Coordinated Security & Privacy Disclosure, Final Report

Klarna for Android (com.myklarnamobile)

Licensed EU bank, a bug-bounty-only stance repeated three times in one day, a Swedish DPA reply that took no action, two questions never answered by anyone

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, THREE REDIRECTS, ONE REGULATOR NOTED FOR INFORMATION ONLY, ZERO SUBSTANTIVE ANSWERS

Target	Klarna Bank AB, Stockholm, Sweden
Product audited	Klarna for Android, com.myklarnamobile v26.25.309
Disclosure reference	REF KLARNA-C1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Chucker interceptor / C3 Firebase, 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

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Positive Observations 4

4 Findings 4

4.1 C1: Chucker HTTP interceptor active in production, logging credit and payment data . . . 5

4.2 C2: FullStory session replay on payment, IBAN, credit-application, and debt-repayment screens . . . 5

4.3 C3: Two hardcoded Firebase API keys in the production APK . . . 6

4.4 H1: LexisNexis Risk / ThreatMetrix device fingerprinting feeding automated credit decisions . . . 6

4.5 H2: Plaid: EU bank-account access via a US aggregator . . . 7

4.6 H3: Persona KYC: facial biometrics and government ID to a US company . . . 7

4.7 H4: CoBrowse live agent screen-share and Rokt post-transaction ad injection 7

4.8 H5: Tencent MMKV: PRC-origin code in EU banking infrastructure . . . 8

5 Klarna's Response, and the Swedish Data Protection Authority's, Recorded in Full 8

6 Data Protection, Article by Article 9

7 Disclosure Timeline & Outcome 10

8 Residual Risk & Recommendations 11

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Klarna Android application, a licensed EU bank's consumer credit and payment platform, and identified eight findings, three CRITICAL, five HIGH. The most significant: the Chucker debug HTTP interceptor is active in production, logging credit-application data, payment authorization responses, Plaid bank-linking traffic, and KYC verification responses to a local plaintext database with a system notification, the most severe instance of this class of finding in RFI-IRFOS's audit series to date.

FullStory session replay, 178 classes, records every tap on payment, IBAN-entry, credit-application, and debt-repayment screens, transmitted to US servers. Two hardcoded Firebase API keys were also extracted from the production binary.

Klarna's Accountable Lead Offensive Security redirected the disclosure to Klarna's HackerOne bug bounty program three times on the day of first contact, ultimately declaring the matter closed from a security-vulnerability-triage perspective and routing two specific privacy questions to unnamed internal functions that never answered them. The Swedish data protection authority, IMY, replied the same week that it had received the filing for information only and would take no action absent a formal complaint, a position RFI-IRFOS's own correspondence is careful to distinguish from any supervisory finding on the merits. A generic customer-support reply from a separate Klarna mailbox on 19 August asked RFI-IRFOS to provide an account email and date of birth to 'locate the correct account,' treating a regulatory disclosure as a customer service query. All eight findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026 to Klarna's Privacy and Security teams. Mats Engman, Klarna's Accountable Lead Offensive Security, redirected the disclosure to Klarna's HackerOne bug bounty program three times within a single day, the third time declaring the case closed from a security-vulnerability-triage perspective and routing the two privacy questions to unnamed 'appropriate Klarna functions.' The Swedish data protection authority, IMY, acknowledged receipt as information only and stated it would take no action absent a formal complaint. Neither Klarna's unnamed privacy function nor IMY on the merits ever answered the two questions RFI-IRFOS raised on 20 June.

ID	Severity	Title
C1	CRITICAL	Chucker HTTP interceptor active in production, logging credit and payment data
C2	CRITICAL	FullStory session replay on payment, IBAN, credit-application, and debt-repayment screens

ID	Severity	Title
C3	CRITICAL	Two hardcoded Firebase API keys in the production APK
H1	HIGH	LexisNexis Risk / ThreatMetrix device fingerprinting feeding automated credit decisions
H2	HIGH	Plaid: EU bank-account access via a US aggregator
H3	HIGH	Persona KYC: facial biometrics and government ID to a US company
H4	HIGH	CoBrowse live agent screen-share and Rokt post-transaction ad injection
H5	HIGH	Tencent MMKV: PRC-origin code in EU banking infrastructure

Subject & Operator Analysis

Klarna Bank AB (Stockholm, Sweden) is a licensed EU bank offering consumer credit, payment, and buy-now-pay-later services, supervised by Finansinspektionen and, for data protection, IMY.

Positive Observations

- TLS certificate pinning is correctly implemented for primary API endpoints, a meaningfully stronger baseline than the majority of RFI-IRFOS's 2026 audit series.
- No cleartext HTTP traffic exceptions were identified in the network security configuration.

Findings

C1: Chucker HTTP interceptor active in production, logging credit and payment data

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

com.chuckerteam.chucker is active in the production binary, capturing credit application data, payment authorization responses, Plaid account-linking traffic, KYC verification responses, transaction history, and authentication tokens to a local plaintext SQLite database with a persistent system notification.

Klarna's 22 June reply, 14:14, disputes the finding's validity in general terms rather than this specific one: "we do not consider the report to contain a validated exploitable security vulnerability or a confirmed personal data breach... Several assertions rely on static SDK or class presence and extrapolate to conclusions not supported by runtime evidence." No Klarna reply at any point addressed Chucker's compiled presence specifically, requested a version/build hash to reconcile it, or confirmed whether the interceptor is gated behind a runtime flag in the distributed production build.

Impact: If active as compiled, a debug interceptor in a licensed bank's production app locally persists complete financial transaction and KYC data in plaintext, a direct PSD2 Art. 95 and EBA/GL/2019/04 exposure.

Fix: Confirm whether Chucker is gated at runtime in the distributed build, publish the specific build configuration, and remove the dependency from the production build variant entirely regardless.

C2: FullStory session replay on payment, IBAN, credit-application, and debt-repayment screens

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

178 FullStory classes record and transmit tap-level session replay data from the app's payment, IBAN-entry, credit-application, and debt-repayment screens to US servers.

The recurring standing question, restated in every RFI-IRFOS follow-up from 17 July through 4 September, unanswered: does FullStory have active session recordings of Klarna users specifically on payment, credit-application, or debt-repayment screens? No Klarna reply, from Mats Engman, from privacy@klarna.com, or from IMY, has answered this yes-or-no question.

Impact: Session replay capturing financial-hardship and payment-detail screens, if active, engages GDPR Art. 5(1)(c) and Art. 9(1) directly, and is transmitted to a US third party.

Fix: Answer directly whether FullStory session recording is active on the named screens, and if so, publish the Art. 46 transfer mechanism and the specific data minimization applied to financial-hardship contexts.

C3: Two hardcoded Firebase API keys in the production APK

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

Two distinct Firebase API keys, AIzaSyAS1FfISxdn7kamCpcBpxL9YwPDEWZ53qM and AIzaSyBWD4xSNN7qGAjXNiS9czXIAw1Qm4kbJgs, extracted from the production binary, database klarna-app.firebaseio.com (stated disabled by Klarna, key itself remains valid in every distributed copy).

Not individually addressed in any Klarna reply beyond the general 22 June statement that findings rely on "static SDK or class presence."

Impact: A publicly extractable key on a licensed bank's app enables, at minimum, quota-exhaustion and probing exposure regardless of the stated database's disabled status, since the key itself is not confirmed revoked.

Fix: Confirm the key is fully revoked, not merely pointed at a disabled database, and restrict any replacement to the production certificate fingerprint.

H1: LexisNexis Risk / ThreatMetrix device fingerprinting feeding automated credit decisions

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

Device fingerprinting data is transmitted to LexisNexis Risk/ThreatMetrix, a US data broker, for use in credit scoring.

The second recurring standing question, restated in every follow-up from 17 July through 4 September, unanswered: who at Klarna is the correct contact for Art. 22 GDPR automated-decision-making concerns specific to this device profiling feeding into credit decisions? No Klarna reply has named a contact or a decision-review process.

Impact: Automated credit decisions may rely on device-fingerprint data with no confirmed Art. 22 human-review pathway or data broker transfer safeguard disclosed to the applicant.

Fix: Name the specific internal function responsible for Art. 22 review of this data flow, and disclose the Art. 44-49 transfer basis for LexisNexis Risk/ThreatMetrix.

H2: Plaid: EU bank-account access via a US aggregator

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

3,461 Plaid classes broker EU bank-account access through a US-based account-aggregation service.

Not individually addressed in any Klarna reply. RFI-IRFOS's original disclosure noted Plaid's 2022 US class-action settlement (approximately $58M) concerning its data-collection practices as relevant context for the scale of financial data an aggregator of this kind can access.

Impact: Direct EU bank-account access is intermediated by a US aggregator with no Art. 46 transfer mechanism confirmed in this correspondence.

Fix: Disclose Plaid as a named Art. 28 sub-processor with its applicable transfer mechanism.

H3: Persona KYC: facial biometrics and government ID to a US company

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

6,398 Persona classes, the largest single SDK in the application, process facial biometric and government identity document data for KYC verification.

Not individually addressed in any Klarna reply beyond the general 22 June statement that findings are unsupported by runtime evidence.

Impact: Art. 9(1) special-category biometric data is processed by a US KYC vendor with no Art. 46 transfer confirmation in this correspondence.

Fix: Name Persona as an Art. 28 sub-processor for biometric KYC data specifically, publish its transfer mechanism, and confirm the Art. 9(2)(a) legal basis relied upon.

H4: CoBrowse live agent screen-share and Rokt post-transaction ad injection

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

312 CoBrowse classes (live customer-support screen-sharing) and 3,463 Rokt classes (post-transaction advertising injection) are both present in the production binary.

Not individually addressed in any Klarna reply.

Impact: A live screen-sharing capability alongside post-transaction ad injection on a financial application both warrant explicit, separately disclosed consent bases.

Fix: Disclose CoBrowse and Rokt as named data recipients under Art. 13(1)(e), each with its own consent basis.

H5: Tencent MMKV: PRC-origin code in EU banking infrastructure

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

Tencent's MMKV key-value storage library is compiled into the production binary of a licensed EU bank's application.

Not individually addressed in any Klarna reply. RFI-IRFOS's standing concern, applied consistently across every case in this research series carrying PRC-origin SDKs, is China's National Intelligence Law (2017) and PIPL as a structural transfer-risk question independent of MMKV's specific function as a local storage library.

Impact: A PRC-origin component in a licensed bank's application raises a structural Art. 44 transfer-risk question regardless of the library's narrow local-storage function.

Fix: Confirm whether MMKV can be replaced with a non-PRC-origin equivalent, or document the specific data (if any) it handles and the applicable transfer safeguard.

Klarna's Response, and the Swedish Data Protection Authority's, Recorded in Full

Mats Engman, Klarna's Accountable Lead Offensive Security, replied three times on 22 June 2026 alone. First, 07:58: "The Klarna app is in scope in our public bug bounty program. You can find our program here: https://hackerone.com/klarna." RFI-IRFOS declined, 08:02: "we will not be using the HackerOne portal. this is not a bug bounty submission. this is a formal regulatory disclosure from a registered Austrian research institute to a licensed EU bank." Second, 11:50: "security findings must be submitted through Klarna's established VDP process... Based on the evidence submitted, we do not consider the report to contain a validated exploitable security vulnerability." Third, 14:14: "we do not consider the report to contain a validated exploitable security vulnerability or a confirmed personal data breach... privacy/legal-basis/international-transfer questions are handled by the appropriate Klarna functions... we consider this matter closed from a security-vulnerability triage perspective and will not continue debating unsupported or repetitive assertions by email."

The Swedish data protection authority, IMY, replied on 2 July 2026, in full: "IMY har fått del av din skrivelse. Vi bedömer att skrivelsen endast har skickats till myndigheten för kännedom och vi kommer därför inte att vidta några åtgärder" ("IMY has received your letter. We assess that the letter was sent to the authority for information only, and we will therefore not take any action"). RFI-IRFOS's own correspondence is explicit that this is a procedural, for-information acknowledgment, not a supervisory finding on the merits: "it isn't ours, and it isn't IMY's supervisory finding either, no supervisory authority has reviewed this on the merits yet."

On 19 August 2026, a reply arrived from a separate mailbox, privacy@klarna.com, ticket #6985266, signed by a Service Specialist at Klarna's customer service center: "we need you to clarify what specific assistance you are requesting from Klarna customer support... please also provide the email address registered to your Klarna account and your date of birth (mm/dd/yyyy), so we can locate the correct account." A regulatory disclosure, cc'ing a supervisory authority, was answered by a request to verify a personal customer account.

Two questions, repeated in every RFI-IRFOS follow-up from 17 July through 4 September, were never answered by Klarna Security, by the customer-support mailbox, or by IMY: whether FullStory has active session recordings on payment, credit-application, or debt-repayment screens, and who at Klarna is the correct Art. 22 contact for the LexisNexis/Thre

atMetrix device-profiling finding feeding into credit decisions. A third question, on Chucker's removal and SHA-256 re-verification, was added 18 August and is equally unanswered.

Data Protection, Article by Article

Finding	Provision	Concern
C1	PSD2 Art. 95; EBA/GL/2019/04 4.3; GDPR Art. 32	Debug interceptor logging financial and KYC data in production
C2	GDPR Art. 5(1)(c), Art. 9(1)	Session replay on payment and financial-hardship screens
C3	GDPR Art. 32(1)(b)	Hardcoded, publicly extractable credentials
H1	GDPR Art. 22	Automated credit decisioning, device fingerprinting, no named review contact
H2	GDPR Art. 44, Art. 13(1)(e)(f)	US aggregator bank-account access
H3	GDPR Art. 9(1)	Biometric KYC data to a US processor
H4	GDPR Art. 13(1)(e)	Undisclosed screenshare and post-transaction ad injection
H5	GDPR Art. 44	PRC-origin component in EU banking infrastructure

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to Klarna Privacy/Security, cc IMY, Austrian DSB, CERT.at; 8 findings
2026-06-22	Three redirects/rejections from Mats Engman within one day; final one declares triage closed, routes privacy questions elsewhere
2026-07-02	IMY: received for information only, no action absent a formal complaint
2026-07-17 / 07-27 / 08-09	Follow-ups restate the two open questions; no answer from any party
2026-08-18	Follow-up formally documents the reassignment-then-closure pattern, adds a third question, sets 25 August deadline
2026-08-19	Generic customer-support reply, ticket #6985266, requests account email and date of birth
2026-09-04	Final follow-up, 76 days since R1, restates all open items
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Across 91 days, Klarna's security function redirected the disclosure to a bug bounty portal three times in one day, then closed its own triage while reassigning two specific privacy questions to functions that never answered. The Swedish data protection authority treated the filing as informational only, explicitly declining to assess the underlying claims. A third, unrelated Klarna mailbox treated the disclosure as a customer support ticket requiring account verification. No party at any point provided a substantive technical or legal answer to either standing question.

Residual Risk & Recommendations

- Answer directly: is FullStory session recording active on payment, credit-application, or debt-repayment screens?
- Name the specific internal contact responsible for Art. 22 review of the LexisNexis/ThreatMetrix credit-decisioning data flow.
- Confirm Chucker's build-time exclusion from production and provide a SHA-256 hash for independent re-verification.
- Disclose Plaid and Persona as named Art. 28 sub-processors with their respective transfer mechanisms.
- Route regulatory and security disclosures received by any Klarna mailbox, including customer support, to a function equipped to answer them rather than requesting account-holder verification.

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, 22, 32, 44; PSD2 Art. 95. REF KLARNA-C1-2026-R1.