



Security & Privacy Disclosure, Final Report

IONITY for Android (com.cleevio.ionity.android.app, versionCode 2088093427 / v2.500.1)

AWS Cognito AppClientSecret hardcoded in every Play Store install — full OAuth2 backend authentication compromise on a pan-European EV charging joint venture of BMW, Ford, Hyundai, Mercedes-Benz, and Volkswagen Group

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26 SEPTEMBER 2026, FOUR FINDINGS REMAIN UNADDRESSED

Target	IONITY GmbH
Package	com.cleevio.ionity.android.app
Versions Audited	versionCode 2088091998 (initial, 2026-06-26) · versionCode 2088093427 / v2.500.1 (re-verification, 2026-10-17)
Joint Venture	BMW Group · Ford Motor Company · Hyundai Motor Group · Mercedes-Benz AG · Volkswagen Group
Disclosure Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (3 Critical, 1 High)
CISO Engaged	Michael Kanhäuser, 2026-08-19
Authorities Notified	Austrian DSB · German BfDI · Bavarian BayLDA

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 & Infrastructure Context	5
3	Engagement Summary	5
4	Findings	6
4.1	C1: AWS Cognito AppClientSecret hardcoded in res/raw/amplifyconfiguration.json — full OAuth2 backend authentication compromise	6
4.2	C2: Firebase API key, Google App ID, and Cloud Storage bucket hardcoded in res/values/strings.xml	7
4.3	C3: FirebaseInitProvider (initOrder=100) and MIKitInitProvider (initOrder=99) — 2x pre-consent SDK initialisation on every cold start, RECEIVE_BOOT_COMPLETED registered	7
4.4	H1: Braze marketing SDK (New York) receives behavioural data from EV charging and payment session interactions	8
5	Impact Analysis	8
6	The Complete Chain: App to Account Takeover	9
7	Data Protection — Article by Article	10
8	Critical Infrastructure & NIS2 Context	11
9	Regulatory & Legal Landscape	11
10	Indicators of Compromise	12
11	Disclosure Timeline & Outcome	13
12	What IONITY Got Right	13
13	Residual Risk & Recommendations	14

Executive Summary

IONITY GmbH operates pan-European high-power EV charging infrastructure as a joint venture of BMW Group, Ford Motor Company, Hyundai Motor Group, Mercedes-Benz AG, and Volkswagen Group — five of the world's largest automotive manufacturers. IONITY accounts store payment methods, subscription tiers, RFID charging card associations, and full session-by-session charging histories for hundreds of thousands of users across seventeen European countries.

The production Android application ships with an AWS Cognito AppClientSecret hardcoded in a plaintext JSON configuration file. This is the private half of a server-side OAuth2 credential pair that AWS explicitly documents must never be embedded in a public client binary. Any Android developer with standard reverse-engineering tooling can extract this file in under sixty seconds, compute valid SECRET_HASH values, and interact with IONITY's Cognito User Pool as the official IONITY application — probing user accounts, initiating authentication flows, and invoking authenticated API endpoints.

Three additional findings were identified: Firebase API key and Cloud Storage bucket hardcoded in the binary, two SDK ContentProviders initialising data collection before any consent screen is shown (structural GDPR Art. 7(1) violation), and a Braze marketing platform receiving behavioural events from subscription, payment, and charging session interactions.

RFI-IRFOS disclosed these findings under REF IONITY-2026 on 26 June 2026. After seven follow-up contacts with no reply, IONITY's CISO Michael Kanhäuser replied on 19 August 2026, confirmed the findings had been shared with Security, Privacy, and Engineering teams, and indicated interest in a separate security engagement. The 90-day embargo elapsed on 26 September 2026. Re-verification against v2.500.1 on 17 October 2026 confirms all four findings remain unaddressed — the AppClientSecret value is unchanged and now appears in two locations within the same configuration file, compared to one location in the originally audited build.

ID	Severity	Title
C1	CRITICAL	AWS Cognito AppClientSecret hardcoded in res/raw/amplifyconfiguration.json — full OAuth2 backend authentication compromise
C2	CRITICAL	Firebase API key, Google App ID, and Cloud Storage bucket hardcoded in res/values/strings.xml
C3	CRITICAL	FirebaseInitProvider (initOrder=100) and MIKitInitProvider (initOrder=99) — 2x pre-consent SDK initialisation on every cold start, RECEIVE_BOOT_COMPLETED registered
H1	HIGH	Braze marketing SDK (New York) receives behavioural data from EV charging and payment session interactions

Subject & Infrastructure Context

IONITY GmbH (HRB 234408, Amtsgericht München) is headquartered at Bahnbogen 21, 81671 Munich, Germany. The company operates a pan-European high-power charging network with more than 600 locations across seventeen countries, serving electric vehicles from all major OEM brands. Its joint venture structure — BMW Group, Ford Motor Company, Hyundai Motor Group, Mercedes-Benz AG, and Volkswagen Group — gives IONITY a position as shared critical digital infrastructure for EV mobility across the European Union.

The audited application, `com.cleevio.ionity.android.app`, was developed by Cleevio s.r.o. (Prague). It provides account management, RFID card administration, active session monitoring, payment method storage, subscription management, and charging history. Users link payment cards and bank accounts through the application and interact with payment flows during active charging sessions.

The combination of payment data, precise location data (EV charging session coordinates), subscription tiers, and RFID physical-access associations makes the IONITY account data model substantively richer than a typical consumer retail application. Compromise of the Cognito authentication layer exposes not only identity credentials but a full behavioural and financial profile of the user's mobility patterns.

Engagement Summary

RFI-IRFOS sent the initial disclosure to `privacy@ionity.eu` and `security@ionity.eu` on 26 June 2026 (REF IONITY-2026), with CC to `press@ionity.eu` and `contact@ionity.eu`, and BCC to the Austrian DSB and the German BfDI. The `security@ionity.eu` relay returned a permanent delivery failure (550 5.4.4) on the first attempt and again on a subsequent follow-up — this address is a dead relay. All subsequent contact was via `privacy@ionity.eu`.

Seven follow-up contacts were sent between 6 July and 15 August 2026 with no substantive reply. On 19 August 2026 — 54 days after the initial disclosure — IONITY's CISO Michael Kanhäuser (`michael.kanhaeuser@ionity.eu`) replied, confirming the findings had been shared with Security, Privacy, and Engineering teams. He noted that some findings had already been identified internally and were being addressed, with the remainder under technical assessment. He also requested clarification on which German supervisory authorities had been notified, and separately indicated interest in exploring a security review engagement.

RFI-IRFOS replied the same day, adding the Bavarian BayLDA to open CC alongside the DSB and BfDI already in the thread, and describing the methodology available for a separate engagement. No further substantive communication was received from IONITY before the embargo date of 26 September 2026. A concrete engagement proposal was sent on 15 September 2026 and has not been acknowledged.

Findings

C1: AWS Cognito AppClientSecret hardcoded in res/raw/amplifyconfiguration.json — full OAuth2 backend authentication compromise

CRITICAL (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) — AWS Cognito AppClientSecret hardcoded

```
CognitoUserPool / Default:
  PoolId:      "eu-central-1_epWSpwuf"
  AppClientId: "16nc3jqjdulljuc5mc7iklottm"
  AppClientSecret: "1o35kc354s9fp85lk42n4spvqf5m5p6pj6oqhjapop423g227u53"
  Region:      "eu-central-1"

Auth.Default.OAuth (v2.500.1 only -- secret now appears twice):
  AppClientSecret: "1o35kc354s9fp85lk42n4spvqf5m5p6pj6oqhjapop423g227u53"

CognitoIdentity / Default:
  PoolId: "eu-central-1:55904b8f-8418-46e0-86be-26ebf55237da"
  Region: "eu-central-1"
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL. The AppClientSecret is the private half of a server-side OAuth2 credential pair that AWS explicitly documents must never be embedded in a public mobile client. With the AppClientSecret, AppClientId, and PoolId all present in the binary, an attacker can compute a valid SECRET_HASH and initiate USER_SRP_AUTH flows, authenticate as the official IONITY application to the Cognito User Pool, probe user accounts, reset credentials, and invoke any authenticated backend endpoint. The Cognito Identity Pool PoolId additionally allows requesting temporary AWS IAM credentials. The exploitable surface is every Play Store installation of the current version — no special access, account, or relationship with IONITY is required.

C2: Firebase API key, Google App ID, and Cloud Storage bucket hardcoded in res/values/strings.xml

CRITICAL (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) — Firebase API key and storage bucket hardcoded

```
google_api_key:      AIzaSyD80961p-sUu88CeulhMbSSHd6ndpz7bgI
google_app_id:       1:5281879950:android:62f6f29e822ef873cc76df
google_storage_bucket: ionity-apps.appspot.com
project_id:          ionity-apps
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL. The Cloud Storage bucket ionity-apps.appspot.com is directly addressable and publicly reachable — if bucket-level IAM rules are permissive (a common misconfiguration in Firebase projects where the default rules allow authenticated reads), all stored application assets are accessible without IONITY credentials. The Firebase API key enables unauthenticated probing of Firebase Remote Config, Cloud Messaging quota exhaustion attacks, and, depending on security rules, reads against the Firebase project's data.

C3: FirebaseInitProvider (initOrder=100) and MLKitInitProvider (initOrder=99) — 2x pre-consent SDK initialisation on every cold start, RECEIVE_BOOT_COMPLETED registered

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9) — pre-consent data collection on every cold start

```
FirebaseInitProvider  initOrder=100  directBootAware=true  (Firebase Analytics)
MLKitInitProvider     initOrder=99                      (Google ML Kit)

Permission: android.permission.RECEIVE_BOOT_COMPLETED
```

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL. Both Content Providers initialise before any Activity is shown and therefore before any consent dialog can be presented to the user. Firebase Analytics and ML Kit begin data collection on every cold start regardless of the user's subsequent consent decision. RECEIVE_BOOT_COMPLETED means the app also activates and begins operation on every device restart, independently of any user interaction. This architecture structurally prevents GDPR Art. 7(1)-compliant consent — the data collection begins before consent can be captured.

H1: Braze marketing SDK (New York) receives behavioural data from EV charging and payment session interactions

HIGH (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)
— Braze SDK on payment and charging session data

```
smali classes containing 'braze': 537 files
assets/braze-html-bridge.js
assets/braze-html-in-app-message-bridge.js
```

Braze Inc. 330 W 34th Street, New York, NY 10001, USA
 EU entity: Braze International Limited, Dublin, Ireland

Impact: Braze Inc. (New York / Dublin) is a US-based customer engagement platform used for push notifications and in-app messaging campaigns. In the IONITY application, users manage active charging sessions, payment methods, subscription tiers, and RFID charging card associations. Behavioural events generated during these interactions flow to Braze for marketing automation. The presence of both `braze-html-bridge.js` and `braze-html-in-app-message-bridge.js` in assets confirms in-app messaging is active. GDPR Art. 5(1)(c) data minimisation applies to the transmission of payment-adjacent behavioural signals to a third-party marketing platform. Art. 13(1)(e) requires disclosure of Braze as a data recipient — its presence was not confirmed in IONITY's published transparency notice at the time of audit.

Impact Analysis

C1 is the dominant risk vector. The Cognito AppClientSecret is not a low-value credential — it is the authentication secret for the server-side OAuth2 application client that controls access to IONITY's entire user account system. With it, an attacker can:

1. Compute `SECRET_HASH(username, AppClientId, AppClientSecret)` for any known IONITY account email
2. Initiate `USER_SRP_AUTH` via AWS SDK or direct API call
3. Respond to SRP challenges as the official IONITY application
4. Receive valid Cognito tokens for the targeted account
5. Call any authenticated IONITY API endpoint using those tokens
6. Access stored payment methods, charging session history, RFID card associations, and subscription data

The Identity Pool PoolId separately enables an attacker to call `GetCredentialsForIdentity` and receive temporary AWS IAM credentials (access key, secret key, session token), potentially expanding the attack surface to AWS services the IONITY backend depends on.

C2 adds an independent persistence path: the Firebase API key enables manipulation of Remote Config values that may control application behaviour, and quota exhaustion against Cloud Messaging.

C3 and H1 represent systematic data governance failures. C3 cannot be addressed without a structural change to the application's ContentProvider ordering — a manifest-level architectural fix, not a configuration toggle. H1 raises the question of whether IONITY holds a signed Art. 28 DPA with Braze covering these specific data flows, and whether Braze is disclosed as a processor in the transparency documentation provided to users.

The Complete Chain: App to Account Takeover

The following sequence requires no special access, no IONITY account, and no network-level attack capability. It is executable from a standard Android developer workstation.

Step 1 — Download: Install IONITY (com.cleevio.ionity.android.app) from the Google Play Store. No account required for download.

Step 2 — Extract: Pull the installed APK from the device using adb pull, or obtain the split APK bundle directly from Play. The base.apk is approximately 31 MB.

Step 3 — Decompile: Run apktool d base.apk. The tool baksmali all DEX classes and decompresses all resource files. Total time: under 60 seconds.

Step 4 — Extract credential: Open res/raw/amplifyconfiguration.json. The AppClientSecret, AppClientId, PoolId, and IdentityPoolId are in plaintext. No obfuscation, no encryption, no additional step required.

Step 5 — Compute SECRET_HASH: HMAC-SHA256(message = username + AppClientId, key = AppClientSecret). This is a standard operation available in any programming language.

Step 6 — Initiate auth: Call Cognito InitiateAuth with AuthFlow=USER_SRP_AUTH, AppClientId, SECRET_HASH, and the target account username. The Cognito endpoint is the public AWS service endpoint — no IONITY-specific infrastructure access required.

Step 7 — Complete SRP: Respond to the SRP challenge using standard Secure Remote Password protocol. The AWS Amplify library used by IONITY handles this automatically.

Step 8 — Access account: Use the returned AccessToken and IdToken to call authenticated IONITY API endpoints, accessing payment methods, session history, RFID associations, and subscription data.

Total time from APK download to authenticated API access: under 10 minutes for a developer familiar with the toolchain.

Data Protection — Article by Article

Art. 32 GDPR — Security of processing: The hardcoded `AppClientSecret` (C1) and Firebase API key (C2) represent a failure of appropriate technical measures to protect personal data. AWS's own documentation explicitly identifies `AppClientSecrets` as server-side credentials that must not be distributed in mobile clients. Art. 32(1)(b) requires measures that ensure ongoing confidentiality, integrity, and availability of personal data systems — a publicly extractable authentication secret fails this requirement.

Art. 7(1) GDPR — Conditions for consent: C3 (pre-consent `ContentProvider` initialisation) means Firebase Analytics and ML Kit begin processing before any consent signal can be captured. The GDPR requires that processing based on consent does not begin before consent is given. The manifest-level `ContentProvider` architecture makes this impossible to satisfy without a structural code change.

Art. 6(1) GDPR — Lawfulness of processing: If Braze (H1) processes user data for marketing automation, the legal basis for this processing must be identified and documented. Behavioural data derived from EV charging and payment interactions constitutes data about the user's mobility patterns and payment behaviour, which may require explicit consent or a documented legitimate interest assessment.

Art. 5(1)(c) GDPR — Data minimisation: The transmission of EV charging session behavioural data to a third-party marketing platform (Braze) requires justification under data minimisation principles. Marketing optimization is not a purpose that requires access to the full behavioural context of payment and charging interactions.

Art. 13(1)(e) GDPR — Transparency: Recipients of personal data, including processors such as Braze, must be disclosed in the Art. 13 information provided to users. Non-disclosure of Braze as a data recipient is an independent transparency violation.

Art. 33 GDPR — Notification of a personal data breach: The `AppClientSecret` exposure constitutes a personal data security incident. If the supervisory authority or IONITY determines that there is a risk to the rights and freedoms of natural persons, a 72-hour notification obligation to the BayLDA applies. The notification window under Art. 33 runs from when IONITY became aware of the vulnerability — which, at the latest, is the date of the RFI-IRFOS disclosure on 26 June 2026.

Critical Infrastructure & NIS2 Context

IONITY operates charging infrastructure across seventeen EU member states. The German NIS2 implementation (NIS2UmsuCG, in force since October 2024) places cybersecurity governance liability directly on the management body under § 38 — the board is personally responsible for approving and supervising cybersecurity measures, not merely delegating to a security team.

EV charging infrastructure may fall under Annex II of the NIS2 Directive as Important Entities in the transport sector (specifically road transport and electric vehicle supply equipment). The applicability of a formal NIS2 classification requires a sector and size assessment that RFI-IRFOS has not independently conducted. However, the direction is unambiguous: an EV charging network operated by five of the world's largest automotive manufacturers, serving hundreds of thousands of users across EU member states, occupies a position in the European mobility infrastructure that is exactly the type of entity the NIS2 Directive was designed to protect.

A hardcoded backend authentication secret — extractable from a public app download in under 60 seconds — is precisely the class of supply-chain and credential hygiene failure that NIS2 Article 21 security measures are intended to prevent.

Regulatory & Legal Landscape

Lead supervisory authority: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Promenade 27, 91522 Ansbach, Germany (poststelle@lda.bayern.de). IONITY GmbH is headquartered in Munich — the BayLDA is the competent lead authority under Art. 56 GDPR for cross-border cases.

Additional authorities notified: Austrian Datenschutzbehörde (dsb@dsb.gv.at) — notified BCC on 26 June 2026; German Bundesbeauftragter für den Datenschutz und die Informationsfreiheit / BfDI (poststelle@bfdi.bund.de) — notified BCC on 26 June 2026; BayLDA added to open CC on 19 August 2026.

Fine exposure: Art. 83(4) GDPR applies to violations of Art. 5, 7, and 13 — administrative fines up to EUR 10,000,000 or 2% of total worldwide annual turnover, whichever is higher. Art. 83(5) applies to Art. 32 violations — up to EUR 20,000,000 or 4% of total worldwide annual turnover. In the case of a joint venture, the turnover of the five JV parent groups (BMW Group, Ford Motor Company, Hyundai Motor Group, Mercedes-Benz AG, Volkswagen Group) is relevant context for proportionality assessment — their combined annual revenue exceeds EUR 700 billion.

Indicators of Compromise

The following identifiers were extracted from the production APK and confirmed present and unchanged in v2.500.1 (re-verification 2026-10-17). Any access logs, authentication attempts, or API calls using these identifiers outside of IONITY's own legitimate application traffic should be treated as potential unauthorized access.

```
C1 -- Cognito AppClientSecret
Value:    1o35kc354s9fp85lk42n4spvqf5m5p6pj6oqhjapop423g227u53
Location: res/raw/amplifyconfiguration.json (CognitoUserPool.Default and Auth.
         Default.OAuth)
Status:    UNROTATED as of 2026-10-17 (re-verification confirmed)

C1 -- Cognito AppClientId
Value:    16nc3jqjdulljuc5mc7iklottom

C1 -- Cognito UserPool ID
Value:    eu-central-1_epwSpswuf

C1 -- Cognito Identity Pool ID
Value:    eu-central-1:55904b8f-8418-46e0-86be-26ebf55237da

C2 -- Firebase API Key
Value:    AIzaSyD80961p-sUu88CeulhMbSSHd6ndpz7bgI
Status:    UNROTATED as of 2026-10-17

C2 -- Firebase Google App ID
Value:    1:5281879950:android:62f6f29e822ef873cc76df

C2 -- Cloud Storage Bucket
Value:    ionity-apps.appspot.com

H1 -- Braze SDK volume
537 smali files + braze-html-bridge.js + braze-html-in-app-message-bridge.js
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure (R1) sent to privacy@ionity.eu and security@ionity.eu, CC_press@ionity.eu and contact@ionity.eu. BCC: Austrian DSB, German BfDI. security@ionity.eu returned permanent 550 delivery failure.

2026-07-06 10-day follow-up. security@ionity.eu bounced again — confirmed dead relay.

2026-07-17 21-day follow-up. privacy@ionity.eu confirmed delivery.

2026-07-23 28-day follow-up. security@ionity.eu included again — bounced again.

2026-07-27 Follow-up, privacy@ionity.eu only.

2026-08-04 40-day follow-up.

2026-08-15 50-day escalation. DSB and BfDI added to open CC.

2026-08-19 CISO Michael Kanhäuser (michael.kanhaeuser@ionity.eu) replied. Findings confirmed routed to Security, Privacy, and Engineering. Some findings noted as independently identified and in progress. Remainder under technical assessment.

2026-08-19 RFI-IRFOS replied same day. BayLDA added to CC alongside DSB and BfDI. Engagement methodology described.

2026-09-15 Concrete engagement proposal sent to Michael Kanhäuser. No acknowledgment received.

2026-09-26 Coordinated disclosure embargo elapsed. No confirmed remediation received.

2026-10-17 Re-verification against v2.500.1 (versionCode 2088093427). All four findings confirmed unaddressed. `AppClientSecret` value identical and now present in two locations in the same config file. This report published.

What IONITY Got Right

The IONITY application demonstrates deliberate security decisions in two areas. The Network Security Configuration (`AndroidManifest.xml`) correctly sets `cleartextTrafficPermitted` to false for both the base config and the `ionity.cloud` domain, forcing all API traffic over TLS. The `allowBackup` attribute is set to false, preventing automatic backup of application data to Google Cloud — a non-default setting that protects session tokens and cached user data from extraction via backup mechanisms.

These choices reflect active security awareness in the development process. The `AppClientSecret` exposure is a deployment configuration error in a single JSON file, not evidence of absent security thinking. The fix for C1 is targeted and well-understood: remove the `AppClientSecret` from the Amplify configuration and switch to a Cognito App Client configured for use without a client secret, which AWS recommends for all public mobile client applications.

Residual Risk & Recommendations

C1 — Immediate: Rotate the Cognito AppClientSecret. Create a new Cognito App Client with no AppClientSecret configured (the recommended configuration for mobile clients per AWS documentation). Remove AppClientSecret from res/raw/amplifyconfiguration.json in all future builds. Audit Cognito access logs for anomalous InitiateAuth calls using the exposed credentials.

C2 — Immediate: Rotate the Firebase API key. Apply API key restrictions in the Firebase console (Android app restriction + API method restrictions). Audit ionity-apps.appspot.com bucket IAM policies and ensure no public or unauthenticated read access.

C3 — Structural: Disable automatic initialisation of FirebaseInitProvider and MIKitInitProvider in AndroidManifest.xml using tools:node='remove' on both ContentProvider declarations. Implement Firebase initialisation explicitly after consent is captured, using FirebaseApp.initializeApp() in application code. The RECEIVE_BOOT_COMPLETED permission should be audited for necessity.

H1 — Governance: Confirm that a signed Art. 28 Data Processing Agreement with Braze Inc. exists and covers the EV charging and payment interaction data flows identified. Add Braze to the Art. 13 transparency notice provided to users. Review which behavioural events are transmitted to Braze and whether they satisfy the Art. 5(1)(c) data minimisation principle.

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 All findings derive from static root-level analysis

of the published application using publicly available tooling. No servers, accounts or IONITY infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF IONITY-2026.