Coordinated Privacy Disclosure, Final Report

Shell Android (com.shell.sitibv.retail)

Shell International Trading and Shipping Company B.V. (SITI B.V.), Den Haag, Netherlands

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, TWO DAYS AFTER THE EMBARGO, NINE MESSAGES ACROSS NINE ADDRESSES AND BOUNCES, ONE AUTOMATED ACKNOWLEDGMENT, ZERO SUBSTANTIVE REPLY

Target	Shell, a fuel retail and loyalty Android app (payments and loyalty card handling)
Package	com.shell.sitibv.retail
Operator	Shell International Trading and Shipping Company B.V. (SITI B.V.), Carel van Bylandtlaan 30, 2596 HR Den Haag, Netherlands; app built by Mobgen B.V. (Accenture subsidiary)
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators	Dutch Autoriteit Persoonsgegevens (lead SA), Austrian DSB, CERT.at
Total Outbound Messages	9, across 92 days, cycling through five contact addresses (privacy@shell.com, dpo@shell.com, dataprotection@shell.com, privacy-office-SI@shell.com) after repeated bounces before delivery began succeeding consistently from 15 August 2026.
Inbound Replies	1, a pure automated acknowledgment on 31 July 2026 confirming receipt only. Zero substantive human reply 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 Shell International Trading and Shipping Company B.V. that its fuel and loyalty Android app, a payments-handling application storing card and key-fob data, ships Facebook Stetho, a Chrome DevTools debug bridge, compiled into the production binary. If initialized, Stetho exposes local SQLite databases, including payment token and loyalty card tables, and live HTTP traffic to any device reachable on the same network, without authentication. PairIP code obfuscation prevented confirming Stetho's actual runtime activation state through static analysis alone; that confirmation would have required dynamic analysis, which depended on a level of engagement that was never reached.

A second finding names a payment-pipeline processor gap, not a single data flow: the app's optional WeChat Pay flow routes transaction data, amounts, timestamps, merchant and device identifiers, through Tencent's SDK. Tencent is a PRC-incorporated company subject to China's National Security Law Art. 7, an obligation to cooperate with PRC state intelligence on demand, without a court order or user notification. No EU adequacy decision covers the PRC, and no third-country transfer is documented for this processor in Shell's privacy materials as reviewed.

Nine messages were sent across 92 days, cycling through four contact addresses after repeated bounces (privacy@shell.com, dpo@shell.com, dataprotection@shell.com) before privacy-office-SI@shell.com began accepting delivery consistently from 15 August 2026. One reply was received on 31 July 2026, a pure automated acknowledgment confirming receipt only, not a substantive response. The 90-day embargo, set at first contact, elapsed on 23 September 2026. This report and the accompanying closure notice publish two days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Shell Android application (com.shell.sitibv.retail, version 8.5.0, 75.1 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Shell's or Tencent's backend infrastructure was performed; the Stetho activation-state question in C1 remains unconfirmed for that reason.

Disposition

Nine findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. A Facebook Stetho debug inspector bundled in a production payment binary and an optional WeChat Pay pipeline routed through Tencent, a PRC-NSL-obligated processor, both reach HIGH on the computed CVSS score alone, no editorial escalation needed; the Stetho finding's activation state was never independently confirmed by dynamic analysis, since no substantive reply was ever received to make that verification possible. Pre-consent Firebase initialization, a dual APM stack, advertising-ID attribution, hard-coded Firebase keys, and an undisclosed Braintree payment processor all correct to MEDIUM. A boot-time auto-start receiver corrects to OBSERVATIONAL, and an undocumented RECORD_AUDIO permission corrects to LOW on its own computed band. Nine messages were sent across 92 days. Only one reply was ever received, a pure automated acknowledgment; no substantive human answer followed.

ID	Severity	Title
C1	HIGH	Facebook Stetho Debug Inspector Compiled Into a Production Payment Binary
C2	MEDIUM	Firebase Initializes Before Any Consent Screen
C3	HIGH	WeChat Pay Routes Payment Data Through Tencent, a PRC-NSL-Obligated Processor
H1	MEDIUM	Two Competing APM Platforms Capture Payment API Traffic
H2	MEDIUM	Advertising ID and Attribution Tracking in a Fuel Loyalty App
H3	MEDIUM	Two Firebase API Keys Hardcoded and Extractable
H4	OBSERVATIONAL	Boot-Time Auto-Start Registered for Notification Scheduling
M1	LOW	Undocumented RECORD_AUDIO Permission
M2	MEDIUM	Braintree (PayPal Subsidiary) as Undisclosed Payment Processor

Subject & Operator Analysis

Shell’s fuel and loyalty app is operated by Shell International Trading and Shipping Company B.V. and built by Mobgen B.V., an Accenture subsidiary. It is a payments-handling application: users store card and key-fob payment methods, scan loyalty cards, and pay at the pump.

Several genuine positives are worth naming. allowBackup is correctly set to false, preventing unencrypted backup of payment data. usesCleartextTraffic is correctly set to false. A network security configuration is present. Adyen, a reputable, PCI-DSS certified, EU-based processor, handles card payments. PairIP code obfuscation raises the reverse-engineering barrier and is also the reason C1’s activation state could not be confirmed through static analysis alone.

Nine Messages, Five Addresses, One Automated Acknowledgment

This case's correspondence record involved repeated address failures before a working channel was found. Early attempts to privacy@shell.com, dpo@shell.com, and dataprotection@shell.com bounced across multiple rounds between 25 June and 23 July 2026. From 31 July 2026 onward, privacy-office-SI@shell.com was tried; the first two attempts to that address also bounced, but delivery began succeeding consistently from 15 August 2026. Nine messages were sent in total across 92 days, cc'ing the Dutch Autoriteit Persoonsgegevens on later rounds. One reply was received, on 31 July 2026, a pure automated acknowledgment confirming receipt only, not a substantive response. No human reply of any kind followed, before or after delivery began succeeding.

Findings

C1: Facebook Stetho Debug Inspector Compiled Into a Production Payment Binary

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

Stetho, Facebook's Chrome DevTools debug bridge, is compiled into the production binary (com.facebook.stetho.inspector.database.SqliteDatabaseDriver, .network.DefaultResponseHandler, .elements.android.MethodInvoker, and related classes are all present). If initialized in the Application class, Stetho opens a local debugging server reachable over the same WiFi network, allowing any device on that network to read and write any local SQLite database without authentication, including ChargeCardTokensRemoteEntity (payment tokens) and ScanCardLoyaltyTracker (loyalty card data), and to inspect all in-flight HTTP requests. PairIP obfuscation prevented confirming, through static analysis, whether Stetho is actually initialized at runtime; that confirmation requires dynamic analysis, which was never reached because no substantive reply was ever received.

```
com.facebook.stetho.inspector.database.SqliteDatabaseDriver
com.facebook.stetho.inspector.database.ContentProviderSchema
com.facebook.stetho.inspector.network.DefaultResponseHandler
com.facebook.stetho.inspector.network.GunzippingOutputStream
com.facebook.stetho.inspector.elements.android.MethodInvoker
com.facebook.stetho.dumpapp.DumperContext
com.facebook.stetho.DumperPluginsProvider
```

Impact: If active, any device on the same network as a user could read payment tokens and loyalty data from local storage and observe live payment traffic, without authentication. The activation state was never confirmed one way or the other; the presence of the debug tooling in a shipped payment binary is itself the finding, independent of whether it is currently switched on.

Fix: Confirm and, if present, strip all Stetho classes from production release builds via ProGuard/R8 exclusion. No confirmation that this has occurred was ever received.

C2: Firebase Initializes Before Any Consent Screen

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.

FirebaseInitProvider is declared with android:initOrder=0x64 (100) and android:direct BootAware=true, meaning it initializes at process creation, before MainActivity, before SplashActivity, and before any consent screen, and can begin before the device is fully unlocked.

```
com.google.firebase.provider.FirebaseInitProvider
  android:initOrder=0x64 (100), android:directBootAware=true
```

Impact: Firebase begins collecting before a user has seen a single consent notice, in a payment-handling application.

Fix: Defer FirebaseInitProvider initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

C3: WeChat Pay Routes Payment Data Through Tencent, a PRC-NSL-Obligated Processor

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

Shell's optional WeChat Pay flow routes transaction data through Tencent's SDK (com.tencent.mm), confirmed via genTokenForOpenSdk and openBusiLuckyMoney content-provider calls and Adyen's WeChatPayActionConfiguration integration class. Tencent is a PRC-incorporated company, fully subject to China's National Security Law Art. 7, an obligation to cooperate with PRC state intelligence on demand, without a court order or user notification. No EU adequacy decision exists for the PRC, and no such transfer is disclosed as a named third-country processor in Shell's privacy documentation as reviewed.

```
content://com.tencent.mm.sdk.comm.provider/genTokenForOpenSdk
content://com.tencent.mm.sdk.comm.provider/openBusiLuckyMoney
com.adyen.checkout.wechatpay.WeChatPayActionConfiguration
```

Impact: A user paying for fuel via WeChat Pay exposes transaction amount, timestamp, merchant identifier, and device identifier to a processor legally obligated to cooperate with PRC state intelligence without notice, with no EU adequacy decision covering the transfer.

Fix: Document an Art. 44-49 transfer mechanism for the WeChat Pay pipeline or remove the integration, and name Tencent as a third-country processor under Art. 13(1)(e). No confirmation that this has occurred was ever received.

H1: Two Competing APM Platforms Capture Payment API Traffic

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.

Both Dynatrace (com.dynatrace.android.agent) and NewRelic mobile agents are compiled into the same binary. Both capture all outbound HTTP requests and responses, including payment-initiation calls to Adyen and Braintree, crash reports with full stack traces, and session data. Both are US companies subject to the CLOUD Act, and neither appears as a named processor in Shell's publicly accessible privacy policy as reviewed.

```
com.dynatrace.agent.OneAgentEventDispatcher
com.dynatrace.android.agent.communication.RequestScheduler
com.newrelic (NewRelic mobile agent)
```

Impact: Payment API calls, token exchange flows, and transaction responses pass through two undisclosed US-based APM processors.

Fix: Name Dynatrace and NewRelic explicitly as processors under Art. 28 and Art. 13(1)(e), or remove the redundant second APM. No confirmation that this has occurred was ever received.

H2: Advertising ID and Attribution Tracking in a Fuel Loyalty App

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

AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_AD_ID are all declared. Advertising attribution tracking and advertising ID collection have no documented purpose in a fuel-station loyalty app and enable linking a user's Shell loyalty activity to their broader device advertising profile. No mention of advertising attribution was located in the privacy policy.

Impact: A user's fuel-purchase and loyalty activity can be linked to their advertising profile across other apps, with no disclosed purpose or legal basis located.

Fix: Document an individual Art. 6(1) legal basis and Art. 13(1)(c) disclosure for the advertising-attribution pipeline, or remove it. No confirmation that this has occurred was ever received.

H3: Two Firebase API Keys Hardcoded and Extractable

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

Two distinct Firebase project API keys are hardcoded in the binary, both extractable in seconds with strings. A misconfigured security rule on either project would allow unauthorized reads or writes; either key also enables quota-exhaustion denial of service against legitimate users of Firebase-dependent features.

```
AIzaSyBcJSdEMhZuz_eX2Y-5tottihqvANTUu3Y
AIzaSyDK8BYuf1PPGFK4nno4R1x1kZC8v6epkPo
```

Impact: Both keys are trivially extractable and, depending on the security-rule configuration behind each, could enable unauthorized database access or quota-exhaustion denial of service.

Fix: Restrict both Firebase API keys by package name and SHA-1 certificate fingerprint, and audit both projects' security rules. No confirmation that this has occurred was ever received.

H4: Boot-Time Auto-Start Registered for Notification Scheduling

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

RECEIVE_BOOT_COMPLETED is declared, with Urban Airship's automation engine also registering for TIME_SET and TIMEZONE_CHANGED to recalculate notification schedules. The app begins running at device boot, before any user interaction or consent flow.

Impact: The app and an embedded notification-scheduling SDK begin running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start and Urban Airship's scheduling recalculation, or gate it behind consent. No confirmation that this has occurred was ever received.

M1: Undocumented RECORD_AUDIO Permission

LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 1.0.

RECORD_AUDIO is declared with no documented voice feature in the app to justify it. A duplicate, malformed permission string (RECORD_AUDI0, a literal zero in place of the letter O) is also present in the manifest, suggesting the permission was added without rigorous review.

```
android.permission.RECORD_AUDIO
android.permission.RECORD_AUDI0  (malformed duplicate: zero instead of letter O)
```

Impact: Microphone access is present in a payment-handling app with no corresponding disclosed feature; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low despite the access itself being undocumented.

Fix: Remove the permission if unused, or document the specific voice feature it supports. No confirmation that this has occurred was ever received.

M2: Braintree (PayPal Subsidiary) as Undisclosed Payment Processor

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.

Braintree, a PayPal subsidiary and US company subject to the CLOUD Act, handles 3D Secure flows and PayPal vault payments (com.braintreepayments.api.PayPalAccount Nonce, .ThreeDSecureActivity, .PayPalVaultRequest). It is not identified as a named processor in Shell's privacy documentation as reviewed.

Impact: Card details and vaulted payment tokens pass through an undisclosed US-based processor subject to the CLOUD Act.

Fix: Name Braintree explicitly as a processor under Art. 28 and Art. 13(1)(e). 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, Art. 5(1)(f)	C1	Debug-inspection tooling compiled into a production payment binary.
Art. 7, Art. 25	C2	Pre-consent Firebase initialization via a directBootAware ContentProvider.
Art. 44-49, Art. 13(1)(e)	C3	Undisclosed transfer of payment data to a PRC-NSL-obligated processor.
Art. 28, Art. 13(1)(e)	H1	Two undisclosed US-based APM processors capturing payment API traffic.
Art. 5(1)(b), Art. 6(1)	H2	Undisclosed advertising-attribution tracking.
Art. 5(1)(f), Art. 32	H3	Two hardcoded, trivially extractable Firebase API keys.
Art. 28, Art. 13(1)(e)	M2	Undisclosed Braintree/PayPal payment processor.

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 and C3 reach HIGH on their computed CVSS v4.0 scores alone, no editorial escalation applied; C2, H1, H2, H3, and M2 correct to MEDIUM to match their own computed bands; M1 corrects to LOW on its own computed band; H4 is classified OBSERVATIONAL because boot-time auto-start alone carries no direct scoreable impact. C1's activation state was never independently confirmed, since the dynamic analysis required to do so was never reached. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: SHELL-2026-R1.