chose to install the app.

The first group is the installers. They grant contacts, call log, SMS, location and microphone permissions to an app that runs five advertising, analytics and support SDKs at launch, wires in Huawei and Mintegral components and exposes an account-state provider with a weak permission. Premium subscribers pay for an ad-free experience, and their device still starts the same SDKs.

The second group is the contacts of the installers. Their names and numbers are the input of the pipeline that C1 describes, and the schema counts contacts uploaded per installer. They have no screen to see and no relationship to the operator.

The third group is the people on the other end of a call and the users of third-party apps that embed the Truecaller SDK. Call counterparties are analysed by AI Call Scanner, and users of partner apps route a phone number through an endpoint family whose EU treatment is not explained. This report does not claim that harm has occurred. It describes who stands in the path of each mechanism.

The Complete Chain

Step	Evidence	Finding
A person installs the app and grants contacts, call log, SMS, location and microphone access	Manifest permissions, store listing with 1 billion or more downloads	L1
Five providers start advertising, analytics and support SDKs before any screen and regardless of Premium	Manifest, initOrder 100 to 500	H2
Huawei push and Mintegral ad components are registered	Manifest, Huawei and Mintegral	H1
The app counts contacts identified and contacts uploaded per run	AppUgcUpload schema, sync method names	C1
A phone number from a partner app's verification flow touches a -noneu endpoint family	Hostnames in the string pool	C2
A live call counterparty's voice is classified	AICallScanner strings	H4
Other apps on the same phone can query an account-state provider	Exported provider, normal permission	H3
The operator answers with a general reachability statement and no itemised reply	Thread, 18 Sep and 17 Oct 2026	All

The chain runs from the install through to the contact who never installed. Its weakest link is the same in C1, C2 and H4: the package shows that the mechanism is built, and only the operator can say whether it runs for EEA users. That is why the three questions carry the open part of the report.

Inference Data, Bystanders and Control

Six categories of invisible data were considered. Non-events were not evaluated in this pass. A household graph through Family Protection and location is plausible and UNVERIFIED. A relationship graph from notifications is applicable as a capability (M3). Bystander data is applicable and confirmed in the design of C1 (phonebook contacts) and H4 (call counterparties). Inference data is applicable and confirmed: spam and scam classifications (SpamReportColors, inTopSpammerList, filterMatchAction) and the human-versus-synthetic voice determination are values that did not exist as raw data before the operator computed them. Control data is applicable: the Family Protection Admin and Member services and the order of SDK initialisation are set by the operator and not by the user.

Identity linkage, server-side persistence of the crowdsourced database and its retention were not established in this pass. The deletion path named by the Data Safety label (”You can request that data be deleted”) was not verified and is UNVERIFIED.

Consumer Protection & Platform Disclosures

The Google Play listing states that Truecaller does not upload the phonebook, and the Data Safety label lists Device or other IDs as shared and Location, Personal info and 9 other types as collected. The binary contains a metric for contacts actually uploaded, which the plain reading of the first statement excludes. The two texts that the notes compare (the Play wording and the APKMirror mirror copy) differ in what they exclude, and the binary is consistent with the second.

The content rating is ”Parental Guidance Recommended”. Age ratings assess content risk to the installing user. They do not describe the footprint on the people in the installer’s phonebook, who include minors. This is a structural gap in how store ratings map onto an intermediary app. It is not a defect of the binary and no mismatch is asserted for the rating level itself.

Premium is sold as an ad-free experience, and the initialisation described in H2 does not depend on subscription state. Whether that is a deceptive design depends on what the SDKs transmit, which was not observed.

Data Protection: Article by Article

Article	Relevance	Finding
5(1)(a)	Lawfulness, fairness and transparency: store claim against the upload pipeline	C1
5(1)(f), 32(1)(a), (b)	Confidentiality and integrity: cleartext exception, no pinning, exported provider, hardcoded key	M2, H3, M1
6(1)	Legal basis for contacts of non-users and for a counterparty's voice	C1, H4
7(1)	Consent must precede processing: provider initialisation before any screen	H2
9(1), 9(2)	Voice as potential biometric data, names that reveal health context in contacts	H4, C1
13, 14	Information duties toward users of SDK partner apps and toward non-user contacts	C2, C1
25	Data protection by design: manifest providers, normal-level permission	H2, H3
28	Processor due diligence for ad and push SDK vendors	H1
35	Impact assessment for AI Call Scanner, refused for disclosure	H4
44, 46	Transfers: -noneu hosts, Huawei and Mintegral	C2, H1

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 5, 6, 7, 9, 13, 14, 25, 28, 32, 35, 44 and 46, and Directive 2002/58/EC Article 5(3) for the consent timing in H2. The disclosure follows ISO/IEC 29147 and rests on the freedom of research under Article 17 of the Austrian Staatsgrundgesetz and Article 89 GDPR.

The Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) were in copy of the notice. The operator is Swedish and its main establishment is UNVERIFIED, so the competence of the IMY as lead authority under Article 56 is an inference. An Article 27 representative does not apply if the main establishment is in the EU.

The report makes no comparison with other applications.

Indicators of Compromise & Reproducible Evidence

Every item can be reproduced from the package named below. No Truecaller server was contacted, the Firebase key was not tested and no account was created.

```
Package       com.truecaller 26.32.7 (2632007)
XAPK          b2d6994237ba302f48bc54b537ebf01e9a99812edcf9ae4f1a7f047eb385b210
base.apk      c8ac7ae6e684d5c9625412d5e0f417db335d3b5f27e4a7b818d8619f6d3e9406
Signer SHA-1  0ac1169ae6cead75264c725febd8e8d941f25e31
Schema        com.truecaller.tracking.events.AppUgcUpload (classes7.dex)
Code path     tagsPhonebookForcedUpload, syncContactByUri, SyncContactsResult
Hosts         sdk-otp-verification-noneu.truecaller.com, cloud-telephony-noneu.
    truecallerstatic.com
              testing-ads-router-noneu.truecaller.net, testing-leadgen-noneu.
    truecaller.net
              assets.api.tcpay.in, assets.tcpay.in (cleartext), messenger-dev-se1.
    truecaller.com
Policies      https://privacy.truecaller.com/privacy-policy, .../privacy-policy-eu
Firebase      https://truecallerapis.firebaseio.com, sender 22378802832
API key       AIzaSyB-U1NIB36__pxbjuXECXX28S8PK6l672g
App ID        1:22378802832:android:d040f8b97ff358e8
Permission    com.truecaller.permission.sdk.internal.read_account_state (normal)
Provider      com.truecaller.sdk.utils.TcInfoContentProvider (exported)
Support       support@truecaller.com, ticket 6022352
```

The full values of all identifiers are given in clear text as they appear in the package.

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	Notice REF TRUECALLER-2026-R1 to support@truecaller.com at 14:19 UTC, Datenschutzbehörde and EDPS in copy. Ten scored findings, one unscored note on the permission surface (L1), three questions. Publication stated as 20 November 2026. Automatic reply 20 seconds later: ticket 6022352, request for screenshots and a phone number.
12 Sep 2026	Follow-up: the intake ticket does not answer the findings, the three questions repeated, answer requested by 19 September 2026.
18 Sep 2026	08:33 UTC: Truecaller replies with a no-breach conclusion, a general unreachable-code statement, a refusal to share compliance documents and a pointer to security.txt. 10:07 UTC: RFI-IRFOS names two response patterns, repeats the three questions and asks for an itemised reply or a written statement of declining.
17 Oct 2026	Follow-up 34 days before publication from security@rfi-irfos.com: open items restated, the three questions unchanged, publication date unchanged.

Date	Event
15 Nov 2026	12:59 UTC: follow-up from s.kepp@rfi-irfos.com, five days before publication, three questions and open items restated. 12:59 UTC: automated ticket 6460053 from the support system, "you can expect a response from us within 48 business hours". No further message from Truecaller followed.
20 Nov 2026	Publication date, unchanged since 22 August 2026.
21 Nov 2026	Publication, the day after the stated publication date. No itemised reply and no answer to any of the three questions on record.

Outcome as of 21 November 2026: one general written response, no itemised reply, no answer to any of the three questions, one stated change to the release process and two automated ticket confirmations. The thread holds no bounce and no mark of closure.

What Truecaller Got Right

A real IAB TCF v2 and Google User Messaging Platform consent stack is present and wired, which is genuine engineering investment in consent tooling even though it does not decide provider instantiation. Every sibling internal SDK permission except the one in H3 correctly uses protectionLevel signature, so the stricter setting was available and used. A distinct EU privacy policy URL and an EU-labelled storage bucket show deliberate EU-specific design, with a scope that is not established. Family Protection is a disclosed opt-in feature. No cleartext traffic is permitted globally, only the two named TCPay domains. The Data Safety label states encryption in transit, a deletion path and an independent security review, commitments that the analysis did not contradict and also did not verify. Truecaller answered in writing, within 27 days, and states that it changed its release process.

Priority	Action	Finding

Residual Risk & Recommendations

Priority	Action	Finding
1	Answer in writing the legal basis for non-user contacts and the Article 14 path, and align the store listing with the pipeline	C1
2	Name the host and the Article 46 safeguard for EEA phone verification	C2
3	Move advertising and analytics initialisation behind consent and subscription state	H2
4	Document the Huawei, Mintegral and other ad SDKs that run on EEA devices	H1
5	Raise the read permission of the account-state provider	H3
6	Publish the outcome of the AI Call Scanner impact assessment or state the legal basis for non-user voices	H4
7	Restrict the Firebase key, confirm deny-by-default rules, remove cleartext exceptions	M1, M2

Residual risk: the weekly comparison of shipped builds that was announced in the follow-ups of 12 and 18 September 2026 has no result recorded in the case folder. The stated dead-code elimination can only be confirmed by diffing a newer build against version 26.32.7, and this report describes version 26.32.7 only. A comparison of a newer build is not part of this report.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published application plus the live Google Play listing. No Truecaller servers were probed and the Firebase key was not tested. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 6, 7, 9, 13, 14, 25, 28, 32, 35, 44, 46, Directive 2002/58/EC Art. 5(3). RFI-IRFOS ZVR 1015608684, GISA 39261441. REF TRUECALLER-2026-R1.