



Security & Privacy Disclosure, Final Report

SumUp Business Android (com.kaching.merchant)

A merchant payment and banking app persists Plaid bank access tokens, bundles four biometric identity vendors at once and starts Firebase before consent, and the first disclosure never reached the privacy mailbox it was addressed to

PUBLIC DISCLOSURE, 17 OCTOBER 2026: EMBARGO REACHED 3 OCTOBER 2026, FIVE MESSAGES SENT, TWO BOUNCED, NO REPLY FROM SUMUP, THREE QUESTIONS UNANSWERED

Target	SumUp Limited (Dublin, Ireland), SumUp Payments Limited (London), SumUp EU Payments UAB (Vilnius), named as joint controllers in the app privacy policy
Package	com.kaching.merchant v2.173.0 (label: SumUp Business)
Platform Audited	Android, root level code analysis of the production APK
Initial Disclosure (R1)	2026-07-05, addressed to privacy@sumup.com (bounced, 550 5.1.1), delivered in CC to support@sumup.com, press@sumup.com, Austrian Datenschutzbehörde, EDPS and Irish Data Protection Commission
Disclosure / Embargo Date	2026-10-03
Report Published	2026-10-17
Overall Severity	HIGH
Findings	8 (4 High, 3 Medium, 1 Low, 0 Critical)
Correspondence	5 messages sent by RFI-IRFOS over 69 days (2026-07-05 to 2026-09-12); the first two went to privacy@sumup.com and bounced; the DPO address dpo@sumup.com received the last three; 0 replies from SumUp; 1 automatic reply from the Irish DPC contact channel on 2026-08-24; 35 days of silence after the last message
Authorities Notified	Austrian Datenschutzbehörde · EDPS · Irish Data Protection Commission

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

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	H1: Live Plaid (US) open-banking integration persists external bank account access tokens	5
4.2	H2: Four overlapping biometric and liveness identity vendors bundled simultaneously	6
4.3	H3: Pre-consent Firebase and ML Kit auto-init, no working CMP behind the Cookies Preferences screen	6
4.4	H4: No certificate pinning on the payment authorisation and open-banking channel	7
4.5	M1: Repealed standard contractual clauses cited in the live published merchant DPA	7
4.6	M2: Three hardcoded Google API keys including a live Firebase Realtime Database URL	8
4.7	M3: Advertising attribution permissions and a five-vendor marketing stack on a B2B payment app	8
4.8	L1: Location, contacts and call permissions each with an identifiable purpose	9
5	Impact Analysis	9
6	The Complete Chain: Five Messages, Two Bounces, 104 Days, Zero Replies	9
7	Data Protection: Article by Article	10
8	Regulatory & Legal Landscape	10
9	Indicators of Compromise	11
10	Disclosure Timeline & Outcome	11
11	Residual Risk & Recommendations	12

Executive Summary

SumUp Business is the merchant app for card acceptance and the SumUp business account. Root level code analysis of production APK v2.173.0 shows a large product with real engineering depth: jPOS ISO 8583 messaging, Play Integrity through Firebase App Check, an isolated Tap to Pay process, cleartext allowed only for 76 private LAN addresses, Mixpanel on its EU endpoint, and a dedicated anti-spoofing package query list.

Four findings carry HIGH weight. H1: a live Plaid Link integration saves a Plaid access token through SavePlaidAccessTokenUseCase, a standing credential on a merchant external bank account. H2: Onfido, FaceTec, Sumsu and Unico/Acesso Bio ship in one global APK for the same purpose of merchant identity verification, each with live endpoints, processing Art. 9 biometric data. H3: Firebase and ML Kit providers start at process creation with no working consent layer. H4: no certificate pinning on the payment and open-banking channel. Three MEDIUM findings cover a published merchant DPA that still cites the repealed 2010/87/EU standard contractual clauses, three hardcoded Google keys with a live Realtime Database URL (withheld), and a five-vendor marketing stack.

The first disclosure of 5 July 2026 and the follow-up of 24 July were addressed to privacy@sumup.com, which returned 550 5.1.1 on both occasions. Both messages reached support@sumup.com, press@sumup.com and the authorities in CC. RFI-IRFOS corrected the address on 9 August 2026 after finding dpo@sumup.com in the live SumUp privacy policy, and sent three further messages there (9 August, 24 August, 12 September). SumUp never replied. The embargo of 3 October 2026 passed 14 days before publication.

ID	Severity	Title
H1	HIGH	Live Plaid (US) open-banking integration persists external bank account access tokens
H2	HIGH	Four overlapping biometric and liveness identity vendors bundled simultaneously
H3	HIGH	Pre-consent Firebase and ML Kit auto-init, no working CMP behind the Cookies Preferences screen
H4	HIGH	No certificate pinning on the payment authorisation and open-banking channel
M1	MEDIUM	Repealed standard contractual clauses cited in the live published merchant DPA
M2	MEDIUM	Three hardcoded Google API keys including a live Firebase Realtime Database URL
M3	MEDIUM	Advertising attribution permissions and a five-vendor marketing stack on a B2B payment app
L1	LOW	Location, contacts and call permissions each with an identifiable purpose

Subject & Operator Context

SumUp operates as a multi-entity group. The app privacy policy names SumUp Payments Limited (England and Wales, 07836562), SumUp Limited (Ireland, 505893, Central Bank of Ireland EMI licence C195030, also the code signing entity of the APK) and SumUp EU Payments UAB (Lithuania, 305074395) jointly as controllers. SumUp Services GmbH, Berlin, appears as the CE marking manufacturer for card readers. The Irish Data Protection Commission is the plausible lead authority; this is a candidate determination for SumUp to confirm, not a finding of fact. No named DPO is published; the live privacy policy lists dpo@sumup.com.

Engagement Summary

The R1 letter of 5 July 2026 went to privacy@sumup.com, the mailbox listed in the findings research, and bounced within the minute. RFI-IRFOS repeated the same address on 24 July and stated that this was the first delivery to a working address, which was wrong because no address check was made before that send. The error was corrected in writing on 9 August 2026. The substance of the R1 reached SumUp through the CC addresses support@sumup.com and press@sumup.com from 5 July 2026; the data protection officer address received the findings first on 9 August 2026, 55 days before the embargo date and 69 days before this publication. The embargo date of 3 October 2026 stayed unchanged throughout.

Findings

H1: Live Plaid (US) open-banking integration persists external bank account access tokens

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 (persisted bank access token)

```
com.sumup.bank.account.ui.plaid.BankAccountAddPlaidFragment / ViewModel / Repository /  
Service  
plaid/CreatePlaidAccountUseCase, GetAccountHolderNameUseCase, GetPlaidLinkTokenUseCase  
, SavePlaidAccessTokenUseCase  
https://production.plaid.com/ https://sandbox.plaid.com/ https://development.plaid.  
com/  
StartupActivity deep links: /screen/open-banking, /screen/link-card
```

Impact: SumUp wraps Plaid Link in its own repository and use-case classes and saves the resulting access token through SavePlaidAccessTokenUseCase. A saved token is a standing authorisation on a merchant external bank account, held via a US financial data aggregator. All four Plaid environments appear as literal endpoints.

H2: Four overlapping biometric and liveness identity vendors bundled simultaneously

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 (Art. 9 biometric data)

```
Onfido: CoreActivity, OnfidoActivity, CaptureActivity (:onfido_process), api.onfido.com/v3/  
FaceTec: com.facetec.sdk.FaceTecSessionActivity  
Sumsb: SNSAppActivity, api.sumsb.com ; com.sumup.kyc.eid.features.SumsbTestActivity  
Unico: SelfieXActivity, DocumentXActivity, io.unico.liveness.*
```

Impact: Onfido, FaceTec, Sumsb and Unico/Acesso Bio each ship Activities and live API endpoints in the single global APK, next to SumUp KYCActivity and ForceKycActivity. Face geometry, liveness video and ID documents are special category data under Art. 9, spread across four processors for one purpose. A SumsbTestActivity ships in the release build.

H3: Pre-consent Firebase and ML Kit auto-init, no working CMP behind the Cookies Preferences screen

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9 (pre-consent analytics)

```
AndroidManifest.xml: FirebaseInitProvider initOrder=100 directBootAware=true ;  
    MLKitInitProvider initOrder=99  
    AppMeasurementReceiver / Service / JobService enabled=true  
    io.sentry.auto-init=false  
res/values/strings.xml: sumup_cookie_preferences = "Cookies Preferences"
```

Impact: Firebase and Google Measurement components initialise as ContentProviders during Application creation, mechanically before any screen or consent notice can render. Processing starts on first launch for every installation, before consent can be given. A Cookies Preferences string exists, and no consent banner copy or CMP vendor appears in the binary. Sentry auto-init is disabled in the same manifest, so the team controls SDK start where it chooses to. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the processing starts on every installation of a merchant payment and banking app before any consent surface can render, across several marketing vendors.

H4: No certificate pinning on the payment authorisation and open-banking channel

HIGH, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 7.6 (payment channel TLS trust)

```
res/xml/network_security_config.xml: debug-overrides user trust; domain-config  
  cleartext only for 76 RFC 1918 addresses;  
  no base-config, no pin-set  
CertificatePinner in classes13.dex, classes17.dex, classes24.dex ; grep sha256/ pin  
  values -> no match in 25 dex files
```

Impact: TLS trust rests on the device system CA store alone. A party that controls a trusted root on the device (enterprise MDM profile, security software, rooted or compromised hand-set) can read and modify the channel between the app and its backend. The channel carries card payment authorisation, Plaid tokens and KYC traffic. Three shaded CertificatePinner copies ship in the dex without a single pin value.

M1: Repealed standard contractual clauses cited in the live published merchant DPA

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (outdated transfer instrument)

```
http://legal.sumupecommerce.com/en/dpa/ (fetched 2026-07-05):  
"...shall be undertaken in accordance with the Standard Contractual Clauses  
  (2010/87/EU)..."
```

Impact: The public SumUp merchant DPA names Standard Contractual Clauses 2010/87/EU as the transfer instrument. Commission Implementing Decision 2021/914 replaced them, with a migration deadline of 27 December 2022. A merchant reading the document today relies on a legal basis that no longer exists.

M2: Three hardcoded Google API keys including a live Firebase Realtime Database URL

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9 (keys and database URL)

```
AndroidManifest.xml com.google.android.geo.API_KEY: [REDACTED IN PUBLIC REPORT --  
disclosed privately in R1]  
res/values/strings.xml google_api_key, firebase_database_url: [REDACTED IN PUBLIC  
REPORT -- disclosed privately in R1]  
classes15.dex Static Maps key: [REDACTED IN PUBLIC REPORT -- disclosed privately in R1  
]
```

Impact: A Maps key in the manifest, a Firebase key with a Realtime Database URL in strings.xml and a Static Maps key in classes15.dex are readable by any party decompiling the APK. Google documents such keys as non-confidential; the exposure is quota and billing abuse plus reliance on correct database rules.

M3: Advertising attribution permissions and a five-vendor marketing stack on a B2B payment app

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (marketing stack)

```
AndroidManifest.xml: AD_ID, ACCESS_AD SERVICES_ATTRIBUTION,  
BIND_GET_INSTALL_REFERRER_SERVICE  
Mixpanel endpoint api-eu.mixpanel.com ; Optimizely DatafileRescheduler,  
EventRescheduler
```

Impact: AD_ID and ACCESS_AD SERVICES_ATTRIBUTION sit beside AppsFlyer, Firebase Measurement, Mixpanel, Iterable and Optimizely. The wide-open allowAllToAccess configuration found in the Bluecode case is absent here. Two Optimizely receivers run on BOOT_COMPLETED.

L1: Location, contacts and call permissions each with an identifiable purpose

LOW, CVSS v4.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0
(permission scope)

AndroidManifest.xml: ACCESS_FINE_LOCATION, READ_CONTACTS, GET_ACCOUNTS, CALL_PHONE,
MANAGE_OWN_CALLS

Impact: Each permission maps to a feature: location to card-present payments, contacts to payment links, call permissions to VoIP support callback. Coarse location would be the narrower grant.

Impact Analysis

The technical findings concern a payment and banking product with a large sensitive data surface: biometric verification data, bank account tokens and card payment authorisation. The procedural record adds a second fact: the privacy mailbox published in the first research pass did not exist, and no SumUp reply followed any of the three messages sent to the DPO address.

The Complete Chain: Five Messages, Two Bounces, 104 Days, Zero Replies

Step 1: Disclosure sent on 5 July 2026 to privacy@sumup.com with support@, press@ and three authorities in CC. The address bounced with 550 5.1.1 within the minute.

Step 2: Follow-up on 24 July 2026 to the same address, bounced again.

Step 3: On 9 August 2026 RFI-IRFOS corrects the address to dpo@sumup.com, taken from the live SumUp privacy policy, documents its own error in the message and resends the findings and three questions. No reply.

Step 4: Follow-up on 24 August 2026 to dpo@sumup.com. The only response is an automatic message from the Irish DPC general contact channel, which states that it does not accept reports under the EU AI Act. No reply from SumUp.

Step 5: Follow-up on 12 September 2026, 69 days after the first message. No reply.

Step 6: Embargo passes on 3 October 2026 with the correspondence unanswered.

Step 7: Publication on 17 October 2026 with the full record intact: five messages, two bounces, zero replies from SumUp.

Data Protection: Article by Article

Art. 44, Art. 13(1)(f)/14(1)(f), Art. 5(1)(a), Art. 28 GDPR: H1, Plaid token persistence and the missing transfer disclosure.

Art. 9, Art. 5(1)(c), Art. 25, Art. 35, Art. 28 GDPR: H2, four biometric vendors for one purpose.

Art. 6(1), Art. 7(1), Art. 5(1)(a) GDPR and Art. 5(3) ePrivacy: H3, pre-consent initialisation.

Art. 32(1)(a)(b) GDPR: H4, pinning absent on a payment and open-banking channel.

Art. 44, Art. 46(2)(c), Art. 5(1)(a) GDPR: M1, the published DPA cites Decision 2010/87/EU, repealed with a migration deadline of 27 December 2022.

Art. 32(1)(b), Art. 5(2) GDPR: M2. Art. 5(1)(c), Art. 25 GDPR: M3 and L1.

Regulatory & Legal Landscape

Three entities in Ireland, the United Kingdom and Lithuania appear as joint controllers. The Irish Data Protection Commission was in CC on the first four messages and is the plausible lead authority. The Bank of Lithuania and the UK ICO keep independent competence for their regulated entities.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 28, Art. 32 and Art. 35 issues in H1, H2 and H4, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 5, Art. 6, Art. 7, Art. 9 and Art. 44 issues, up to EUR 20,000,000 or 4% of total worldwide annual turnover. The published merchant DPA citing a repealed transfer instrument is verifiable by anyone at the public URL. The privacy mailbox listed in the first research pass did not exist, and the operator reached its own DPO address through a published link on its live privacy policy.

Indicators of Compromise

Root level code analysis of the published application. No servers, accounts or infrastructure of the operator were probed. Credentials and identifiers referenced below are withheld from this public report; full values were disclosed privately in the R1 letter.

```
H1: com.sumup.bank.account.ui.plaid.* ; SavePlaidAccessTokenUseCase ; production.plaid.com, sandbox.plaid.com

H2: Onfido (:onfido_process), FaceTec, Sumsup (api.sumsup.com), Unico/Acesso Bio ; SumsupTestActivity in release build

H3: FirebaseInitProvider initOrder=100, MLKitInitProvider initOrder=99 ; sumup_cookie_preferences string without consent copy

H4: res/xml/network_security_config.xml has no base-config and no pin-set ; CertificatePinner in classes13, classes17, classes24 without pin values

M1: legal.sumupecommerce.com/en/dpa cites Standard Contractual Clauses (2010/87/EU)

M2: three Google API keys and firebase_database_url [REDACTED IN PUBLIC REPORT -- disclosed privately in R1]

M3: AD_ID, ACCESS_ADSEVICES_ATTRIBUTION ; AppsFlyer, Firebase, Mixpanel, Iterable, Optimizely
```

Disclosure Timeline & Outcome

2026-07-05 Initial disclosure addressed to privacy@sumup.com. Bounced 550 5.1.1. Delivered in CC to support@, press@ and authorities. Embargo stated as 2026-10-03.

2026-07-24 Follow-up to privacy@sumup.com. Bounced again.

2026-08-09 Address corrected to dpo@sumup.com, error documented, findings and questions resent. No reply.

2026-08-24 Follow-up to dpo@sumup.com. Automatic reply from the Irish DPC contact channel only. No reply from SumUp.

2026-09-12 Follow-up to dpo@sumup.com, 69 days after the first message. No reply.

2026-10-03 Embargo date reached and passed with no reply.

2026-10-17 This report published, 14 days after the embargo. Correspondence record: five messages, two bounces, zero replies from SumUp, zero of three questions answered.

Residual Risk & Recommendations

H1: disclose the Plaid legal entity, the Chapter V transfer mechanism and the token retention period before the Plaid Link flow starts.

H2: document why four biometric vendors serve one purpose, route by market, remove unused SDKs from the global build and complete the Art. 35 DPIA.

H3: hold Firebase and ML Kit initialisation until consent is recorded and put real consent copy behind the Cookies Preferences screen.

H4: ship a pin-set for the SumUp API, Plaid, Onfido and Sumsup domains.

M1: replace the repealed 2010/87/EU reference with the 2021/914 clauses in the published DPA.

M2: restrict all three Google keys and verify the Realtime Database rules.

M3: remove AD_ID and attribution permissions that no function needs.

Procedural: keep dpo@sumup.com monitored and reply in writing to the three questions. RFI-IRFOS will update this report with any substantive reply.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from root level code analysis of

the published application using publicly available tooling. No operator servers, accounts or infrastructure were probed. Credentials and database identifiers are withheld from this public report; full values were disclosed privately in the original R1 letter and remain available to the operator or to a supervisory authority on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF SUMUP-2026-R1-001.