Coordinated Security & Privacy Disclosure, Final Report

VR Banking Ecosystem (Fiducia GAD, 6 apps)

Fiducia & GAD IT AG, the core IT provider for Germany's Volksbanken and Raiffeisenbanken cooperative banking group

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 95 DAYS AFTER DISCLOSURE, SIX MESSAGES SENT, ZERO REPLY OF ANY KIND

Target	Six Android apps in the VR Banking ecosystem, built and maintained by Fiducia & GAD IT AG for Germany's Volksbanken/Raiffeisenbanken cooperative banking group
Packages	de.fiduciagad.banking.vr (VR Banking), de.fiduciagad.android.vrsecurego (VR SecureGo+, TAN generator), de.fiduciagad.android.vb.id (VB ID), de.fiduciagad.banking.vbpay (VB Pay), de.fiduciagad.android.vrbanking (VR Bank), de.fiduciagad.quck (Quck)
Operator	Fiducia & GAD IT AG, core banking IT provider for the German Volksbanken/Raiffeisenbanken cooperative group
Initial Disclosure	2026-06-21
Original Embargo	2026-09-21 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-24, three days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Austrian DSB, German BfDI (poststelle@bfdi.bund.de), CERT.at
Total Outbound Messages	6, across 95 days. The initial CC address, security@volksbank.at, bounced on the very first send and was dropped from all subsequent messages, which went to datenschutz@fiduciagad.de alone.
Inbound Replies	0. No reply, automated or human, was ever received from datenschutz@fiduciagad.de or security@volksbank.at.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS disclosed to Fiducia & GAD IT AG, the core IT provider for Germany's Volksbanken and Raiffeisenbanken cooperative banking group, that VR SecureGo+, the TAN one-time-code generator used to authorize banking transactions across the group, trusts user-installed CA certificates in its network security configuration. This is not a theoretical weakness: Volksbank.at had already published a security warning, before this disclosure, documenting an active quishing campaign in which attackers mail physical letters containing QR codes that lead victims to a fake VR SecureGo synchronization page instructing them to install a "security certificate," an attacker-controlled CA that VR SecureGo+'s own configuration is built to trust, positioning the attacker to intercept TAN confirmation traffic for real banking transactions.

A separate finding concerns VR Banking's own Play Store Data Safety declaration, which states "Keine Daten erhoben" and "Keine Daten an Drittunternehmen weitergegeben," no data collected, no data shared with third parties, directly contradicted by a 441-class AppsFlyer attribution SDK integrated deliberately enough that the app ships a custom-written backup-exclusion XML file naming AppsFlyer's own database paths individually. A deliberate backup-rules file for a specific third-party SDK is not consistent with that SDK's absence.

Six messages were sent to datenschutz@fiduciagad.de across 95 days, cc'ing security@volksbank.at on the first attempt, which bounced immediately and was dropped from every subsequent message, and bcc'ing the Austrian DSB, the German BfDI, and CERT.at throughout. Not one reply, automated or human, was ever received. The 90-day embargo, set at first contact, elapsed on 21 September 2026. This report and the accompanying closure notice publish three days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of six production Android applications in the VR Banking ecosystem (de.fiduciagad.banking.vr, de.fiduciagad.android.vrsecurego, de.fiduciagad.android.vb.id, de.fiduciagad.banking.vbpay, de.fiduciagad.android.vrbanking, de.fiduciagad.quck), covering the AndroidManifest, network security configuration, resource strings, decompiled dex/smali, and the Play Store Data Safety section, as pulled and reviewed on 21 June 2026. No dynamic instrumentation, live traffic capture, TAN interception, account creation, or interaction with Fiducia GAD's or Volksbank's backend infrastructure was performed.

Disposition

Five findings were disclosed on 21 June 2026, later re-scored under CVSS v4.0. One finding is held at CRITICAL under an explicit, stated blast-radius escalation: VR SecureGo+, the TAN authentication generator used across the cooperative banking group, trusts user-installed CA certificates in its base network configuration, the exact misconfiguration exploited by an active quishing campaign against VR SecureGo synchronization that Volksbank itself had already publicly warned customers about before this disclosure was sent. A second finding, a Play Store "no data collected" declaration directly contradicted by a deliberately-integrated 441-class attribution SDK, corrects down to MEDIUM, as do two further findings. A fifth finding, concerning whether a purchase-attribution database is actually erased on account closure, is classified OBSERVATIONAL as an unconfirmed retention question, not a demonstrated technical gap. Six messages were sent across 95 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	CRITICAL	VR SecureGo+ Trusts User-Installed CA Certificates, the Exact Vector an Active, Bank-Acknowledged Quishing Campaign Already Exploits
C2	MEDIUM	VR Banking's Play Store "No Data Collected" Declaration Is Contradicted by a Deliberately-Integrated 441-Class Attribution SDK
H1	MEDIUM	Behavioral Biometrics SDK Injected Into the Banking WebView, No Disclosed Art. 9 Legal Basis
H2	MEDIUM	MANAGE_ALL_FILES_ACCESS_PERMISSION Declared in the TAN Generator
H3	OBSERVATIONAL	Whether the AppsFlyer Purchase Database Is Actually Erased on Account Closure Is an Open Question, Not a Demonstrated Gap

Subject & Operator Analysis

Fiducia & GAD IT AG is the core IT provider for Germany's Volksbanken and Raiffeisenbanken cooperative banking group, and builds and maintains the six Android apps covered by this disclosure: VR Banking, VR SecureGo+ (the TAN generator), VB ID, VB Pay, VR Bank, and Quck. The findings here concern shared infrastructure used across a large, systemically significant cooperative banking network, not an isolated app.

Several genuine positives are worth naming. VR SecureGo+ correctly sets allowBackup=false, appropriate for a TAN authentication app. VR Banking correctly disables cleartext traffic in its base network configuration. HTTPS is enforced across all primary banking endpoints in every app reviewed. The user-CA trust finding (C1) sits inside an otherwise reasonably hardened network configuration, which makes its presence more surprising, not less serious.

A Vulnerability the Bank Had Already Publicly Warned Customers About

C1 is unusual among the findings in this campaign in one specific respect: RFI-IRFOS did not have to argue that the misconfiguration was exploitable in theory. Volksbank.at had already published its own security warning, before this disclosure was sent, describing an active quishing campaign engineered around exactly this weakness, tricking VR SecureGo+ users into installing an attacker-controlled certificate their own app's configuration is built to trust. The gap between the bank's public warning to customers and the underlying configuration fix, a single line of XML, remaining unaddressed for the full 95 days of this disclosure is the central fact of this report.

Findings

C1: VR SecureGo+ Trusts User-Installed CA Certificates, the Exact Vector an Active, Bank-Acknowledged Quishing Campaign Already Exploits

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6. RFI-IRFOS blast-radius escalation: raised from HIGH/8.6 to CRITICAL because this is not a theoretical weakness, an active quishing campaign specifically targeting this exact misconfiguration was already publicly documented by Volksbank itself before this disclosure was sent, against a TAN mechanism relied on across the entire cooperative banking group.

VR SecureGo+'s network security configuration trusts user-installed CA certificates in its base-config: <certificates src="user"/>, alongside the system trust store. Volksbank.at published a security warning, before this disclosure, describing an active quishing campaign: attackers mail physical letters with QR codes leading to a fake VR SecureGo synchronization page, which instructs victims to install a 'security certificate,' in reality an attacker-controlled CA. Because VR SecureGo+'s own base-config trusts user-installed CAs, a victim who completes that installation step has handed the attacker a working man-in-the-middle position over their TAN confirmation traffic, the one-time codes that authorize real banking transactions. RFI-IRFOS blast-radius escalation: raised from HIGH/8.6 to CRITICAL because this exact misconfiguration is the mechanism an active, bank-acknowledged phishing campaign already exploits, against a TAN generator used across Germany's Volksbanken/Raiffeisenbanken cooperative banking group.

```
de.fiduciagad.android.vrsecurego, network_security_config.xml
<base-config cleartextTrafficPermitted="false">
    <trust-anchors>
        <certificates src="system"/>
        <certificates src="user"/>  <!-- trusts attacker-installed CAs -->
    </trust-anchors>
</base-config>

Attack chain (documented by Volksbank's own public security warning, pre-dating this
    disclosure):
1. Victim receives a physical letter with a QR code (quishing)
2. QR code leads to a fake VR SecureGo synchronization page
3. Page instructs the victim to install a 'security certificate'
4. VR SecureGo+ trusts the resulting attacker-controlled CA per its own config
5. TAN confirmation traffic is now interceptable by the attacker's CA
```

Impact: A victim who completes the certificate-installation step of an already-active phishing campaign hands the attacker a working interception position over the one-time codes that authorize their real banking transactions, on a TAN generator used across an entire cooperative banking group.

Fix: Remove <certificates src="user"/> from VR SecureGo+'s base network security configuration; a TAN authenticator has no legitimate reason to trust certificates a user, or an attacker who has social-engineered that user, can install. No confirmation that this has occurred was ever received.

C2: VR Banking's Play Store "No Data Collected" Declaration Is Contradicted by a Deliberately-Integrated 441-Class Attribution SDK

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

VR Banking's Play Store Data Safety section states 'Keine Daten erhoben' and 'Keine Daten an Drittunternehmen weitergegeben,' no data collected, no data shared with third parties. The production APK contains AppsFlyer, a mobile attribution SDK, across 441 smali classes, together with a custom-written backup-exclusion file, appsflyer_backup _rules.xml, individually naming AppsFlyer's own database and shared-preference paths. Writing a dedicated exclusion rule for a specific SDK's specific data files is conclusive evidence of deliberate integration, not an accidental transitive dependency, and directly contradicts the app's own public declaration of collecting no data.

```
Play Store Data Safety (screenshot captured 2026-06-21):
"Keine Daten an Drittunternehmen weitergegeben"
"Keine Daten von dieser App erhoben"

res/xml/appsflyer_backup_rules.xml (custom-written, not a default):
<exclude domain="database" path="afpurchases.db"/>
<exclude domain="database" path="appsflyer-data"/>
<exclude domain="sharedpref" path="appsflyer-purchase-data"/>

com/appsflyer/ -- 441 smali classes
```

Impact: Customers relying on the Play Store's own data-safety disclosure to make an informed choice about a banking app are given a declaration directly contradicted by a deliberately-configured third-party attribution SDK present in the same binary.

Fix: Correct the Play Store Data Safety declaration to name AppsFlyer as a data recipient, or remove the SDK entirely if the 'no data collected' claim is meant to hold. No confirmation that this has occurred was ever received.

H1: Behavioral Biometrics SDK Injected Into the Banking WebView, No Disclosed Art. 9 Legal Basis

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

WebSupportInjectJS.smali injects JavaScript into VR Banking's WebView, including BehavioSec's behavioral biometrics SDK: keystroke dynamics, swipe velocity, tap pressure, device orientation during typing, and interaction timing. BehavioSec, a US company (LexisNexis Risk Solutions/RELX Group subsidiary), processes this data for the purpose of uniquely identifying a natural person, which constitutes special category biometric data under GDPR Art. 9. No Art. 9(2) legal basis for this processing is disclosed to banking customers, and BehavioSec is not named as an Art. 28 sub-processor.

```
de.fiduciagad.banking.vr, WebSupportInjectJS.smali
# injects JavaScript into the banking WebView, including BehavioSec SDK
# collects: keystroke dynamics, swipe velocity, tap pressure, orientation-while-typing
```

Impact: A banking customer's typing rhythm and touch behavior, biometric data capable of uniquely identifying them, is processed by a named third party for identity-verification purposes with no disclosed legal basis or sub-processor agreement.

Fix: Name BehavioSec as an Art. 28 sub-processor, document an Art. 9(2) legal basis for behavioral biometric processing, and disclose the practice to customers. No confirmation that this has occurred was ever received.

H2: MANAGE_ALL_FILES_ACCESS_PERMISSION Declared in the TAN Generator

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.

VR SecureGo+ declares android.permission.MANAGE_ALL_FILES_ACCESS_PERMISSION, a dangerous-level Android 11+ permission granting access to the entire device filesystem, including other apps' external storage, USB storage, and SD cards, intended for file-manager and backup apps specifically. A TAN generator, whose sole function is producing one-time authentication codes for banking transactions, has no demonstrated legitimate need for full filesystem access, and Google Play policy restricts this permission's intended use accordingly.

```
de.fiduciagad.android.vrsecurego, AndroidManifest.xml
<uses-permission android:name="android.permission.MANAGE_ALL_FILES_ACCESS_PERMISSION
    "/>
```

Impact: An authentication-code generator carries an unnecessarily broad attack surface, full filesystem access, that a compromise of the app itself, or of a component with excessive permission, would expose well beyond what generating a TAN requires.

Fix: Remove MANAGE_ALL_FILES_ACCESS_PERMISSION unless a specific, documented feature requires it, and scope any such requirement to the narrowest permission available. No confirmation that this has occurred was ever received.

H3: Whether the AppsFlyer Purchase Database Is Actually Erased on Account Closure Is an Open Question, Not a Demonstrated Gap

OBSERVATIONAL — not independently CVSS-scored; an unconfirmed data-retention question, not a demonstrated technical failure.

VR Banking's Play Store Data Safety section lists 'Kontolöschung verfügbar,' account deletion available, which under GDPR Art. 17 implies complete erasure of personal data on request. The app's own backup-exclusion configuration excludes afpurchases.db, AppsFlyer's purchase-tracking database, from device backup (C2), but this static pass found no documented account-deletion procedure that references deleting this database specifically. Whether afpurchases.db actually persists after account closure was not demonstrated by static analysis alone and is stated here as an open question for the operator, not an assertion of a confirmed Art. 17 violation.

Impact: If afpurchases.db is not included in the account-deletion procedure, a customer's purchase-attribution history could persist after they believe their data has been fully erased, though this was not directly demonstrated.

Fix: Confirm and document explicitly whether afpurchases.db is deleted as part of the account-closure procedure, and correct the Play Store Data Safety claim if it is not. No confirmation that this has occurred was ever received.

Six Messages, 95 Days, Zero Reply

This case's correspondence record is total silence. Six messages were sent to datenschutz@fiduciagad.de across 95 days, cc'ing security@volksbank.at on the first attempt, which bounced immediately, and bcc'ing the Austrian DSB, the German BfDI, and CERT.at throughout. Not one reply, automated or human, was ever received from either address.

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(1)(a)/(b), Art. 25	C1	TAN authentication configuration trusts user-installed CAs, enabling MITM against an active, bank-acknowledged phishing campaign.
Art. 5(1)(a), Art. 13, Art. 28	C2	Public 'no data collected' declaration contradicted by a deliberately-integrated attribution SDK, no disclosed sub-processor.
Art. 9(2), Art. 28	H1	Behavioral biometric data processed via injected SDK, no disclosed legal basis or sub-processor agreement.
Art. 5(1)(c)	H2	Excessive filesystem-access permission declared in a single-purpose TAN authentication app.
Art. 17 (unconfirmed)	H3	Open question whether a purchase-attribution database is erased on account closure as publicly claimed.

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, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, C1 is escalated from HIGH/8.6 to CRITICAL specifically because the misconfiguration matches an already-active, bank-acknowledged phishing campaign, a real-world circumstance CVSS's technical vector does not capture; C2, H1, and H2 correct down to MEDIUM to match their own computed bands; H3 is classified OBSERVATIONAL because it is an open, unconfirmed retention question, not a demonstrated technical failure. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: VR-BANKING-2026-R1.