IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

RAY LEON
11 Plaza Real S.
Apt. 712
Boca Raton, FL 33432;

RICHARD INZA
2451 SW 126th Way
Miramar, FL 33027;

MICHAEL INZA;
14826 SW 45 Lane
Miami, FL 33185;

VOIP-PAL.COM INC.;
7215 Bosque Blvd
Suite 102
Waco, TX 76710;

Plaintiff,

v.

APPLE INC.
1 Apple Park Way,
Cupertino, California 95014

ALPHABET INC.
1600 Amphitheatre Parkway,
Mountain View, California 94043

GOOGLE LLC
1600 Amphitheatre Parkway,
Mountain View, California 94043

SAMSUNG ELECTRONICS AMERICA INC.
700 Sylvan Avenue,
Englewood Cliffs, NJ 07632

Defendants.

Civil Action No. 1:25-cv-01970(RDM)

JURY TRIAL DEMANDED

FIRST AMENDED COMPLAINT

COMES NOW Plaintiffs Ray Leon, Richard Inza, Michael Inza, and VoIP-Pal.com Inc., by and through the undersigned counsel, and makes its Complaint against Defendants Apple Inc., Alphabet Inc., Google LLC, and Samsung Electronics America Inc., stating:

INTRODUCTION

THE PLATFORM PROVIDER DEFENDANTS AND CO-PARTICIPANT CONSPIRATORS USE A LOCK–AND–KEY SYSTEM THAT VIOLATES ANTITRUST LAWS INCLUDING SHERMAN ACT § 2

1. Plaintiffs, on behalf of a device-owner class, bring this antitrust class action against a unified exclusionary design implemented at certain checkpoints in smartphone devices and smartphone operating systems by the Platform Providers and Device Manufacturers (Apple, Google, and Samsung hereinafter "Platform Provider Defendants"). This unified exclusionary design has anticompetitive effects, including monopolization/monopoly maintenance, conspiracy to monopolize (including maintenance conspiracy), and attempted monopolization in violation, for example, of Sherman Act § 2 . Together with their Carrier Co-Conspirators (AT&T, Verizon, and T-Mobile hereinafter "Carrier Co-Conspirators" pleaded as non-party co-participants), whose conduct evidences and facilitates the Platform Provider Defendants' anticompetitive conduct, the Platform Provider Defendants' have combined and conspired to monopolize or attempt to monopolize native telephony calling (including Wi-Fi Calling) and have foreclose independent competition in the market.

Three Enterprise Structures Within One Exclusionary Design

Platform Provider Enterprise

2. The Platform Provider Defendants encode operating-system and firmware rules (the "Lock") such that native telephony calling activates only upon carrier validation (entitlement checks, default-dialer gating, allow-lists). Absent validation, owner devices are denied native behavior on non-carrier lines. The Platform Provider Defendants have combined and conspired to monopolize or attempt to monopolize native telephony calling at the device/OS chokepoint that controls non-replicable native telephony surfaces across the smartphone base. This Platform

Provider Enterprise utilizes exclusionary defaults and technical restraints designed to foreclose stand-alone native Wi-Fi calling.

Carrier Co-Conspirator Enterprise

3. The Carrier Co-Conspirators operate uniform validation regimes—including SIM/eSIM entitlements and IMS/E911/QoS profiles (the "Key")—that withhold native parity from independent VoIP lines and relegate them to degraded application mode. Alleged solely as co-participants in this Complaint, this Carrier Co-Conspirator Enterprise supplies the inputs and market effects which evidence the Platform Provider Defendants conduct to coordinate to maintain monopoly power at the device/OS layer.

Cross-Tier Enterprise

4. The Platform Provider Defendants and the Carrier Co-Conspirators engage the Lock-and-Key system where the Platform Provider Defendants synchronize the Lock with their Carrier Co-Conspirators Key so that native Wi-Fi calling is functionally conditioned on purchase/retention of carrier voice/text bundles ("no bundle, no native"), eliminating any neutral path for qualified non-carrier providers to obtain native parity. This cross-tier enterprise combines and conspires to monopolize Wi-Fi Calling and have foreclose independent / maintenance conspiracy and monopoly maintenance effected through coordinated device-layer conditioning rather than competition in the Wi-Fi Calling market. This is one enterprise with a single exclusionary design, implemented jointly across platforms and carriers on the merits.

Three Enterprise Structures Each With Individual and Combined Anticompetitive Effect

5. These three enterprise structures have monopoly power and control of essential interfaces. iOS/Android—reinforced by OEM firmware—control non-replicable native telephony surfaces (default dialer; inbound wake/ring without push; system call-logs; E911 hooks; QoS). Carrier Co-

Conspirators control validation for the overwhelming share of subscribers. These three enterprise structures utilize exclusionary control at the device/OS layer. Entitlement-gated defaults and associated firmware rules deny native parity to qualified non-carrier providers on owner devices, foreclosing stand-alone native Wi-Fi calling.

6. The Platform Provider Defendants willfully maintain monopoly power at the OS chokepoint by embedding synchronized, entitlement-gated restraints that block stand-alone entry notwithstanding feasible less-restrictive alternatives (neutral certification meeting safety/E911/lawful-access requirements). The Carrier Co-Conspirators utilize exclusionary/predatory pricing, which are plus-factors in finding an implied agreement. Bundle-conditioned "included/no extra charge" representations and pricing structures operate in tandem with device-layer denial of parity to (i) foreclose effective access to the native lane, (ii) raise rivals' costs, and (iii) extract supercompetitive bundle premiums while offloading voice traffic to subscriber-funded Wi-Fi.

7. Their conduct has anticompetitive effects. Higher prices (bundle premiums), reduced quality (degraded application mode), suppressed entry and innovation, and durable foreclosure at scale. Aligned defaults across competing platforms and uniform carrier validations demonstrate concerted design and exclusionary purpose; the Platforms' conduct reflects specific intent and a dangerous probability of further entrenchment at the device/OS layer.

8. Plaintiff believes a less-restrictive alternative exists. A neutral certification pathway would confer native parity without conditioning access on carrier bundles, confirming that the challenged restraints constitute maintenance by exclusion rather than technical necessity.

Clarifying the Lock and the Key

9. **Lock (Platform Provider Defendants):** Google, Apple, and Samsung's OS/firmware gating that controls access to native telephony surfaces.

10. **Key (Carrier Co-Conspirators):** AT&T, Verizon, and T-Mobile's validation inputs (SIM/eSIM entitlements; IMS/E911/QoS profiles) required by the Lock to open the native lane.

11. In this Complaint, the Carrier Co-Conspirators are pleaded as co-participants only; allegations against carriers are presented to establish agreement, inputs, plus-factors, market effects, and the feasibility of less-restrictive alternatives that underscore the Platform Provider Defendants' antitrust liability, including under Sherman Act § 2.

OPERATION OF THE LOCK-AND-KEY SYSTEM VIOLATES ANTITRUST LAWS

12. **How Native Calling Works:** For normal operation, every smartphone needs to be tied to a globally unique PSTN number, which the device recognizes as its "native identity." This number is bound to the default phone features and controls core functions: dialing, ringing, call-log entries, E911 emergency access, background operation, and quality-of-service priority. Normally, this native number is provisioned through a SIM card or eSIM and validated when the phone is powered up. Once validated, the operating system unlocks the full native telephony stack. In the United States, native treatment on Apple's iOS mobile operating system ("iOS") and Google's Android mobile operating system ("Android") is granted only when the SIM/eSIM presents OS-recognized carrier entitlements and IMS provisioning. Those entitlements are issued through Apple/Google carrier programs and OEM carrier configurations, and they are not available to independent VoIP providers. As a result, buyer-owned devices treat carrier-validated infrastructure as "native" and relegate independent rivals to degraded application mode. There is no pathway that would allow an independent VoIP provider to obtain the same native status, for example:

13. Apple utilizes iOS (as the Lock) to tie native telephony (default dialer, inbound wake/ring without third-party push, system call-log, E911 hooks, QoS) to carrier entitlements and eSIM/SIM provisioning recognized through Apple's carrier programs. Absent those entitlements, iOS withholds native behaviors and forces non-carrier PSTN identities into app mode. Google utilizes Android/Pixel (as the the Lock) to grant native behaviors when carrier privileges/provisioning and IMS profiles are detected by OS checks; otherwise, non-carrier PSTN identities are confined to app mode without default-dialer parity or native inbound wake/ring. Samsung utilizes OEM firmware on Android (as the Lock) to enforce carrier configuration/allow-lists and IMS/RIL profiles before enabling native dialer, system call-log, E911 hooks, and QoS; non-listed providers are denied native parity on Galaxy devices

14. **Why Independent VoIP Providers Are Blocked:** Even if an independent VoIP provider owns PSTN numbers, operates its own validation servers, and issues its own SIM/eSIM profiles, the operating system will not recognize those credentials as "native." The consequences are stark: outgoing calls under a VoIP PSTN identity cannot be placed natively; incoming calls from outside the VoIP network are not recognized as native incoming calls, do not wake the Phone app, appear in the call log, or allow access to emergency functions; and consumers are relegated to degraded "app mode," dependent on delayed push notifications and stripped of full system integration, for example:

15. Using iOS instantiation, third-party PSTN identities are denied default-dialer control, native inbound wake/ring (push-free), and system call-logging/E911 hooks without Apple-recognized carrier entitlements. Using Android/Pixel instantiation, without Android-recognized carrier privileges/IMS provisioning, third-party PSTN identities cannot obtain default-dialer parity, native inbound ring/wake, or system call-log/E911 integration. Using Samsung instantiation, third-party

PSTN identities are confined to app mode on Galaxy devices and cannot access native telephony surfaces absent Samsung CSC/IMS allow-listing and carrier profiles.

16. In practice, this means that only carrier-controlled PSTN numbers—those that pass through the OS-controlled entitlement and IMS gates—can function as true native numbers. Independent providers are categorically locked out, no matter how complete their own infrastructure may be.

17. Cross-tier conditioning ("no bundle, no native") is in effect because platform Locks open only when consuming carrier Keys (SIM/eSIM entitlements, IMS/E911/QoS profiles), native Wi-Fi calling is functionally conditioned on purchase/retention of carrier voice/text bundles—eliminating any neutral path for qualified non-carrier providers to obtain native parity on owner devices. A less-restrictive alternative would include a neutral certification pathway—meeting safety, E911, lawful-access, and QoS requirements—and would confer native parity without conditioning access on carrier bundles.

Plaintiffs Have Public Evidence of The Lock–and–Key Framework

18. **The Lock (Platform Provider Defendants):** iOS, Android, and Samsung OS software and device firmware contain the device-layer rules that control native telephony. By design, they permit native status only when OS-recognized carrier validation is present. With ~97% market share between Apple and Google, this chokepoint gives the platform providers and device manufacturers decisive control. **The Key (Designed Exclusively by Platform Provider Defendants for Carrier Co-Conspirators):** AT&T, Verizon, and T-Mobile supply the entitlement servers, SIM/eSIM profiles, IMS specifications, E911 routing, and QoS rules that the Lock checks. Without an authorized carrier Key, the Lock remains closed. **Together the Platform Provider Defendants and the Carrier Co-Conspirators ensure that only bundled carrier lines are treated as native.**

19. **Apple (iOS — the Lock)** enforces entitlement-gated native telephony: default dialer/UI, push-free inbound wake/ring, system call-log, E911 hooks, and QoS unlock only on Apple-recognized carrier validations. **Google (Android/Pixel — the Lock)** grants native parity when OS checks (e.g., carrier privileges/provisioning and IMS profiles) succeed; otherwise third-party PSTN identities are confined to app mode. **Samsung (OEM firmware on Android — the Lock)** govern native behaviors on Galaxy devices; non-listed providers lack native parity with Samsung firmware/CSC allow-lists and IMS/RIL profiles. **Carrier Co-Conspirators (the Key)** provide SIM/eSIM entitlements, IMS/E911/QoS inputs, and provisioning tokens consumed by each platform's Lock. **Cross-tier result ("no bundle, no native")** is in effect because the Locks open only when consuming carrier Keys, owner devices treat bundled carrier lines as native and exclude a neutral path for qualified non-carrier providers.

Plaintiffs Allege Antitrust Violations, including Sherman Act § 2

20. This Lock–and–Key arrangement constitutes distinct but complementary violations of Sherman Act § 2. The Platform Provider Defendants monopolize wi-fi calling (device-layer foreclosure) when it is unlawful to maintain monopoly power through exclusionary conduct. Apple and Google, reinforced by Samsung, coded their platforms to deny native access to non-carrier numbers. This preserves monopoly control over the only viable distribution channel for telephony, even though neutral certification is feasible. Exclusion occurs at the post-sale, service level — here, device interfaces — to lock out rivals.

21. Apple utilizes iOS instantiation with Apple's entitlement-gated rules restrict native interfaces to carrier-validated lines, foreclosing stand-alone native Wi-Fi calling; a neutral certification pathway meeting E911/lawful-access/QoS would confer native parity without bundles. Google utilizes Android/Pixel instantiation where Google conditions native telephony on

carrier privileges/IMS provisioning, excluding non-carrier providers from native parity; neutral certification is a less-restrictive alternative. Samsung's instantiation includes Samsung's firmware/CSC and allow-lists to enforce carrier-driven native access. In contrast, a neutral certification would permit native parity independent of carrier bundles.

22. The Platform Provider Defendants combine or conspire to monopolize Wi-Fi Calling (coordinated foreclosure) when Apple, Google, and Samsung each enforce the identical entitlement-gated restriction, producing the same no bundle, no native calling outcome. This uniformity is not independent design but coordinated foreclosure, amounting to a § 2 conspiracy. Apple, Google, and Samsung have used similar tactics to Microsoft whose conduct was condemned in *United States v. Microsoft Corp.*, 253 F.3d 34, 58–67 (D.C. Cir. 2001) (*en banc*), where the D.C. Circuit found that technical restraints and default settings implemented at the OS level foreclosed browser rivals. There is a cross-platform alignment. Parallel Locks across iOS/Android/Samsung firmware consume the same carrier Keys and yield the same conditioning outcome, evidencing concerted design and exclusionary purpose.

23. The Carrier Co-Conspirators combine or conspire to monopolize Wi-Fi Calling (bundle tying and market lock-in) when AT&T, Verizon, and T-Mobile as carriers uniformly condition native calling on cellular bundle purchase. The carriers exploit the Lock provided by the Platform Provider Defendants using vertical entitlements (SIM/eSIM, IMS, QoS) to block independent competitors in Wi-Fi Calling. Accordingly, a device-layer tie is in effect. Synchronization of carrier Keys with platform Locks conditions native access on bundle purchase/retention, foreclosing a neutral path for qualified non-carrier providers and sustaining monopoly maintenance at the device/OS chokepoint.

The Platform Provider Defendants and Carrier Co-Conspirators Act as One Enterprise to Enforce One Rule

24. The Platform Provider Defendants (and the Carrier Co-Conspirators) act as one enterprise maintain monopoly power of Wi-Fi Calling in violation of Sherman Act § 2. The Platform Provider Defendants and Carrier Co-Conspirators implement the Lock–and–Key system technical mechanism for exclusion. The result is a closed, enterprise-wide system where consumers are denied choice, competitors are foreclosed, and one rule is absolutely enforced: no carrier bundle means no native calling.

25. Apple (utilizing iOS as the Lock) encodes entitlement-gated native access that opens only with carrier validations, effectuating the "no bundle, no native" rule on iPhone. Google (utilizing Android/Pixel as the Lock) only unlocks Android's native telephony upon carrier privileges/IMS provisioning, enforcing the rule across Pixel and other Android devices. Samsung (utilizing its OEM firmware as the Lock), implement the same rule on Galaxy devices with Samsung firmware/CSC allow-lists and IMS profiles. Carriers (supplying the Key) AT&T, Verizon, and T-Mobile provide SIM/eSIM entitlements, IMS/E911/QoS inputs that each Lock consumes to determine native status.

26. The harm begins with competition and extends to the public. More than 373 million U.S. mobile subscribers are trapped in the same closed system. Consumers must buy bundled cellular calling and texting services in order to access Wi-Fi Calling, even though Wi-Fi Calling uses networks and devices they already pay for. Device owners are forced to pay supracompetitive bundle prices to unlock native functions on their own phones, or else accept functional degradation in app-mode: delayed wake/ring, incomplete call logs, reduced E911 behavior, and no QoS parity. A feasible stand-alone native option could be offered at far lower prices (approximately $6.50 per line or $20 per family), but that path is foreclosed by the code-level tie—producing nationwide

overcharges and loss of consumer choice. This structure has produced extraordinary profits for Defendants — estimated at more than $560 billion annually — while families across the country, including over 100 million Americans living just above the federal poverty threshold, are forced into inflated monthly costs. The disparity is striking. A stand-alone Wi-Fi Calling option could cost as little as $6.50 per month for an individual or $20 for a family of four. Instead, families must routinely pay $50–$60 per month for voice/text bundles plus $40–$50 for mobile data they may not want to have purchased as a bundle. The result is systematic overcharge, lack of choice, and nationwide exclusion of a lower-cost alternative.

27. Apple's entitlement gating prevented VoIP numbers from obtaining default-dialer, native inbound wake/ring, system call-log, and E911 parity. Android's carrier-privilege/IMS checks denied VoIP native behaviors, confining it to app mode. Samsung's firmware/CSC allow-lists withheld native parity from VoIP numbers absent carrier validation. This had a cross-tier effect. The synchronized Locks and Keys ensure native access only with a carrier bundle, converting owner devices into distribution bottlenecks and eliminating a neutral path to native parity.

28. **VoIP-Pal as Exemplar (Non-Class Co-Plaintiff).** VoIP-Pal was a ready-and-able entrant that developed and validated technology for stand-alone native Wi-Fi Calling. The Lock–and–Key blocked native access on owner devices, chilling pilot programs, distribution agreements, and capital formation. VoIP-Pal's experience exemplifies the same exclusion the class faces. In this class action, VoIP-Pal does not seek damages; it appears in a limited posture aligned with class injunctive relief.

Sherman Act § 2 Applies to the three Enterprises

29. Sherman Act § 2 liability attaches when monopoly power is willfully acquired or maintained through exclusionary conduct, when multiple actors conspire to monopolize, and when multiple

dominant firms align to jointly preserve monopoly power through exclusionary practices. The Platform Provider Defendants and Carrier Co-Conspirators function in concert through the Lock-and-Key system, creating market-wide exclusionary effects similar to the anticompetitive conduct addressed in these cases.

30. Identical entitlement-gated rules across platforms, uniformly consumed carrier validations, and the common "no bundle, no native" outcome demonstrate concerted exclusion Even if the Court were to analyze the Platform Provider Defendants and Carrier Co-Conspirators in separate tiers rather than as a unified enterprise, each tier independently violates Sherman Act § 2. The Platform Provider Defendants—Apple and Google, with Samsung reinforcing restrictions at the firmware layer—maintained monopoly power by coding their operating systems to foreclose rivals from the only viable distribution channel for mobile telephony. In addition, the Platform Provider Defendants jointly enforced entitlement-gated restrictions across iOS, Android, and Samsung firmware. This coordinated adoption of uniform restraints preserved monopoly power at the device layer and constitutes a maintenance conspiracy actionable under § 2.

31. Platform tier (individual liability). Each platform's Lock independently maintains monopoly power at the device/OS chokepoint. Platform tier (concerted liability). Cross-platform uniformity in entitlement-gated restrictions constitutes a § 2 maintenance conspiracy.

32. The Carrier Co-Conspirators—AT&T, Verizon, and T-Mobile—are likewise independently liable. The national carriers uniformly conditioned native calling on the purchase of bundled plans. By exploiting entitlement and IMS inputs, the carriers vertically foreclosed stand-alone Wi-Fi Calling. Whether viewed separately or together, the result is the same: each set of defendants willfully maintained monopoly power and conspired—both horizontally and vertically—to foreclose rivals, in violation of Sherman Act § 2. Corporate separateness does not shield conduct

that in practice operated as a unified exclusionary scheme.

33. Carrier tier (individual liability). Bundle-conditioned native access is exclusionary and forecloses stand-alone entry. Vertical & horizontal coordination. Carriers align horizontally on conditioning, and vertically with platform Locks, to maintain monopoly power

34. In related complaints already filed against the Carrier Co-Conspirators—AT&T Inc., Verizon Communications Inc., and T-Mobile US, Inc.—and in this complaint against the Platform and Device Manufacturer Defendants—Apple, Google, and Samsung—Plaintiffs challenge a unified enterprise scheme designed to foreclose all stand-alone competition in Wi-Fi Calling. The Lock–and–Key mechanism is pleaded consistently across actions to show single-scheme exclusion with platform/device chokepoints and carrier validations

35. Defendants' actions do not allow them to contend that Sherman Act § 2 applies only to a single enterprise or single-firm conduct. Section 2 applies in at least three circumstances: (a) when a single firm willfully maintains monopoly power through exclusionary conduct; (b) when multiple actors coordinate so that their conduct functions as a unified enterprise to foreclose rivals; and (c) when multiple dominant firms jointly preserve monopoly power through maintenance conspiracies. Sherman § 2 applies to the conduct alleged here: dominant platform and carrier firms (as if they were a single enterprise) integrating operating-system and firmware restraints with entitlement gating and tying arrangements to foreclose rivals. The Platform Locks plus carrier Keys jointly effectuate post-sale conditioning—no bundle, no native—that forecloses stand-alone competitors from native parity.

36. Conduct by the Platform Provider Defendants and Carrier Co-Conspirators is proven by publicly available materials, including Apple and Google developer documentation, Samsung firmware policies, carrier entitlement specifications, and marketing statements that falsely promise

"Wi-Fi Calling included / no extra charge" while enforcing "no bundle, no native." The uniformity of these public records across all Defendants confirms the exclusionary design without the need for extended discovery. Public-record proof points. Platform developer docs, OEM firmware/CSC policies, carrier entitlement/IMS materials, and uniform "included/no extra charge" messaging collectively corroborate the same exclusionary mechanism and outcome as shown in Appendices B-D.

ADDITIONAL DIRECT ANTITRUST BREACHES BY THE PLATFORM PROVIDER DEFENDANTS (APPLE, GOOGLE, AND SAMSUNG)

37. The Platform Provider Defendants' anticompetitive conduct extends beyond monopoly maintenance and conspiracy to monopolize under Sherman Act § 2. Their operating systems and firmware implement entitlement programs, hasCarrierPrivileges() checks, CarrierConfig gating, CallKit/PushKit limitations, removal of SIP/RTP stacks, default-dialer restrictions, and Samsung firmware allow-lists. These practices together constitute direct violations of Sherman Act § 1 and the Clayton Act by tying, exclusive dealing, and concerted foreclosure.

38. Apple (with iOS) utilized entitlement programs; CallKit/PushKit constraints; default-dialer exclusivity; native E911/QoS reserved to carrier-validated lines. Google (with Android/Pixel) utilized hasCarrierPrivileges(); CarrierConfigManager; IMS single-registration binding; deprecation/removal of native SIP/RTP; native dialer privileges withheld absent carrier validation. Samsung (with its OEM firmware) utilized boot-time allow-lists; CSC/carrier-config gating; and default-dialer capture aligned to carrier entitlements. This allowed cross-platform coordination. Parallel device-layer rules across iOS/Android/Samsung firmware implement concerted foreclosure and eliminate a neutral path to native parity for stand-alone providers.

Sherman Act § 1 — Tying / Hub-and-Spoke Restraint

39. The Platform Provider Defendants' conduct restrains trade by encoding the tie into the

device. iOS and Android, reinforced by Samsung firmware, are coded so that native telephony functions (default dialer, inbound wake/ring without push, system call-log, E911 hooks, and QoS) activate only when the operating system detects carrier entitlements and IP Multimedia Subsystem ("IMS") provisioning. The Platform Provider Defendants' conduct restrains trade by gatekeeping mechanisms:

40. **Apple (utilizing iOS)** restrained trade with carrier bundle and entitlement checks; third-party VoIP confined to CallKit/PushKit with background timing and latency limits; no parity with the native Phone role. **Google (utilizing Android)** restrained trade with hasCarrierPrivileges(), CarrierConfigManager, IMS single-registration binding; removal or deprecation of native SIP/RTP stacks in later Android versions; native dialer privileges withheld from non-entitled lines. **Samsung (utilizing its OEM firmware)** restrained trade with boot-time allow-lists and default-dialer capture aligned to carrier entitlements. The **"no bundle, no native"** caused a tying arrangement by wiring native activation to carrier entitlements/IMS, the Platforms embed the carrier-bundle condition at the device layer, eliminating any neutral certification route to native parity.

41. Consumers cannot access Wi-Fi Calling unless they also purchase and maintain a carrier bundle. The Platform Provider Defendants' software transforms the carrier's contractual requirement into a device-level operating system mandate. The Platform Provider Defendants write and ship the operating system code that embeds the carrier-bundle condition at the device layer. Without the Lock imposed by the Platform Provider Defendants' software and firmware, the authorized Keys of the Carrier Co-Conspirators could not compel the tie of the carrier-bundle. By encoding this condition into iOS, Android, and Samsung firmware, the Platform Providers are co-authors of the tying arrangement under Sherman Act § 1. They provide the device-level coercion

that makes the purchase and retention of a carrier bundle a prerequisite for Wi-Fi Calling, thereby foreclosing stand-alone VoIP competitors from parity access.

42. Apple utilizes iOS for entitlements/provisioning to convert carrier bundle terms into device-level preconditions for native telephony. Google utilizes Android's carrier-privilege/IMS checks operationalize the bundle tie within OS logic. Samsung utilizes firmware/CSC allow-lists to enforce bundle-conditioned native access across Galaxy devices. In contrast, a neutral certification path (safety/E911/lawful-access/QoS) would enable native parity without bundle conditioning.

Sherman Act § 1 — Exclusive Dealing / De-Facto Exclusivity

43. The Platform Provider Defendants' conduct restrains trade through exclusion dealing to reserve native privileges. The Platform Provider Defendants reserve native telephony privileges exclusively for carrier services, while withholding those same interfaces from independent providers. The Platform Provider Defendants' conduct restrains trade through exclusion dealing to implement the restriction in code. Owner devices become exclusive distribution channels for carrier-validated lines; stand-alone providers are confined to degraded app mode with no neutral path to native parity.

44. **Apple (utilizing iOS)** restrained trade with carrier bundle and entitlement checks; third-party VoIP confined to CallKit/PushKit with background timing and latency limits; no parity with the native Phone role. **Google (utilizing Android)** restrained trade with hasCarrierPrivileges(), CarrierConfigManager, IMS single-registration binding; removal or deprecation of native SIP/RTP stacks in later Android versions; native dialer privileges withheld from non-entitled lines. **Samsung (utilizing its OEM firmware)** restrained trade with boot-time allow-lists and default-dialer capture aligned to carrier entitlements. The **"no bundle, no native"** is evidence of exclusive dealing by wiring native activation to carrier entitlements/IMS, the Platforms embed the carrier-

bundle condition at the device layer, eliminating any neutral certification route to native parity.

45. Exclusive-dealing restraints that substantially foreclose rivals violate § 1 under the rule of reason. The relevant foreclosure is measured at the only viable distribution lane for mobile voice on smartphones — the native telephony features controlled by the operating system and firmware. By coding those features to be exclusive to carrier-validated lines, the Platform Provider Defendants foreclose nearly the entire smartphone base to non-carrier competitors. Apple, Google, and Samsung unilaterally control access to the native telephony features. By hard-coding exclusivity for carrier services and denying equal privileges to qualified independents, they author the foreclosure. This is exclusive dealing in code: the Platform Providers' design choices — not any physical network limitation — exclude stand-alone entrants from competing at parity. Near-total device base foreclosed at the native lane (default dialer, inbound wake/ring, call-log, E911, QoS). The code-level exclusivity authored by the Platforms (not network scarcity) drives the restraint; neutral certification remains a feasible, less-restrictive alternative.

PRIVATE PROPERTY RIGHTS AND HOW THEY STRENGTHEN THE ANTITRUST CLAIMS

46. The handset is the subscriber's paid property. The Wi-Fi and broadband link are the subscriber's paid infrastructure. When the subscriber taps "Call," initiation occurs on the subscriber's device over their own Wi-Fi before any carrier completion. VoIP-Pal is a third-party technology provider foreclosed from native use of every subscriber's phone because Platform Providers have coded the device to withhold access to native telephony features from non-carriers.

47. Apple (iOS—Lock on owner's device) withholds native dialer, push-free inbound wake/ring, system call-log, E911, and QoS from non-carrier lines on the owner's iPhone, despite the device and Wi-Fi being the owner's property. Google (Android/Pixel—Lock on owner's device) gates native behaviors behind carrier privileges/IMS provisioning, limiting the owner's

Pixel/Android device from using non-carrier PSTN identities natively on their own Wi-Fi. Samsung (OEM firmware—Lock on owner's device) prevents non-carrier lines from using the owner's phone natively over the owner's Wi-Fi utilizing Samsung firmware/CSC allow-lists control native parity on Galaxy devices.

THE PARTIES

THE PLAINTIFFS

Device-Owner Class Representatives

48. The device-owner Class Plaintiffs are individuals who purchased and own smartphones running iOS or Android and were subjected to the same post-sale OS/firmware Lock–Key gating that conditions native telephony on carrier validation. Named Class Representatives include Ray Leon, Richard Inza, and Michael Inza.

Shareholder–Consumer Subclass Representatives (Individuals)

49. The Shareholder–Consumer Subclass consists of device owners who also hold VoIP-Pal common stock. The subclass proceeds solely for consumer/device-owner injuries (overcharge and functional degradation on their own phones) and does not assert derivative or enterprise-value claims. Subclass Representatives include Ray Leon, Richard Inza, and Michael Inza.

Non-Class Co-Plaintiff (Limited Appearance)

50. VoIP-Pal.com Inc. is a Nevada corporation with principal place of business in Waco, Texas. VoIP-Pal is the inventor and developer of call classification and routing systems for VoIP services, holding federally validated patents. VoIP-Pal appears here only in a limited, non-class capacity, seeking injunctive/declaratory relief coextensive with class relief and asserting no damages in this action; VoIP-Pal reserves any damages to its separate direct platform action. VoIP-Pal is the inventor and developer of call classification and routing systems for VoIP services; its technology

was foreclosed from deployment by the exclusionary practices alleged herein (Sherman Act §§ 1–2; Clayton Act § 3; RICO §§ 1962(c)–(d)). VoIP-Pal will also arrange finance (e.g., for certification pilots, integration, and monitoring support) to facilitate implementation of a parity injunction benefitting the device-owner class. VoIP-Pal, as lead plaintiff in the carriers class-action antitrust case, will clarify its role to be exactly the same as in this platform class action: limited, non-damages participation aligned with device-owner relief, seeking parity-focused injunctive/declaratory remedies against the same Lock–Key scheme and preserving any VoIP-Pal damages for its separate direct action.

THE DEFENDANTS

APPLE INC.

51. Apple Inc. is a California corporation with its principal place of business at Apple Park, Cupertino, California.

ALPHABET INC. AND GOOGLE LLC

52. Alphabet Inc. is a Delaware corporation with its principal place of business at 1600 Amphitheatre Parkway Mountain View, CA 94043 . Google LLC, a wholly owned subsidiary of Alphabet Inc., is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway Mountain View, CA 94043.

SAMSUNG ELECTRONIC AMERICA (SEA) Inc.

53. Samsung Electronics America Inc. is incorporated in New York, with its principal place of business at 700 Sylvan Avenue, Englewood Cliffs, NJ 07632.

CO-PARTICIPANT CONSPIRATORS (NON-DEFENDANTS)

54. On information and belief, the following individuals served on Apple's board of directors or in executive roles during the period relevant to this Complaint: Tim Cook (Chief Executive

Officer and Director), Katherine L. Adams (Senior Vice President, General Counsel, and Director), Arthur D. Levinson (Chair), Wanda Austin, Alex Gorsky, Andrea Jung, Monica Lozano, Ronald D. Sugar, and Susan L. Wagner. Plaintiff reserves the right to name the aforementioned directors and officers of Apple in a later filing for being co-participant conspirators to the market foreclosure and exclusive dealing resulting from the Lock-and-Key System of the Platform Provider Defendants.

55. On information and belief, the following individuals served on Alphabet Inc.'s and/or Google Inc.'s board of directors or in executive roles during the period relevant to this Complaint: Sundar Pichai (Chief Executive Officer and Director), John L. Hennessy (Chair), Larry Page, Sergey Brin, Frances Arnold, R. Martin "Marty" Chávez, L. John Doerr, Roger W. Ferguson Jr., K. Ram Shriram, and Robin L. Washington. General Counsel: Kent Walker (Chief Legal Officer and General Counsel). Plaintiff reserves the right to name the aforementioned directors and officers of Alphabet Inc. and/or Google Inc. in a later filing for being co-participant conspirators to the market foreclosure and exclusive dealing resulting from the Lock-and-Key System of the Platform Provider Defendants.

56. On information and belief, the following individuals served on Samsung's board of directors or in executive roles during the period relevant to this Complaint: Executive Officers (U.S.): K.S. Choi (President & CEO, Samsung Electronics America). General Counsel: Ken Murata (General Counsel, Samsung Electronics America). Plaintiff reserves the right to name the aforementioned directors and officers of Samsung Electronics America in a later filing for being co-participant conspirators to the market foreclosure and exclusive dealing resulting from the Lock-and-Key System of the Platform Provider Defendants.

57. AT&T Inc., Verizon Communications Inc., and T-Mobile US, Inc. are co-participant

conspirators. Plaintiff reserves the right to name the aforementioned corporations in a later filing for being co-participant conspirators to the market foreclosure and exclusive dealing resulting from the Lock-and-Key System of the Platform Provider Defendants.

JURISDICTION AND VENUE

58. **Subject-Matter Jurisdiction.** This Court has federal-question jurisdiction under 28 U.S.C. §§ 1331 and 1337(a) for claims arising under the Sherman Act §§ 1–2 (15 U.S.C. §§ 1–2), the Clayton Act §§ 3, 4, and 16 (15 U.S.C. §§ 14, 15, 18, 26), and the Racketeer Influenced and Corrupt Organizations Act ("RICO") §§ 1962(c)–(d) and 1964(c) (18 U.S.C. §§ 1962(c)–(d), 1964(c)). The Court may also exercise supplemental jurisdiction over related state-law claims pursuant to 28 U.S.C. § 1367.

59. **Venue and Personal Jurisdiction.** Venue is proper in this District under Clayton Act § 12 (15 U.S.C. § 22) and 28 U.S.C. § 1391(b)–(c). Personal jurisdiction is supported by the nationwide service of process provisions in Clayton Act § 12 and RICO § 1965. These statutes permit suit in this District against corporate defendants and, where appropriate, officers and directors who authorized or directed the conduct alleged.

60. Venue in the District of Columbia is particularly appropriate for several independent reasons. First, all corporate Defendants are publicly traded companies subject to the continuous regulatory oversight of the U.S. Securities and Exchange Commission ("SEC"), a federal agency headquartered at 100 F Street NE, Washington, D.C. Defendants regularly prepare, authorize, sign, and file Forms 10-K, 10-Q, 8-K, proxy statements, registration statements, and other SEC-mandated disclosures through the SEC in this District. These sustained and systematic filings constitute "transacting business" and being "found" in this District within the meaning of Clayton Act § 12 and 28 U.S.C. § 1391. Second, Defendants regularly engage with federal agencies based

in Washington, D.C., including the SEC and the Federal Communications Commission ("FCC"), regarding product features, public disclosures, and policies tied directly to smartphone telephony and communications services. These D.C.-directed regulatory contacts further establish venue and personal jurisdiction here. A substantial part of the events and effects giving rise to these claims occurred in or were directed to this District. The Defendants routinely advertise and sell products in the District, and transact business through brick-and-mortar stores and offices throughout the city. Each of the Defendants is actively registered to do business in the District either itself or through its subsidiary.

FACTS COMMON TO ALL COUNTS

THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-CONSPIRATORS COMBINED AND CONSPIRED AS ONE: PLATFORM "LOCK," CARRIER "KEY"

61. The Defendants' conduct can be viewed through two pillars of foreclosure under Sherman § 2. **Pillar One — Gate Control:** Between them, iOS and Android power virtually the entire smartphone base in the United States; their operating-system rules and OEM firmware control the device-layer native interfaces that make a line behave as the primary number. **Pillar Two — Exclusivity Economics:** Carrier "free/on-us" phone programs are contingent on plan retention. When the same device's OS is coded so the native telephony lane opens only for that carrier's validation (and never for certified independents), the bundle functions as exclusive dealing in code. This is not benign discounting or mere configuration. It is device-level exclusivity layered atop chokepoint control — the precise combination Sherman § 2 forbids where a neutral certification pathway exists.

62. The Defendants in this action are the Platform Providers: Apple, through iOS; Google, through Android; and Samsung, through its covered OEM firmware. The Co-Conspirators are the

Carrier Participants AT&T, Verizon, and T-Mobile. Together, these six actors designed and implemented what can be described as a Lock-and-Key scheme. The Carriers supplied the Key comprising SIM and eSIM credentials, entitlement profiles, and IMS (IP Multimedia Subsystem) policies that collectively validate a phone and native number. The Platforms supplied the Lock. Through operating system code, APIs, default-dialer restrictions, and firmware rules, the Platforms withheld native telephony features from any device that lacked the carrier Key. The result was that critical, telephony features — main-number binding, push-free background wake and ring, system call-log integration, E911 hooks, quality-of-service voice prioritization, and continuity or identity across devices — were activated only for carrier services.

63. For independent VoIP providers, the result was relegation to degraded "app-mode." Instead of calls being treated as native, they were subject to delayed push notifications, unreliable ringing, exclusion from system call-logs, and loss of emergency routing and QoS features. The Platform Provider Defendants encoded the carrier condition into every smartphone, such that the native Phone layer was simply unavailable to non-carrier rivals. This foreclosed native parity across approximately 97 percent of the market. The anticompetitive effect is straightforward. A stand-alone Wi-Fi calling competitor which could have offered service to the class at a consumer-friendly price point of approximately $6.50 per month, could not function at native parity. The market was closed unless consumers purchased and maintained a carrier bundle.

64. The Carriers were not bystanders but co-conspirators. Their Key — entitlements, IMS single-registration rules, E911 routing profiles, QoS standards — was authorized input that the Platform Provider Defendants embedded into their systems to enforce the Lock. Together, the Platform Provider Defendants and the Carrier Co-Conspirators produced uniform exclusion across the market and engaged in exclusive dealing that harmed competition. The conduct constitutes

unlawful tying. The tying product — the product consumers want — is native Wi-Fi calling over subscriber-funded broadband and Wi-Fi. The tied product — what consumers are forced to buy — is the carrier bundle, which includes cellular voice, text, and frequently data services. The mechanism of the tie is coded into the device itself. Unless the carrier Key passes validation, the operating system refuses to grant native behavior. This turns the consumer's privately purchased device into an enforcement point for carrier bundles.

65. Defendants may argue that because carriers provide Wi-Fi Calling as part of their service, they cannot be tying what they do not own. This argument misses the point entirely. Consumers already own the handset. Consumers already pay for the broadband and Wi-Fi access. What they want is standalone Wi-Fi calling — and the platforms have deliberately withheld that function unless the consumer buys and maintains a cellular bundle. Labeling Wi-Fi Calling as *"included / no extra charge"* does not cure the coercion. The conditioning is baked into the operating system and firmware. Consumers must buy the tied bundle to unlock native behavior, regardless of their ownership of the device and network.

66. In contrast, platform Locks commandeer the owner's device/Wi-Fi to enforce carrier bundles, strengthening both antitrust and private-property theories. "Included / no extra charge" messaging masks device-level conditioning; the tie persists because native is withheld absent carrier validation. The absence of a neutral certification path confirms maintenance by exclusion, not technical necessity.

Platform Provider Defendants' Essential Role

67. Each Platform Provider Defendant played their role in developing, creating, and maintaining the Lock. Apple, through iOS, uses carrier bundles and entitlement checks to gate the Phone role. Third-party VoIP applications are confined to CallKit and PushKit, subject to strict

timing and background limits. Without entitlement validation, parity with native carrier services — including E911, QoS, and call-log integration — is withheld. Google, through Android, employs hasCarrierPrivileges(), CarrierConfig, and IMS binding to gate telephony. In later versions, Google removed native SIP and RTP stacks entirely, ensuring that only carrier IMS implementations can access native paths. Pixel devices, marketed as Google's flagship, are shipped as carrier reference models. Applications outside carrier validation are subject to Doze and App Standby restrictions, further degrading functionality. Samsung, through OEM firmware, enforces the Lock at the boot level. Carrier-specific firmware images pre-approve carrier applications as native while blocking third-party VoIP applications from accessing native paths. Default-dialer capture and privileged allow-lists ensure that non-carrier providers cannot achieve parity. The bottom line is that the Platforms supply the Lock that turns the carriers' contractual requirement into a device-level mandate.

68. Apple (iOS — the Lock) includes entitlement checks gate the Phone role; CallKit/PushKit confine third-party VoIP with background/timing limits; E911/QoS/call-log parity withheld absent carrier validation. Google (Android/Pixel — the Lock) includes hasCarrierPrivileges(), CarrierConfig, IMS binding; removal of native SIP/RTP stacks; Doze/App Standby degrade non-validated apps; Pixels ship as carrier reference models. Samsung (OEM firmware — the Lock) includes boot-level enforcement via carrier-specific images; default-dialer capture and privileged allow-lists block native paths for non-carriers. The cross-tier effect is that the Platform Locks convert carrier contract terms into device-level mandates, yielding "no bundle, no native." In contrast, a neutral certification pathway (safety/E911/lawful-access/QoS) would enable native parity without conditioning on carrier bundles.

Why This Remained Hidden

69. The exclusion remained concealed for years because the coercion was written into the code, not displayed on bills. Consumers see a toggle that says "Wi-Fi Calling: On," but unless the carrier Key is present, the operating system denies native behavior. Uniformity across platforms confirms collusion. Identical native-versus-app outcomes across iOS, Android, and Samsung firmware are not plausibly the product of independent design choices. They reveal a single, market-wide mandate. iOS/Android/Samsung uniformity means same entitlement/IMS gating → same denial of native parity for non-carriers on all three platforms. Visibility gap in the billing/marketing say "Wi-Fi Calling: On," but device-code withholds native unless the Key is present. The uniform "no bundle, no native" outcome, absent a neutral certification path, evidences coordinated foreclosure rather than technical necessity.

Harm and Impact — Device Owners First; VoIP-Pal Limited

70. **Device-owner class injury:** A stand-alone native option could be priced in the low single digits per line (approximately $6.50) or offered through affordable family tiering. Code-level tying forecloses that path. Households instead pay bundle premiums of $50–$100 or more each month, while app-mode is degraded by design—delayed push notifications, missing call logs, weakened E911 behavior, and lack of Quality of Service protections. Device owners therefore pay twice: once for their devices and Wi-Fi, and again for carrier bundles, all while losing access to a lower-cost, native-quality alternative.

71. iOS/Android/Samsung OEM firmware had a consumer impact where identical entitlement/IMS gating across platforms enforces "no bundle, no native," leaving households to buy bundles to unlock native calling on owner devices. Additionally, a quality and safety delta existed. App-mode's push latency, incomplete call-logs, and reduced E911/QoS behaviors reflect

code-level deprivation of native features, not consumer choice. Moreover, this caused foreclosure to competition and overcharging of the class. With native parity blocked for stand-alone entrants, consumers lose the ~$6.50/month option and face persistent bundle overcharges; a neutral certification path would remedy access without sacrificing safety or lawful access.

72. **VoIP-Pal exemplar (no damages here):** VoIP-Pal's ready-and-able status—documented by independent audits and *inter partes review* records—demonstrates the feasibility of stand-alone native entry. The Lock–and–Key blocked native access on owner devices, chilling pilot programs and distribution opportunities. In this class action, VoIP-Pal seeks no damages and appears only in a limited posture, supporting injunctive relief that is coextensive with the class.

Property Commandeering and Joint Liability

73. Once a device is sold, it is the subscriber's property. Although subscribers receive only a license to use the operating system and firmware, those licensed layers are embedded in and necessary to operate the owned hardware. Defendants nevertheless pre-condition buyer-owned phones so that native telephony activates only for carrier services and not for independent rivals, implementing post-sale device control in code. Carriers supply the entitlement and IP Multimedia Subsystem, emergency, and quality-of-service inputs; platforms encode the gating at the operating-system and firmware layers. This property-license posture amplifies the coercion and confirms joint responsibility for the market-wide device mandate:

74. Apple (iOS — Lock on owner property) utilized entitlement-gated phone roles to commandeer the owner's device/Wi-Fi to enforce carrier-only native access. Google (Android/Pixel — Lock on owner property) utilized hasCarrierPrivileges()/IMS/CarrierConfig to convert carrier validation into a device-level mandate on owner hardware. Samsung (OEM firmware — Lock on owner property) utilized boot-time CSC/allow-lists to impose carrier-aligned

native access on the owner's Galaxy device. Additionally, the Carrier Co-Conspirators (the Key) utilized SIM/eSIM entitlements and IMS/E911/QoS inputs to drive the Locks. This combined posture confirms joint responsibility for the device mandate. LRA would include a neutral certification path to respect property rights and safety/lawful-access goals without post-sale commandeering.

THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-CONSPIRATORS PROFIT MOTIVE TO UNLAWFULLY ACQUIRE OR MAINTAIN MONOPOLY POWER THROUGH ANTICOMPETITIVE MEANS

75. Platform Provider Defendants Apple, Google, and Samsung as well as non-defendant Carrier Co-Conspirators AT&T, Verizon, and T-Mobile collectively control a multi-trillion-dollar market position and derive hundreds of billions in yearly gross profit. This concentration of power gave them both the incentive and ability to design and maintain the Lock–and–Key system. There was unified incentives and engineered exclusion:

76. The Carriers safeguarded Average Revenue Per User (ARPU), bundle economics, and offload savings by ensuring Wi-Fi Calling carried traffic without reducing voice/text revenues. Apple preserved premium handset margins and carrier-subsidy distribution; protected iMessage and FaceTime integration by relegating rivals to degraded "app mode." Google protected default placement rents (Search, Chrome, Play Store) and ad revenue; enforced carrier-only validation through code restrictions like hasCarrierPrivileges() and CarrierConfig. Samsung monetized preload and firmware exclusivity, generating revenues through carrier-aligned boot images and allow-lists that privileged carrier stacks. Across the tier, profit incentives align with the Locks and Keys, reinforcing the "no bundle, no native" mandate that excludes stand-alone rivals.

77. Together, these incentives ensured rivals could not achieve native parity. The financial logic was clear: exclusion kept bundle economics and platform rents intact. With iOS and Android

covering roughly 97% of the market, Defendants wield durable control over the only commercially viable route to consumers. They maintained that control not through superior products or technical necessity, but through the Lock–and–Key scheme. Native telephony was conditioned on carrier bundles without justification. A neutral certification process—applying the same E911, lawful access, and safety standards carriers already meet—would achieve legitimate aims without foreclosure. Refusing such an alternative is classic exclusionary conduct under § 2. Apple/Google/Samsung maintain device/OS chokepoints by code, not necessity; neutral certification remains feasible. AT&T/Verizon/T-Mobile's Keys ensure bundle retention and offload savings, completing the foreclosure loop.

78. Defendants' coordinated conduct—carrier promotions aligned with OS-level gating—operates as a unified exclusionary design harmful to competition and to VoIP-Pal's entry. The profit motives and exclusionary conduct are inseparable: the same device-level rules that maximize revenues are those that bar market entry for independent VoIP providers and standalone Wi-Fi Calling. The Lock–and–Key system lacks procompetitive justification and persists only because it pays. Uniform Locks and Keys resulted in antitrust injury, that prevented entry (VoIP-Pal) and consumer overcharge; no neutral certification offered despite obvious availability. The property commandeering, profit motives, and coordinated code-based restraints collectively ground § 2 maintenance and § 1 foreclosure theories against Platforms (Lock) and Carriers (Key).

THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-CONSPIRATORS HARM THE COMPETITIVE PROCESS

79. Although VoIP-Pal.com, Inc. is a named co-Lead Plaintiff in this action, it does not seek damages here. Instead, VoIP-Pal supports the Device-Owner Class by contributing concrete evidence of feasibility and exclusion, including the independent Smart421 technical audit and its

successful defense of key patents in *inter partes review* proceedings.[1] These materials demonstrate that stand-alone native Wi-Fi Calling was both technologically practicable and unlawfully foreclosed—facts that reinforce the plausibility of the antitrust claims and strengthen class wide standing.

ARTICLE III AND STATUTORY STANDING OF THE DEVICE-OWNER CLASS REPRESENTATIVES

Injury-in-Fact

80. Each Class Representative is a device owner who (i) paid supracompetitive bundle charges to unlock native calling on their own phone, and/or (ii) suffered functional degradation when declining the tie (push-notification latency, unreliable inbound wake/ring, missing call-logs, reduced E911 behavior, no QoS parity), and (iii) endured post-sale interference with private property because OS/firmware code disabled native behavior on owner devices absent carrier validation. These are economic and functional injuries that are concrete and particularized and the injuries are fairly traceable to Platform Provider Defendants' and Carrier Co-Conspirator's conduct: Platforms/OEMs encoded the Lock (OS/firmware gate); carrier co-conspirators supplied the Key (entitlements/IMS/E911/QoS). Without validation, owners' devices are coded to deny native functionality—directly producing the overcharge (to obtain native) and the functional loss (when refusing the tie).

Causation

81. Regardless of any rival's U.S. Patent Nos. technical capability, the Platform Provider Defendants force smartphone owners to buy/maintain bundles for native calling behavior, including Wi-Fi Calling. Identical native-versus-app outcomes across iOS, Android, and OEM

[1] See Appendix A, Exhibits 2003-2042 for a more extensive history of VoIP-Pal and Digifonica.

firmware foreclose inbound-native parity for the entire device-owner class. The handset is owner property, and the Wi-Fi/broadband path is owner-funded. A call initiates on the owner's device over the owner's Wi-Fi before any carrier completion. The barrier is implemented in the device itself: OS/firmware disable native behavior unless carrier validation passes. This transforms the owner's phone into an enforcement point for the bundle, making the injury concrete, particularized, and traceable.

Redressability

82. The classes injuries are redressable by (i) ordering parity access via neutral certification (native without bundle validation), (ii) entering a durable no-relock injunction (no re-imposition through OS updates, CarrierConfig flips, or firmware changes), (iii) awarding treble damages and restitution/disgorgement for classwide overcharges attributable to the device-level tie and a distribution plan under Rule 23(b)(3), and (iv) ordering a parity injunction requiring neutral certification for native telephony (default dialer, push-free inbound wake, system call-logs, E911 hooks, QoS, and related identity/continuity features) without bundle validation; a no-relock order; and technical monitoring/KPIs.

WI-FI CALLING IS AN ESTABLISHED, GROWING MARKET

Wi-Fi Calling Demand

83. **Adoption Trends (2019–2025).** By 2023–2024, Wi-Fi Calling was enabled on more than 90 percent of major carrier networks worldwide, including AT&T, Verizon, and T-Mobile in the United States and Vodafone and EE in Europe. Device support is now effectively universal: Apple's iOS has supported Wi-Fi Calling since the iPhone 5c (2013), and Google's Android platform has supported it across most models since 2016. Together, iOS and Android cover approximately 99.7 percent of the U.S. smartphone base. Usage spiked during the COVID-19

pandemic as home-based calling became routine, and it has remained elevated with the rise of unlimited plans that encourage carriers to offload voice traffic to Wi-Fi. These facts establish that Wi-Fi Calling is not experimental or niche but a present, mainstream market whose adoption curve continues to rise. The mainstream status of Wi-Fi calling underscores that demand exists; device-layer gating determines who can offer it natively:

84. In Apple (iOS), system-level Wi-Fi Calling support is longstanding; native activation depends on carrier entitlements (the Lock consuming the Key). In Google (Android/Pixel), Platform support is broad since ~2016, with native paths conditioned on hasCarrierPrivileges()/IMS provisioning. With Samsung (OEM firmware), Galaxy firmware implements carrier-aligned allow-lists/CSC configs to enable native Wi-Fi calling.

85. **Market Scale Indicators.** Industry data further confirms the scale of Wi-Fi Calling. In 2022, the Federal Communications Commission reported that Wi-Fi offload (voice and data) accounted for 60 to 70 percent of total mobile traffic in U.S. urban areas, with Wi-Fi initiation estimated at 10 to 20 percent of calls in supported markets. In 2021, the GSMA projected that Voice over Wi-Fi (VoWiFi) would carry 15 to 25 percent of global voice traffic by 2025 in regions with high Wi-Fi penetration. Telecom industry analyses in 2023 likewise indicated that in advanced markets, more than 50 percent of completed mobile calls already rely on IP-based telephony (including Wi-Fi), up from under 30 percent in 2019. With iOS/Android controlling the base, platform Locks decide native vs. app-mode despite large, proven usage.

86. **Consumer Use and Misrepresentation.** Consumers adopt Wi-Fi Calling because they believe it saves money and improves coverage. That demand already exists and is growing. If Defendants' device-level and entitlement-based restrictions were removed — and Wi-Fi Calling were permitted to operate as a stand-alone service without being tied to a cellular bundle — the

same adoption drivers (widespread home and office Wi-Fi, stronger indoor coverage, and consumer cost expectations) would cause stand-alone Wi-Fi Calling to expand even faster than current, bundle-tied usage. In practice, however, the savings are captured by Defendants. Wi-Fi calls complete only if the subscriber also maintains a paid cellular bundle. Consumers pay for their broadband connections and devices, while carriers and platforms offload network costs onto subscriber-funded Wi-Fi. "No bundle, no native." Platform Locks encode the bundle condition; carriers capture the savings from Wi-Fi offload.

87. **Barriers to Independent Entry.** Despite proven demand, independent providers such as VoIP-Pal could not enter or raise capital because Defendants blocked access to essential native telephony functions. Without native parity — including main-number binding, wake and ring capability, call-log integration, E911 functionality, and Quality of Service priority — a stand-alone offering is commercially non-viable. Apple, Google, and Samsung embedded device-level gates to ensure that native telephony is activated only for carrier-validated services, creating a Lock-and-Key design that allowed carriers to monopolize the Wi-Fi Calling market. With iOS and Android together controlling approximately 99.7 percent of U.S. smartphones, and with their OS, API, and default-dialer rules reinforced by OEM firmware, the result was categorical device foreclosure across virtually the entire smartphone base.

88. Apple (Lock) utilized entitlements for native parity; third-party providers relegated to app-mode. Google (Lock) utilized hasCarrierPrivileges()/IMS/CarrierConfig to gate native telephony; non-carrier lines lack parity. Samsung (Lock) utilized firmware/CSC allow-lists to tie native enablement to carrier validation. In contrast, a neutral certification pathway would unlock native access without bundle conditioning.

U.S. Record (admissible, domestic authorities)

89. U.S. regulators and industry sources confirm that Wi-Fi Calling is a mainstream, nationwide voice mode—offered by all national carriers and used at scale by U.S. subscribers. These domestic sources establish ubiquity; platform Locks decide parity and thereby control who can supply native Wi-Fi calling:

1. FCC (Orders/Dockets; Communications Marketplace Reports). Since at least 2016, the FCC has recognized Wi-Fi Calling as a standard, nationwide service implemented by AT&T, Verizon, T-Mobile, and Sprint, and regularly referenced in Commission proceedings as part of network operations, coverage, and 911 routing. (e.g., FCC orders addressing Wi-Fi Calling/TTY replacement; annual Communications Marketplace Reports noting carrier VoWiFi deployment and usage.)

2. CTIA (Wireless Industry Survey & testimony). CTIA reports present Wi-Fi Calling as a standard feature used by tens of millions of U.S. subscribers and integral to carrier coverage and spectrum-offload strategies.

3. Carrier admissions (public plan pages/FAQs). AT&T, Verizon, and T-Mobile advertise Wi-Fi Calling as "included at no additional charge", instructing subscribers to use Wi-Fi Calling routinely for indoor coverage and reliability—contemporaneous acknowledgments of substantial U.S. usage.

Ofcom (international regulator, time-series corroboration)

90. Ofcom's Connected Nations reports show VoWiFi's share of all mobile calls across UK MNOs rose from 0.22–12% (2019) to 9–17% (2024)—roughly one-tenth to one-sixth of all calls now occur over Wi-Fi. **Scope & source:** Ofcom's annual *Connected Nations* reports publish, for each UK mobile network operator (MNO), the share of all mobile calls made over Wi-Fi

(VoWiFi). Ofcom reports these as per-MNO ranges, not a single national average. Below are the exact ranges, year by year, with Ofcom as the primary source. Mature-market time series confirms rising Wi-Fi voice share consistent with U.S. ubiquity:

- 2019 (baseline): "The percentage of calls made using voice over Wi-Fi by the MNOs ranges from 0.22% to 12%." (Connected Nations 2019, p. 27).[2]
- 2020: "…has increased to between 2% and 18% per MNO (up from 0.2% to 12% last year)." (Connected Nations 2020, p. 40).[3]
- 2021: "…remained relatively stable… between 2% and 16% per MNO (compared with 2% to 18% in 2020)." (Connected Nations 2021, p. 40).[4]
- 2022: "…ranging between 2% and 17% across individual MNOs (compared with 2% and 16% in 2021)." (Connected Nations 2022, UK report).[5]
- 2023: "The percentage of voice over WiFi calls reported by MNOs range between 3% and 16% across individual MNOs." (Connected Nations 2023, p. 41).[6]

[2] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/infrastructure-research/connected-nations-2019/connected-nations-2019-uk-final.pdf

[3] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/infrastructure-research/connected-nations-2020/connected-nations-2020.pdf

[4] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/infrastructure-research/2021/connected-nations-2021-uk.pdf

[5] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/infrastructure-research/connected-nations-2022/connected-nations-uk-report.pdf

[6] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/multi-sector/infrastructure-research/connected-nations-2023/connected-nations-2023-uk-report

- 2024: "The percentage of voice over WiFi calls reported by three of the MNOs ranges between 9% and 17% across individual MNOs." (Connected Nations 2024, p. 34).[7]

91. Over six years the lower bound rose from 0.22% to 2% to 3% to 9%, while the upper bound settled in the 16–18% range. In plain terms, Wi-Fi Calling moved from near-zero to roughly one-tenth to one-sixth of all mobile calls by 2024 — despite being tied to paid cellular bundles. That is clear, regulator-verified evidence of strong user demand for native Wi-Fi voice. The growth occurred even under platform Locks; removing bundle conditioning via neutral certification would increase addressable standalone demand.

How the U.S. and Ofcom records work together

92. The U.S. record (FCC/CTIA/carrier admissions) establishes domestic ubiquity and significant usage of Wi-Fi Calling. Ofcom's time series supplies the quantified trajectory (2019–2024) that U.S. public sources do not publish, corroborating the same adoption pattern in a mature, highly comparable mobile market. Together, they show latent, addressable demand for native Wi-Fi voice; the reason that demand has not become a U.S. standalone native-parity market is device-layer gating (entitlements/CarrierPrivileges/allow-lists) plus bundle-conditioning. Open the gate (neutral certification) and decouple from bundles, and the same demonstrated usage becomes addressable demand for standalone native Wi-Fi Calling in the U.S. Platform Locks (Apple/Google/Samsung) and carrier Keys explain the gap between usage and standalone supply.

Subscriber perception vs. economic reality (why this matters)

93. Subscribers naturally believe a Wi-Fi call saves them money because it rides over

[7] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/multi-sector/infrastructure-research/connected-nations-2024/connected-nations-uk-report-2024.pdf

their broadband. In reality, the savings flow to carriers: the call remains tied to a paid bundle, while device software withholds native inbound parity unless the line is carrier-validated. Carriers capture cost reductions by offloading from licensed spectrum to subscriber-funded Wi-Fi without lowering bundle prices. Consumers pay for the device and the broadband, then pay again for the bundle; the carrier pays less to carry the call. Code-level conditioning (no bundle, no native) shifts savings to carriers and maintains platform rents; neutral certification would realign benefits to consumers and enable stand-alone competition.

Technical Interdependence

94. **Appendices B and C** demonstrate that the exclusion of third-party Voice over IP (VoIP) providers from competing equally with mobile carrier telephony is the result of an interdependent mechanism, described as the Lock-and-Key scheme. Carriers provide the necessary credentials (the Key) through specifications, entitlement servers, and IMS profiles, while Platforms (Apple and Google) and Major OEMs (Samsung) embed the mechanisms (the Lock) that validate and consume those credentials, restricting system access to only authorized services. Without the Lock embedded in the operating system or firmware, non-carrier VoIP applications could achieve parity with native telephony features; conversely, without carrier credentials, the Platforms' Locks would be inoperable. This collaboration yields market-wide exclusion. The specific roles and expansion of the Lock mechanism for Apple, Google, and Samsung are detailed below:

Apple (The iOS Lock)

95. As discussed in Appendix B, Section D, Apple implements the Lock in iOS by embedding entitlement/IMS checks that require the carrier's Key before native telephony features, such as Wi-Fi Calling, can activate. This system systematically grants carriers privileged OS integration, starkly sidelining independent VoIP providers. Carrier Bundles and Entitlement Checks: Apple

provides deep support and entitlements for carrier telephony via "carrier bundles". These bundles are carrier-specific configuration files containing network settings, feature flags, and crucial entitlement server addresses. The use of entitlement servers requires an Apple proprietary protocol called the "Entitlement Layer Protocol" for VoWiFi operation on any Apple device. Privileged System Access: Carriers leverage these bundles to set up their telephony, including VoWiFi and VoLTE, without needing separate applications or standard App Store review. Carrier apps may use special entitlements to gain access to Core Telephony APIs (like eSIM APIs) that are unavailable to non-carrier apps, enabling deep iOS, modem, and network stack integration.

96. Exclusion of Third Parties: Apple's architecture reserves privileged frameworks, native IMS implementations (which include integrated SIP and RTP protocols), and direct modem interaction for carrier telephony only. Independent VoIP apps are confined to sandboxed execution and must rely on standard public APIs like CallKit and PushKit for basic user interface and notification integration. QoS Advantage: Native carrier VoWiFi traffic benefits from powerful, OS-level Quality of Service (QoS) controls by default, enabled through carrier bundles. This allows the OS to apply IP-layer Differentiated Services Code Point (DSCP) markings to prioritize carrier voice packets, an advantage unavailable to third-party apps, which lack public APIs for direct DSCP manipulation.

Google (The Android Lock)

97. As discussed in Appendix B, Section C, Google implements the Lock in Android by reserving true OS integration as a carrier-exclusive domain, structurally guaranteeing carrier supremacy over independent VoIP competition. Android's design choices consistently align with carrier telephony while failing to provide equivalent system-level support for independent VoIP telephony. Carrier Bundles and Entitlement Checks: Android uses the `TelephonyManager` API

method `hasCarrierPrivileges()` to consume the Key. This method acts as a "lock" or a code-level gate that determines if the calling application has been granted carrier privileges by the carrier. If not granted, many powerful `TelephonyManager` API features are unavailable to the application, locking VoIP apps out of numerous functions like manipulating network selection and accessing subscriber data. Android uses `CarrierConfigManager` to dynamically apply hundreds of carrier-specific settings (including VoLTE, APNs, and Wi-Fi Calling) via the `CarrierService`. This functionality is exclusive to carriers. The Lock is also enforced through IMS binding, where the built-in carrier IMS framework (`ImsService`) enables carrier Wi-Fi Calling, VoLTE, and RCS, often authenticated through carrier-specific entitlement checks.

98. Silent Configuration: CarrierConfig allows carriers to maintain silent, remote control over device settings, enabling the seamless provision of fundamental device configurations without requiring user consent or interaction. Independent VoIP providers have no symmetrical configuration mechanism. Systemic Disadvantage: Google reinforces this Lock by abandoning native support for independent VoIP protocols like SIP and RTP, transferring development burden and performance challenges onto third-party VoIP developers. This ensures that true OS integration remains a carrier monopoly.

Samsung (OEM Enforcement)

99. Samsung enforces the Lock as a major Android OEM by facilitating carrier dominance through firmware controls and device architecture. Samsung's role is to ensure that the required Lock features are implemented at the device level, particularly for North American carriers. Firmware and CSC Allow-lists: Samsung utilizes the Consumer Software Customization (CSC) system to implement the Lock at boot. CSC profiles load distinct, carrier-specific firmware builds tailored to specific carriers (e.g., Verizon, AT&T), which automatically activate when a carrier

SIM is installed. These customizations deploy carrier applications with system-level privileges and enforce restrictions on features like VoLTE or Wi-Fi Calling if non-certified firmware is detected. Without carrier inputs, native features are withheld. Hardware Locks (Knox): Samsung's Knox security platform enforces firmware controls at the hardware level. If unauthorized software is flashed, a hardware security mechanism (the Knox e-fuse) is irreversibly tripped. Once tripped, access to high-security applications like Samsung Pay is permanently disabled and the device warranty is voided.

100. Bootloader Restrictions: Samsung devices sold in the U.S. and Canada often have permanently locked bootloaders, which is understood to be a requirement from North American carriers, preventing users from installing alternative operating systems that might bypass carrier restrictions. Lack of VoIP Support: In contrast to its extensive customization for carriers, Samsung does not provide equivalent firmware support for independent VoIP telephony services. Coordinated Action: Samsung reinforced carrier control over messaging by transitioning its Android devices to Google Messages, thereby cementing Google's control over the carrier-oriented RCS protocol, which excludes independent VoIP messaging innovation.

Infrastructure Exclusion ("Initiation Edge")

101. **Appendices B and C** also highlight what this exclusion means at the level of infrastructure. A smartphone is not merely a consumer product; it is subscriber-owned property and a node in a network. The broadband path and Wi-Fi access over which calls are transmitted is also subscriber-funded. When a user taps "Call," initiation begins on the subscriber's device over the subscriber's Wi-Fi and broadband. Only after the device-level gate is satisfied does the carrier have any role in completing the call. The challenged Lock decides whether the call will be treated as native — with all the attendant system privileges — or relegated to app-mode. In effect, the Lock denies

subscribers the full use of their own devices and their own networks unless they continue to pay for a carrier bundle. Apple/Google/Samsung include device-code at the Lock determines native vs. app at initiation; the Key only enters after native is granted. Owner devices and Wi-Fi are commandeered by code-level gating to enforce bundle purchase ("no bundle, no native").

Undisputed Facts that Show a Conspiracy to Attempt to Monopolize Wi-Fi Calling

102. **Appendices B and C** documents undisputed facts about how this exclusion is implemented. First, phones must pass SIM or eSIM checks and entitlement validation before the operating system enables native Wi-Fi Calling. On iOS, carrier bundles and entitlements gate access to the native Phone role. When entitlement is absent, third-party VoIP is confined to CallKit and PushKit, which are degraded substitutes subject to notification delays and background restrictions. On Android, functions such as hasCarrierPrivileges(), CarrierConfig, and IMS binding enforce the same rule. Native SIP and RTP stacks have been removed from later versions of Android, and Pixel devices ship as carrier-only reference builds. On Samsung devices, firmware enforces the lock at boot time. Allow-lists block non-carrier applications from being recognized as native, and default-dialer capture ensures that only carrier-approved apps are privileged. The functional gap is stark. Native paths receive full user interface integration, reliable logs, dependable background ringing, E911 hooks, and QoS treatment. App-mode alternatives lack these functions and are throttled by design. The record also proves feasibility. Early implementations of Google Fi provided native-dialer Wi-Fi calling through certification, showing that parity was technically possible with respect to certain functionality.

103. The present limitation is not one of physics, but one of policy encoded into the operating system. Apple utilized entitlement/bundle gating → third-party VoIP confined to CallKit/PushKit (latency/background limits). Google utilized hasCarrierPrivileges()/CarrierConfig/IMS binding;

deprecation of native SIP/RTP; Pixel as carrier-reference build. Samsung utilized boot-time firmware enforcement; allow-lists and default-dialer capture privilege carrier stacks. In contrast, Google Fi's prior certification-based native dialing evidences neutral certification feasibility.

Platform Roles, OEM Enforcement, System Mechanics, And Antitrust Injury

104. **Roles of the Platform Provider Defendants and OEM.** Google functions simultaneously as a gatekeeper and as a competitor. On Android, Google determines which lines are treated as "native" and which are relegated to "app-mode." Controls such as hasCarrierPrivileges(), CarrierConfig, and IMS binding dictate whether a line is recognized as the device's real identity. At the same time, Google competes directly through Google Fi, Google Voice, and Google Messages. By deprecating native SIP and RTP functionality in newer versions of Android, Google forced independent VoIP providers into a degraded lane while its own integrated services retained operating system advantages. In this way, Google both guards the gate and benefits from determining who gains entry. Gatekeeper-competitor conflict (Android/Pixel) mirrors the Lock's design and its competitive effects at the device chokepoint.

105. Apple acts as the platform controller and a direct competitor. It sets the rules for iOS telephony through carrier bundles and entitlement checks. Although third-party VoIP applications may operate through CallKit and PushKit, they are subject to background and timing limitations that never equal the native Phone role. By contrast, Apple's own services—FaceTime, iMessage, continuity features, and identity integrations—as well as carrier Wi-Fi Calling, receive native reliability and full emergency integration. These are not technical necessities but policy choices embedded in code. iOS rules privilege Apple/carrier services at the native lane while relegating rivals to app mode—an implementation of the Lock

106. Samsung is not pleaded as a platform competitor but as the OEM and firmware enforcer. Its

role is to apply carrier-specific firmware images, boot policies, default-dialer allow-lists, and privileged permissions that honor the operating system gates and ensure that native access remains reserved for carrier-approved stacks. Put simply, if the platforms supply the Lock, Samsung ensures that the hinges cannot be removed. OEM enforcement cements platform Locks in hardware/firmware so carrier-validated stacks alone receive native parity.

107. **Resulting Antitrust Injury.** At least one competitor, VoIP-Pal, was prepared to enter the market with a stand-alone, low-cost Wi-Fi Calling service. The encoded Lock, however, denied native parity on subscriber-owned devices, making it impossible for any to enter to market to conduct credible pilots, raise capital, secure distribution, or license its technology. This is prevented-entry injury flowing directly from the exclusionary mechanism condemned by law. Consumers have also been injured. They are required to pay twice: once for the phones and Wi-Fi infrastructure they already fund, and again for carrier bundles that must be purchased to unlock native calling. The "app-mode" alternative is degraded by design—saddled with latency, incomplete logs, weaker E911 behavior, and no QoS parity. These overcharges and functional degradations persist not because of product merit but because Defendants have closed the native lane to stand-alone competitors. Apple/Google/Samsung implement/ enforce the Lock; carriers supply the Key → "no bundle, no native." A neutral certification injunction would restore native parity without compromising safety, E911, or lawful access.

THE PLATFORM PROVIDER DEFENDANTS VIOLATE SHERMAN ACT § 2

Platform Provider Defendants' Monopoly Maintenance

108. On approximately 97 percent of U.S. smartphones, the operating system determines whether a service is treated as "native." When a service is recognized as native, the phone wakes the Phone application, writes to the system call-log, triggers E911 hooks, and receives Quality of Service

priority. Non-native inbound calls are handled in "app-mode," which relies on delayed push notifications, excludes calls from system logs, weakens emergency functionality, and strips away QoS protections.

109. Apple iOS grants default Phone role, push-free inbound wake/ring, call-log, E911, and QoS only to lines it recognizes as native. Google Android's default-dialer/PhoneAccount and system integrations attach to native; app-mode lacks those privileges. Samsung's Galaxy firmware/CSC policies reinforce native privileges and restrict app-mode behaviors.

110. Apple, Google, and Samsung placed the gate at this chokepoint and coded it to open only after carrier validation. That design choice is the foundation of the Platform Provider Defendants' liability under Sherman Act § 2. First, § 2 is violated when monopoly power is maintained by exclusion rather than merit. By writing iOS and Android so that native calling activates only when a carrier validates the line, the Platform Provider Defendants maintain control over the only commercially viable route for mobile voice—by design, not through product superiority. Second, platform-level defaults and technical restraints that close critical distribution channels constitute exclusionary conduct under § 2. The coded rule **no bundle, no native calling** is precisely the sort of foreclosing default that creates a violation. Third, uniform inbound behavior across Apple iOS, Google Android, and Samsung's firmware, to the same carrier specifications, demonstrates coordinated preservation of the native lane—a maintenance conspiracy at the device layer. Samsung's role as the OEM and firmware enforcer of that gate ensures that the coordinated restriction is fully implemented at the device level.

111. Apple (Lock) utilized entitlement/IMS gating opens native only after Apple-recognized carrier validation—an exclusionary default at the chokepoint. Google (Lock) utilized hasCarrierPrivileges()/CarrierConfig/IMS binding condition native on carrier validation across

Android/Pixel. Samsung (Lock) utilized OEM firmware/CSC allow-lists implement the same gate device-wide, evidencing coordinated preservation of the native lane. In contrast, a neutral certification path would achieve E911/lawful-access/QoS aims without foreclosing stand-alone entrants.

Carrier Defendants' Conspiracy and Bundle Preservation

112. The national carriers require that only their validated lines ring natively, and they act in concert to enforce this rule. They refuse to interoperate with independent providers and they supply identical entitlement, IMS, E911, and QoS inputs that the platform gate requires. This conduct satisfies multiple theories of § 2 liability. First, competitors conspire to monopolize when their coordinated conduct reflects a shared exclusionary purpose. The carriers' uniform **no bundle, no native calling** rule, implemented through common validation inputs, is a current, ongoing conspiracy to exclude non-carrier inbound calls from the native lane and to preserve supracompetitive bundle revenues. Second, the carriers' coordinated validation regime—embedded by the platforms into operating system and firmware rules—constitutes concerted maintenance of monopoly power. This exclusion is achieved through device-layer design, not merit. AT&T/Verizon/T-Mobile supply SIM/eSIM, IMS, E911, QoS inputs consumed by the platform Locks to enforce native-only for bundled lines. iOS/Android/Samsung firmware encode the carriers' regime into device code, turning validation into a distribution gate.

113. Third, each carrier controls the validation key to its own subscriber base—the effective lane to those users' native dialers—and, by conditioning inbound validation on paid bundles and denying parity to independent providers, each demonstrates specific intent and a dangerous probability of monopolizing native inbound telephony for its subscribers. Finally, the carriers are liable as co-conspirators in platform maintenance. The platforms' § 2 maintenance at the OS and

firmware gate could not operate without the carriers' coordinated validation inputs. By supplying those inputs, the carriers further and complete the exclusion, making them knowing participants in the platforms' unlawful maintenance scheme. Accordingly, in the carrier-focused complaints, the Carrier Defendants are pleaded as the Sherman Act § 2 defendants (for conspiracy to monopolize, conspiracy to maintain, maintenance conspiracy, and attempted monopolization), while the Platform Provider Defendants are pleaded as co-conspirators whose code embeds the inbound gate that the carriers demand. Specific intent & probability. Conditioning validation on bundles and denying parity results in a dangerous probability of monopolizing native inbound for each carrier's base. Platform Locks depend on carrier Keys; carriers knowingly supply them, completing the § 2 maintenance scheme.

114. The Carrier Co-Conspirators drive a business model to force tying and the Platform Provider Defendants (Apple, Google, Samsung) enable the tie at the device level. Through OS entitlements, default-dialer control, push/wake privileges, call-log access, E911/QoS hooks, and firmware allow-lists, they reserve native phone functions for carrier-validated lines and withhold native parity from independent providers. The net effect is simple: no practical path to standalone Wi-Fi Calling on the phone's native lane—only the carrier-bundled version. Apple/Google author the Locks; Samsung enforces via firmware; carriers supply the Keys—together producing device-level tying in code.

115. Carriers condition access to the native telephony lane on purchase of the bundle and then brand the native Wi-Fi functionality as "no charge" inside that bundle—an economically illusory presentation that masks the exclusion and foreclosure a standalone, native-parity Wi-Fi Calling. Platform-level gating (OS/firmware) comprises the Platform Provider Defendants' Lock (preventing native parity for independents) and the Carrier Co-Conspirators supply the

authorized Key (SIM/eSIM validation and bundling), ensuring the only native path is the bundled one. Meanwhile, the subscriber funds and initiates calls over subscriber-paid broadband, while Defendants profit by (i) conditioning native access on the bundle and (ii) offloading traffic to shift costs onto subscriber-funded infrastructure. Device code and carrier validation converts the subscriber's own device/Wi-Fi into an enforcement point for bundles ("no bundle, no native").

116. Separately, the "no charge" claim by the Carrier Co-Conspirators is predatory pricing—a giveaway that looks consumer-friendly but kills competition. On paper the price is $0; in reality, carriers cover it with bundle revenues and push the actual connection costs onto subscriber-funded Wi-Fi/broadband. At the same time, OS/firmware restrictions block rivals from the native lane, forcing them into inferior "app-only" calling. That makes any standalone native-parity offer look unnecessary or "overpriced," even though the playing field is rigged. Once rivals are deterred, carriers recoup by keeping high bundle margins and banking offload savings from calls shifted onto subscriber-paid networks. The repeated "no charge/included" messaging also trains consumers to believe Wi-Fi Calling has no independent value outside the bundle, choking off demand for true alternatives. This false zero-pricing is not generosity; it is a coordinated device-and-bundle strategy to stamp out standalone Wi-Fi Calling and maintain monopoly control. False zero-price and device-level foreclosure deters entry, sustains bundle margins, and captures offload rents; the remedy is neutral certification and parity access at the native lane.

CONSPIRACY UNDER SHERMAN ACT § 2 BY THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-PARTICIPANTS

117. A conspiracy under Sherman Act § 2 exists when separate firms align their conduct with a shared exclusionary purpose and take overt acts to acquire, maintain, or attempt to maintain monopoly power. Courts treat coordinated conduct as functioning as a single enterprise even in the absence of corporate merger. Platform defaults and technical restraints that close critical routes

to market qualify as exclusionary conduct. Maintenance of monopoly power through exclusion rather than merit violates § 2. The essential elements are agreement or alignment, an exclusionary aim, overt acts such as rules, defaults, or validations, and resulting monopoly maintenance or attempted monopolization. Apple (iOS), Google (Android/Pixel), and Samsung (OEM firmware enforcement) form the platform side of the conspiracy: they each supply or enforce the Lock. AT&T, Verizon, and T-Mobile form the carrier side of the conspiracy: they supply and coordinate the Key. The result is a two-tier conspiracy: Platforms (three enterprises) and Carriers (three enterprises) form one unified § 2 scheme.

The Platform Provider Defendants

118. Apple and Google control the device-layer chokepoint and coded the gate so that native functionality—Phone application wake for inbound calls, call-log entries, E911 hooks, and Quality of Service—activates only after carrier validation. Independent providers are pushed into degraded app-mode. iOS, Android, and OEM firmware apply the same validation-gated rule to the same carrier specifications, producing uniform results that are not plausibly unilateral. The overt acts include entitlement checks, the hasCarrierPrivileges() function, CarrierConfig and IMS binding, removal of SIP and RTP functionality, and OEM boot images and dialer allow-lists. With approximately 97 percent of operating system share, this design maintains control by exclusion. The coordinated defaults constitute exclusionary conduct, establishing a maintenance conspiracy at the device layer. Samsung's role as OEM is pleaded as the firmware enforcer of that gate.

119. Apple iOS utilized entitlements/CarrierBundles to gate native access. Google Android utilized hasCarrierPrivileges(), CarrierConfig, IMS binding, and removal of SIP/RTP stacks to force carrier-only validation. Samsung utilized OEM firmware/CSC allow-lists and default-dialer enforcement to align with iOS/Android rules, ensuring carrier gating is applied at boot.

The Carrier Co-Conspirators

120. AT&T, Verizon, and T-Mobile supply and coordinate the Key through SIM and eSIM entitlements, IMS, E911, and QoS profiles, and they refuse interoperation that would allow non-carrier lines to ring natively. Their uniform **no bundle, no native calling** rule, coupled with identical validation inputs, constitutes a § 2 conspiracy. Their coordinated validation regime, embedded in operating system and firmware rules, represents concerted maintenance of monopoly power. For each carrier individually, control of the validation key to its subscriber base establishes attempted monopolization: anticompetitive conduct, specific intent, and a dangerous probability of success. By conditioning native number validation on bundled purchases and denying parity to independents, each carrier demonstrates the specific intent and probability of monopolizing native telephony for its subscribers. The carriers are also co-conspirators in platform maintenance, because the platforms' exclusionary gate could not operate without the carriers' validation inputs.

Two Tiers of Conspiracy Across the Complaints

121. In the platform-focused complaints, the Platform Provider Defendants are pleaded as the § 2 violators (monopoly maintenance and maintenance conspiracy), with the carriers as co-conspirators supplying the validation key. In the carrier-focused complaints, the Carrier Co-Conspirators are pleaded as the § 2 violators (conspiracy to monopolize, maintenance conspiracy, and attempted monopolization), with the platforms as co-conspirators embedding and enforcing the gate. Three enterprises (Apple, Google, Samsung) form one platform tier; three enterprises (AT&T, Verizon, T-Mobile) form one carrier tier resulting in a two-tier conspiracy.

Recognized Application of Conspiracy Doctrine

122. Although a six-actor, real-time § 2 conspiracy spanning multiple layers of a technology stack is unusual, the aligned code and coordinated validations of the Platform Provider Defendants

and their Carrier Co-Conspirators produce a uniform market result: non-carrier lines are coded not to ring natively unless a carrier bundle is present. That fact reflects agreement, exclusionary intent, and overt acts that together infer or constitute a § 2 conspiracy and its maintenance to monopolize native calling (including Wi-Fi Calling). Agreement is shown by identical validation-gated rules across iOS, Android, and Samsung firmware confirm concerted platform behavior. An exclusionary purpose is shown through carrier validation and bundle conditioning closes the native lane to stand-alone rivals. A market-wide effect is shown through consumers nationwide are forced into bundle purchase to access native calling.

Unified Liability Across Four Complaints

123. Across both platform cases and both carrier cases, the same Sherman Act § 2 liability is alleged: a device-layer inbound-call barrier maintained by platforms and preserved by carriers. This exclusion is proven by the public technical record—including developer documentation, entitlement specifications, and consistent device behavior—and by the existence of a feasible neutral certification alternative for safety, E911, and lawful access.

124. The role alignment is explicit and consistent: platforms first, carriers second—two tiers, one Sherman Act § 2 breach. Apple (Lock) iOS entitlement gating concealed behind "included" messaging. Google (Lock) Android hasCarrierPrivileges()/CarrierConfig gating paired with "included" claims. Samsung (Lock and enforcement) firmware/CSC allow-lists ensure gating persists device-wide. The Carriers (Key) utilized SIM/eSIM, IMS, E911, QoS validations and their "no additional charge" representations.

THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-CONSPIRATORS VIOLATE RICO (18 U.S.C. §§ 1962(c)–(d)) — PREVENTED-ENTRY FRAUD SCHEME

125. The Platform Provider Defendants and Carrier Co-Participants coordinated a scheme to foreclose entry of VoIP providers into the native telephony market by embedding entitlement and

firmware gates across iOS, Android, and Samsung devices, conditioned on carrier validation. This "Lock-and-Key" system was concealed by uniform public claims that Wi-Fi Calling was "included / no additional charge." These acts constitute a pattern of mail and wire fraud carried out through an association-in-fact enterprise, directly injuring competition and the class.

The RICO Enterprise (Association-In-Fact)

126. **Enterprise & Common Purpose.** Apple, Google, Samsung (the "Platform Provider Defendants"), together with AT&T, Verizon, and T-Mobile (the "Carrier Defendants"), form an association-in-fact enterprise under 18 U.S.C. § 1961(4). Their common purpose was to exclude VoIP providers from native telephony access, preserving bundled revenues and platform rents, and causing the class to pay for bundled services.

127. **Roles & Relationships. Platforms (the "Lock"):** Apple required carrier entitlements for default dialer, E911, and QoS functions; Google enforced hasCarrierPrivileges/CarrierConfig rules; Samsung deployed firmware allow-lists tied to carrier validation. **Carriers (the "Key"):** Carriers conditioned validation on bundle purchase and coordinated uniform messaging. **Continuity:** These technical gates and aligned messages were shipped and maintained across OS and firmware cycles, ensuring ongoing enterprise activity. Apple utilized entitlements/CarrierBundle preconditions for native; continuity across iOS releases. Google utilized hasCarrierPrivileges()/CarrierConfig/IMS binding; continuity across Android versions (with SIP/RTP deprecations). Samsung utilized boot-level CSC/allow-lists; continuity via carrier-specific images across device generations. The Carriers utilize ongoing validation/bundle conditioning as well as uniform "included" messaging surrounding Wi-Fi Calling.

Conduct/Participation — "Operation Or Management"

128. The Platform Provider Defendants and Carrier Co-Participants conducted or participated,

directly or indirectly, in the enterprise by designing, shipping, or enforcing gating mechanisms and conditioning validations on carrier bundles. Co-conspirator directors and officers approved these measures, satisfying the "operation or management" standard. The Platforms Provider Defendants code authorship/release management for Locks (iOS/Android/firmware). The Carrier Co-Conspirators design/operation of entitlement servers and validation regimes that the Locks consume.

Pattern Of Racketeering — Mail & Wire Fraud (18 U.S.C. §§ 1341, 1343)

129. The Platform Provider Defendants and Carrier Co-Participants engaged in a pattern of racketeering consisting of fraudulent messaging and transmitted uniform "Wi-Fi Calling is included at no additional charge" messages while omitting that (i) bundle purchase/retention was required, (ii) calls were offloaded to subscriber-funded Wi-Fi, and (iii) independent providers like VoIP-Pal were barred from native parity. The net impression was materially misleading. These omissions and gating practices recurred across defendants and release cycles and showed regular continuity. Apple/Google/Samsung authored/maintained the code that made the omissions material by enforcing device-level gating; carriers amplified the deception via public claims. Exemplars include:

- Carrier web pages advertising "Wi-Fi Calling included / no additional charge" without disclosure of gating[8];
- Apple developer documentation requiring carrier entitlements[9];

[8] See Appendix D.

[9] See "D. Apple's iOS Privileges Carrier Telephony over VoIP Telephony" in Appendix B.

- Android AOSP/SDK materials showing hasCarrierPrivileges and CarrierConfig control telephony policy[10];
- Samsung CSC/firmware allow-lists tying native telephony to carrier-validated apps[11].

Proximate Cause — Direct Injury To VoIP-Pal

130. The Platform Provider Defendants and Carrier Co-Participants controlled both the deceptive messages and the gating mechanisms. No third-party discretion intervened. The direct and intended result was VoIP provider exclusion from native access which corrupted the competitive process. The Locks (Apple/Google/Samsung) and the Keys (carriers) enforce a categorical bar on native parity and caused harm to the class.

RICO Conspiracy (18 U.S.C. § 1962(d))

131. The Platform Provider Defendants and Carrier Co-Participants conspired to violate § 1962(c) by agreeing to maintain the Lock-and-Key enterprise, conceal its exclusionary design, and perpetuate the omission-based messaging. Liability under § 1962(d) attaches even absent proof that each conspirator personally committed two predicate acts, so long as they agreed to the common scheme. Common rules/messages across releases and firms demonstrate an agreement to the scheme's essential nature.

Use of Investment of RICO Income (18 U.S.C. § 1962(a))

132. The Platform Provider Defendants and Carrier Co-Participants used and reinvested racketeering proceeds from the "no-additional-charge" scheme to finance, expand, and enforce the OS/firmware gating infrastructure (iOS entitlements/validation; Android

[10] See "C. Google's Android OS Privileges Carrier Telephony over Non-Carrier VoIP Telephony" in Appendix B.

[11] See "E. Samsung's Android Phones Privilege Carrier Telephony over Non-Carrier VoIP Telephony" in Appendix B.

hasCarrierPrivileges/CarrierConfig; Samsung CSC/allow-lists) and to run coordinated OS-level messaging that normalized the omission. These racketeering proceeds were used to finance, expand, and enforce the extended foreclosure and caused new, incremental injuries to device-owners (continued overcharges; sustained loss of native functionality and device value) beyond the initial misrepresentations; and further foreclosed the native route-to-market of any VoIP provider. Platform code pipelines and carrier validation infrastructure expanded with proceeds, entrenching the scheme across cycles.

Acquisition Or Maintenance Of Control (18 U.S.C. § 1962(b))

133. Section 1962(b) targets injuries by reason of a defendant's acquisition or maintenance of control of an enterprise through racketeering. By using racketeering to lock native telephony channels behind platform gates across successive OS/firmware cycles, Defendants maintained de facto control over the only economically viable native-parity route-to-market. The class was thus required to pay for bundled services at higher prices.

CO-CONSPIRATOR DIRECTORS' LIABILITY & CIVIL CONSPIRACY

Ongoing Knowledge and Inaction

134. More than a year has passed since VoIP-Pal filed its carrier antitrust and parallel class complaints. During that period, the boards of directors and senior officers of Apple, Google, Samsung, AT&T, Verizon, and T-Mobile have been on notice of the exclusionary conduct challenged here. Despite this notice, they have taken no corrective action. The entitlement-gated Lock remains deeply embedded in iOS, Android, and OEM firmware. Carrier Keys are still required for native telephony. And the marketing message that Wi-Fi Calling is *"included / no extra charge"* continues to be disseminated, even though native functionality is in fact conditioned on bundle purchase. This ongoing non-remediation is not accidental. It reflects deliberate inaction

after formal notice of wrongdoing. Courts recognize that continuing a course of conduct after being placed on notice is strong evidence of scienter. Directors and officers cannot plausibly claim ignorance; their silence and ratification prolong the unlawful scheme.

Personal Civil Liability for Individual Co-Conspirators Under Federal Law

135. Under the Sherman Act, corporate officers and directors who authorize, direct, or knowingly participate in the alleged unlawful restraints to trade and monopoly maintenance are personally liable when knowingly participating in effecting an illegal contract, combination or conspiracy, be he one who authorizes, orders or helps to perpetrate the crime, regardless of whether he is acting in a representative capacity. Second, under RICO §§ 1962(c)–(d), an officer who conducts or participates in the enterprise's affairs through a pattern of mail or wire fraud is subject to civil liability and treble damages. This includes officers who approve device-level conditioning and omission-based marketing such as the *"included / no extra charge"* message.

136. Co-conspirator directors and officers (non-defendants) approved and ratified policies that encode entitlement gating into iOS and Android, including Apple's carrier bundles, Android's hasCarrierPrivileges() and CarrierConfig rules, IMS bindings, and Samsung's boot-level allow-lists. They permitted and reinforced default-dialer rules that withhold native parity from independent providers. They authorized market communications falsely advertising Wi-Fi Calling as *"included / no extra charge,"* despite knowing that such service is disabled without a carrier bundle. They concealed from consumers that their devices and Wi-Fi infrastructure are fully capable of supporting stand-alone calling. And they continued this conduct after notice. Even after VoIP-Pal's complaints were filed and regulators were alerted, the boards and executives allowed operating system updates, firmware releases, and carrier profiles to proceed without lifting the Lock. They maintained the device-level mandate despite the existence of less-restrictive

alternatives, such as neutral certification. This post-notice continuation underscores scienter. Directors and officers cannot claim ignorance; they have chosen to perpetuate the scheme rather than remediate it.

Remedies for Co-Conspiratorial Conduct

137. Violations by co-conspirator directors and executives (non-defendants) may be remedied by: Injunctions barring directors from approving any OS, API, firmware, or entitlement changes that condition native access on bundle purchase. Instead, co-conspirator directors and executives should be required to adopt and oversee a parity certification program that applies the same neutral safety, lawful-access, and E911 standards to all providers; Board-level certifications and oversight mechanisms. Each year, boards should certify that native parity is offered on nondiscriminatory, bundle-free terms, and that no re-locking mechanisms have been introduced. Boards should also be required to establish dedicated compliance committees responsible for monitoring parity access.

138. Clawbacks and disgorgement of incentive compensation and equity gains causally tied to the Lock–and–Key scheme. Clawbacks would prevent directors and officers from retaining unjust enrichment and would ensure accountability. Appointment of a neutral technical monitor with authority over parity key performance indicators, entitlement and CarrierConfig decisions, and remediation timelines. Directors and officers should be required to cooperate fully with the monitor, who would provide independent oversight to the Court.

THE PLATFORM PROVIDER DEFENDANTS AND CARRIER CO-CONSPIRATORS VIOLATE ADDITIONAL ANTITRUST LAWS

139. This case presents the Platform Provider Defendants and their non-defendant co-conspirators as a single enterprise (two tiers acting as one) on subscriber-owned devices: Platform Provider Defendants coded the Lock (operating-system, application-programming-interface, default-dialer, and firmware gates) and carrier co-conspirators supplied the Key (SIM or eSIM

entitlements and profiles for the IP Multimedia Subsystem, emergency routing for E911, quality-of-service, and over-the-air provisioning), producing a uniform device-level mandate that excludes independent rivals from non-replicable native interfaces.

140. Apple (Lock) iOS utilized carrier bundles/entitlements and phone-role gating. Google (Lock) Android utilized hasCarrierPrivileges(), CarrierConfig, IMS binding; default-dialer privileges. Samsung (enforcement) utilized firmware/CSC allow-lists, boot policies, default-dialer capture. The Carriers (Key) utilized SIM/eSIM, IMS, E911, and QoS and OTA provisioning provide the validations consumed by the Locks.

Sherman Act § 1 — Unreasonable Restraint

141. Defendants combined and conspired to restrain trade in violation of Section 1 of the Sherman Act by tying native Wi-Fi calling to the purchase of carrier bundles and by implementing exclusive-dealing restrictions at the operating system and device level. The conspiracy operates in a hub-and-spoke pattern. The Platforms — Apple, Google, and Samsung — act as the hub, encoding operating system and firmware rules that enforce the restraint. The Carriers — AT&T, Verizon, and T-Mobile — act as the spokes, supplying entitlement credentials, IMS and E911 specifications, and the marketing message that Wi-Fi Calling is *"included / no extra charge."* Together, the two tiers implement a single device-level mandate: **no bundle, no native calling**. Hub (Platforms). Code-level restraints in iOS/Android/Samsung firmware. Spokes (Carriers). Uniform validations and "included/no extra charge" messaging.

142. Apple, Google, and Samsung orchestrated uniform OS-level rules and smartphone hardware that coordinated the Carriers' inputs into a unified exclusionary design. Apple, Google, Samsung, and the three national Carriers are indisputably separate economic actors pursuing distinct interests, yet their coordination eliminated independent decision-making and deprived the

marketplace of competition in stand-alone Wi-Fi calling. Identical validation-gated outcomes across platforms tied to common carrier specs.

Sherman Act § 2 — Monopolization, Monopoly Maintenance, and Maintenance Conspiracy (Platforms)

Monopolization and Maintenance

143. Section 2 of the Sherman Act is violated when a firm with monopoly power willfully acquires or maintains that power through exclusionary conduct rather than through superior products, business acumen, or historical accident. Apple and Google together control roughly 97 percent of the U.S. smartphone operating system market—the chokepoint for access to native telephony functions such as the default dialer, push-free inbound wake, system call-log, E911 emergency hooks, and Quality of Service. By coding iOS and Android so that these native functions activate only after carrier validation, and by relegating independent providers to degraded app-mode, the Platform Provider Defendants willfully maintained their power over the only commercially viable distribution channel for mobile voice: Apple with entitlement-gated native activation; Google with carrier-privilege/IMS gating and app-mode relegation; and Samsung (OEM enforcer) with firmware/CSC ensures the restrictions persist on devices.

Exclusionary Defaults

144. Platform-level defaults and technical restraints that foreclose rivals from critical routes to market constitute exclusionary conduct under § 2. The device-level rule: **no bundle, no native calling** is encoded into operating system, API, and firmware design. It prevents rivals from competing on the merits and caused the class to pay more for bundled services.

Maintenance Conspiracy

145. Even apart from their individual maintenance conduct, Apple and Google (with Samsung

serving as OEM and firmware enforcer) align their entitlement-gated rules across platforms, producing uniform native-versus-app outcomes in accordance with carrier specifications. This coordinated preservation of monopoly power at the device layer constitutes a maintenance conspiracy actionable under § 2. Samsung's role is pleaded as enforcing the gate at the firmware level to ensure that the restriction operated uniformly across devices. The same gating logic across iOS/Android/Samsung firmware resulted in the same exclusionary outcome.

Less-Restrictive Alternatives

146. The present restraints are not the product of necessity. A neutral certification pathway for safety, E911, and lawful-access requirements would achieve all legitimate objectives without tying native access to carrier bundles. The refusal to adopt such an alternative underscores that the current restraints are willful maintenance by exclusion. Certification can confer native parity to qualified independents without compromising emergency or lawful-access functions.

Conclusion

147. In this case, the Lock is embodied in platform code—iOS carrier bundles and entitlements; Android's hasCarrierPrivileges(), CarrierConfig, and IMS binding; and Samsung's firmware allow-lists—that withhold native parity from non-validated lines. The Key consists of carrier validation inputs, including SIM and eSIM entitlements and IMS, E911, and QoS profiles, which are necessary to flip the native switch. The result is that VoIP-Pal and other independent providers are categorically blocked from the native lane. This uniform exclusion across iOS, Android, and OEM-enforced firmware constitutes willful maintenance. The Platform Provider Defendants monopolized and maintained monopoly power by embedding a carrier-validation gate into the operating systems that control native telephony, and they conspired to maintain that power by aligning those gates across platforms.

Clayton Act § 3 — Exclusive Dealing

148. Defendants' conduct also violates Section 3 of the Clayton Act, which prohibits exclusive dealing that substantially forecloses competition. Platforms and carriers together conditioned access to native privileges on bundle affiliation, thereby foreclosing stand-alone rivals across nearly the entire smartphone base. Here, conditioning native telephony on carrier bundles forecloses the entire stand-alone market. Near-total device base foreclosed at the native lane; rivals limited to degraded app-mode.

Clayton Act § 7 — Vertical Foreclosure

149. The integration of platform OS rules, OEM firmware enforcement, and carrier entitlement requirements also violates Section 7 of the Clayton Act. By combining vertically across different layers of the mobile ecosystem, Defendants have locked the native lane exclusively to carrier-validated lines and eliminated stand-alone alternatives. This is precisely what the OS–firmware–entitlement stack has accomplished: foreclosed rivals, entrenched incumbents, and eliminated any viable channel for stand-alone competition. The vertical stack OS (Apple/Google) controls together with the OEM firmware (Samsung) enforcement resulted in carrier entitlements (AT&T/Verizon/T-Mobile) causing a device-level vertical foreclosure of competition.

PLAINTIFF'S PRELIMINARY DAMAGES ASSESSMENT

Disclaimer

150. This section pleads a class-wide, Comcast-compliant damages model. It measures only the harm caused by the Lock–Key gate: (1) the bundle premium device owners paid to unlock native calling on their own phones, and (2) the lost-function value when owners refused and were stuck in app-mode. To prevent double counting, the model uses a "one phone, one pot" allocation between the Operating System (OS) and the Phone Manufacturer (OEM) (OS share together with

OEM share = 100%). Treble damages are available under Clayton Act § 4; injunctive relief under Clayton Act § 16. The figures below are illustrative and will be refined through discovery and expert testimony; this model is subject to confirmation, revision, or complete replacement following the damages expert's report.

Measure of class wide harm

151. Because the OS/firmware gate delivers native calling only when a carrier validates the line, each device-month falls into one of two outcomes tied to the same restraint:

- Overcharge: owner buys/keeps a carrier voice/text bundle to obtain native → Bundle Premium.
- Lost function: owner refuses and remains in app-mode → App-Mode Penalty (slower/missed ring/wake, missing system call-logs, weaker E911, no QoS).

Monthly Harm per phone

152. Monthly Harm=(Forced Share×Bundle Premium)+(Degraded Share×App-Mode Penalty), where Forced Share = % of device-months on a bundle; Degraded Share = 1−Forced Share. Single Damages per phone = Monthly Harm × Months in Use (sale/activation 12/31/2024). Treble Damages per phone = Single × 3 (Clayton Act § 4).

OS vs. OEM split (no double counting)

153. For each phone-month, allocate the same Monthly Harm into two buckets that sum to 100%:

- OS Damages (Platform): iOS/Android code/defaults (entitlements/IMS gating; default-dialer rules).
- OEM Damages (Manufacturer): device/firmware enforcement (boot allow-lists, dialer capture, CSC/CarrierConfig).

154. OS Share and OEM Share = 100% (grounded in technical evidence; the Court may select a supported point in range).

Assignments (illustrative)

- Apple iPhone: OS (Apple iOS) and OEM (iPhone firmware/hardware)
- Samsung Galaxy: OS (Google Android) and OEM (Samsung firmware)
- Google Pixel: OS (Google Android) and OEM (Pixel firmware/hardware)

155. Per-bucket computations per phone-month:

- OS bucket = Monthly Harm × OS Share
- OEM bucket = Monthly Harm × OEM Share

156. Roll up by Months in Use × Phones Sold for each OEM×Year cohort (2018–2024); compute OS and OEM single & treble damages; sum across all cohorts.

Worked examples (illustrative)

157. Example 1 — Apple iPhone (single cohort ≈ $13.32B single):

- Cohort: 10,000,000 iPhones (2020) • Months in use to 12/31/2024: 60
- Bundle Premium: $24/mo • App-Mode Penalty: $9/mo
- Forced Share: 88% • Degraded Share: 12%
- OS Share (iOS): 60% • OEM Share (iPhone): 40%

Monthly Harm = 0.88×24 + 0.12×9 = $22.20

Single per phone = 60 × 22.20 = $1,332.00

Cohort Single = 10,000,000 × 1,332.00 = $13.32B

Cohort Treble = $39.96B

Split (single): OS $7.992B; OEM $5.328B

Split (treble): OS $23.976B; OEM $15.984B

158. Example 2 — Samsung Android (Galaxy) (single cohort ≈ $7.58B single):

- Cohort: 8,000,000 Galaxy (2020) • Months in use: 60
- Bundle Premium: $18/mo • App-Mode Penalty: $7/mo
- Forced Share: 80% • Degraded Share: 20%
- OS Share (Android): 65% • OEM Share (Samsung): 35%

Monthly Harm = 0.80×18 + 0.20×7 = $15.80

Single per phone = 60 × 15.80 = $948.00

Cohort Single = 8,000,000 × 948.00 = $7.58B

Cohort Treble = $22.75B

Split (single): OS $4.93B; OEM $2.65B

Split (treble): OS $14.79B; OEM $7.96B

159. Example 3 — Google Pixel (single cohort ≈ $1.99B single):

- Cohort: 3,000,000 Pixels (2021) • Months in use: 48
- Bundle Premium: $16/mo • App-Mode Penalty: $6/mo
- Forced Share: 78% • Degraded Share: 22%
- OS Share (Android): 70% • OEM Share (Pixel): 30%

Monthly Harm = 0.78×16 + 0.22×6 = $13.80

Single per phone = 48 × 13.80 = $662.40

Cohort Single = 3,000,000 × 662.40 = $1.99B

Cohort Treble = $5.96B

Split (single): OS $1.39B; OEM $0.60B

Split (treble): OS $4.17B; OEM $1.79B

Illustrative totals (examples only)

Device Cohort	Single Damages	Treble Damages
Apple iPhone (2020)	$13.32B	$39.96B
Samsung Galaxy (2020)	$7.58B	$22.75B
Google Pixel (2021)	$1.99B	$5.96B
Subtotal	$22.89B	$68.67B

OS vs. OEM (single): OS $14.31B; OEM $8.58B.

OS vs. OEM (treble): OS $42.94B; OEM $25.74B.

Full class totals (single & treble; OS & OEM) will be computed by applying the same methodology to every OEM×Year cohort (2018–2024) and summing all cohorts.

Inputs & proof

160. Phones sold/months in use (OEM 10-K/10-Q; device trackers; activation/survival curves to 12/31/2024); Bundle Premium (the native-unlock slice of bundles minus the but-for stand-alone native price; historical feasibility ≈ $6.50/line informs floor); App-Mode Penalty (monthly value for loss of native features — ring/wake, call-logs, E911, QoS — supported by surveys/telemetry); Forced vs. Degraded shares (plan-retention/adoption and usage data); OS vs. OEM shares (technical record: entitlement/IMS binding, default-dialer rules, boot allow-lists/CSC) with expert allocation; Common proof/predominance (same Lock–Key gate; identical native-vs-app outcomes

across iPhone, Samsung Android, Pixel). Comcast compliance: damages are tied strictly to the Lock–Key restraint; causation and allocation are split cleanly between OS and OEM without double counting.

No duplication / netting

161. One phone, one pot. The same Monthly Harm is split once into OS and OEM buckets (OS Share together with OEM Share = 100%). Carrier disgorgement (offload/lock-in) is reserved to the carrier dockets. Any platform-side monetary relief overlapping other proceedings will be netted to avoid duplication.

Specific Performance And Injunctive Relief

162. To correct an inbound-call barrier, the remedy must open the inbound path and prevent its reimposition. Plaintiff accordingly seeks: Parity Injunction in the form of an order requiring certification-based, nondiscriminatory access to native telephony features—including Phone-role binding, push-free wake and ring, system call-log integration, E911 application programming interfaces and behavior, QoS prioritization, and continuity or identity features—without carrier-bundle validation, for any provider meeting the same safety, E911, and lawful-access criteria that carriers must satisfy; No Re-Lock Provision in the form of a prohibition against reinstating parity barriers through operating system releases, CarrierConfig modifications, review-guideline edits, or firmware and boot-level policies, together with requirements for published criteria, versioned specifications, change logs, and advance notice of any breaking change; and Neutral Monitoring with the appointment of a Rule 53 Technical Special Master with authority to audit parity key performance indicators—including inbound wake success rates, call-setup times, call-log parity, E911 invocation, and QoS markings—using platform telemetry, and to certify compliance.

THE COUNTS

COUNT I — SHERMAN ACT § 2 (MONOPOLIZATION AND MONOPOLY MAINTENANCE)

163. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count One. Plaintiffs bring this Count against the Platform Provider Defendants for willful monopolization and attempted monopolization in violation of Section 2 of the Sherman Act, 15 U.S.C. § 2. Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

164. Platform Provider Defendants Apple, Google, and Samsung collectively control approximately 97 percent of the smartphone operating system product market in the United States[12]. Apple (iOS), Google (Android/Pixel), Samsung (OEM firmware on Android) together comprise the platform tier controlling native access.

165. Platform Provider Defendants Apple, Google, and Samsung possess monopoly power over access to native telephony features (including main-number binding as used in Wi-Fi Calling, push-free background wake and ring, system call-log integration, E911 emergency hooks, and QoS prioritization) as evidenced by native telephony functionality that turns on only for carrier-validated lines and not for independent providers of standalone W-Fi Calling.

166. This exclusionary conduct has foreclosed rivals from accessing native telephony on virtually all smartphones in the United States. Exclusive dealing by the Platform Provider Defendants, with national carriers serving the vast majority of U.S. subscribers, created and distributed device-level functions used as chokepoints to prevent standalone Wi-Fi Calling in the

[12] https://gs.statcounter.com/os-market-share/mobile/worldwide

relevant market. Platform Locks consume Carrier Keys to foreclose native parity at scale. This conduct is not competition on the merits but synchronized device/OS gating that maintains existing monopoly power at the native-telephony chokepoint, and therefore constitutes monopoly maintenance under Sherman Act § 2.

167. Publicly accessible documents of the Platform Provider Defendants Apple, Google, and Samsung show that their operating systems, APIs, default-dialers, and firmware rules deny native parity to all non-carrier lines.

168. As a direct and proximate result of the Agreement/Conspiracy and the conduct alleged herein, Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered antitrust injury, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

169. The Platform Provider Defendants' conduct lacks legitimate procompetitive justification, or any benefits are outweighed by the anticompetitive effects.

170. Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass have been injured by reason of the Defendants' violations of Section 2 of the Sherman Act and are entitled to recover treble damages, costs of suit, and reasonable attorneys' fees pursuant to 15 U.S.C. § 15, together with injunctive relief under 15 U.S.C. § 26 to enjoin the unlawful conduct alleged herein, including but not limited to a parity injunction requiring certification-based native access without bundle validation, a no re-locking order prohibiting Defendants from reinstating barriers through future software or firmware updates, and appointment of a Special Master to monitor compliance.

COUNT II — SHERMAN ACT § 1 (TYING; HUB-AND-SPOKE RESTRAINT)

171. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in

this Count Two. Plaintiffs bring this Count against the Platform Provider Defendants for willful restraint of trade in violation of Section 1 of the Sherman Act, 15 U.S.C. § 1. Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

172. Platform Provider Defendants Apple, Google, and Samsung possess monopoly power over access to native telephony features (including main-number binding as used in Wi-Fi Calling, push-free background wake and ring, system call-log integration, E911 emergency hooks, and QoS prioritization) as evidenced by native telephony functionality that turns on only for carrier-validated lines and not for independent providers of standalone Wi-Fi Calling.

173. Publicly accessible documents of the Platform Provider Defendants Apple, Google, and Samsung show that their operating systems, APIs, default-dialers, and firmware rules deny native parity to all non-carrier lines.

174. The Platform Provider Defendants Apple, Google, and Samsung entered into and engaged in an agreement, combination, and/or conspiracy (hereinafter the "Agreement/Conspiracy") [also including the Carrier Co-Conspirators] the purpose and effect of which was to unreasonably restrain trade and commerce in the relevant market in violation of Section 1 of the Sherman Act, 15 U.S.C. § 1.

175. The Agreement/Conspiracy included, without limitation, the following specific wrongful practices and terms: utilizing hub (Platform Providers) and spoke (Carriers) coordination, implemented in operating-system and firmware rules on buyer-owned devices together with carrier entitlements and profiles, an unreasonable restraint of trade on native telephony functionality that conditions access to native Wi-Fi calling on the purchase and retention of a carrier bundle, and

predatory pricing that has foreclosed rivals from accessing native telephony on virtually all smartphones in the United States.

176. The Platform Provider Defendants Apple, Google, and Samsung further entered into and engaged in the Agreement/Conspiracy the purpose and effect of which was to unreasonably restrain trade through a unified Lock–and–Key system by which the Platform Provider Defendants have conditioned access to the tying product — native Wi-Fi calling — on the purchase of a tied product, carrier bundles effecting a market-wide device-level mandate that forecloses stand-alone competition.

177. The Agreement/Conspiracy was not the result of unilateral, independent business decisions. Rather, the Agreement/Conspiracy was the product of conscious, coordinated action among the Defendants and/or co-conspirators, as shown by the unified approaches to main-number binding as used in Wi-Fi Calling, push-free background wake and ring, system call-log integration, E911 emergency hooks, QoS prioritization, and other facts alleged herein.

178. The Agreement/Conspiracy had the object and/or effect of unreasonably restraining trade by causing and resulting in, among other things: artificial, supracompetitive prices for Wi-Fi Calling in the relevant market and suppression of all competition including on price, output, and/or innovation.

179. As a direct and proximate result of the Agreement/Conspiracy and the conduct alleged herein, Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered antitrust injury, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

180. Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass have been

injured by reason of the Defendants' violations of Section 1 of the Sherman Act and is entitled to recover treble damages, costs of suit, and reasonable attorneys' fees pursuant to 15 U.S.C. § 15, together with injunctive relief under 15 U.S.C. § 26 to enjoin the unlawful conduct alleged herein.

181. The wrongful conduct of the Defendants was willful, intentional, and/or in reckless disregard of Plaintiffs' rights, making this matter exceptional and supporting an award of attorneys' fees and enhanced relief, including but not limited to a declaration that the Lock–and–Key constitutes unlawful tying and concerted restraint and a parity injunction requiring equal access to native telephony features.

COUNT III — CLAYTON ACT § 3 (EXCLUSIVE DEALING)

182. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Three. Plaintiffs bring this Count against the Platform Provider Defendants for willful monopolization and attempted monopolization in violation of Section 3 of the Clayton Act, 15 U.S.C. § 14. Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

183. The Platform Provider Defendants have conditioned access to the tying product — native Wi-Fi calling — on the purchase of a tied product, carrier bundles effecting a market-wide device-level mandate that forecloses stand-alone Wi-Fi Calling. This practice operates as de facto exclusive dealing that forecloses stand-alone rivals across nearly the entire smartphone market (the "Conditioned Sales/Exclusive Arrangement"). Customers do not consider the tied and tying products to be reasonably interchangeable because Wi-Fi Calling requires subscriber-funded devices and subscriber-funded Wi-Fi.

184. The Conditioned Sales/Exclusive Arrangement was accomplished through utilizing hub

(Platform Providers) and spoke (Carriers) coordination, implemented in operating-system and firmware rules on buyer-owned devices together with carrier entitlements and profiles that limit native telephony functionality by conditioning access to native Wi-Fi calling on the purchase and retention of a carrier bundle, which has foreclosed rivals from accessing native telephony on virtually all smartphones in the United States.

185. Plaintiff and other actual or potential competitors in the tied product market have been and continue to be injured by the Conditioned Sales/Exclusive Arrangement, including by reason of: lost sales and market opportunities; inability to achieve market entry costs and compete; and increased technical barriers to entry.

186. The Conditioned Sales/Exclusive Arrangement lacks sufficient procompetitive justification to outweigh its anticompetitive effects. Any asserted efficiencies are pretextual or could have been achieved through less restrictive means, such as non-exclusive supply agreements, warranty terms that do not condition purchases of unrelated products, or voluntary bundled discounts.

187. As a direct and proximate result of the Defendants' unlawful conditioning and exclusive dealing, Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered antitrust injury, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

188. Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass have been injured by reason of Defendants' violations of Section 3 of the Clayton Act and is entitled to recover treble damages, costs of suit, and reasonable attorneys' fees pursuant to 15 U.S.C. § 15, together with injunctive relief to prevent continuation of the illegal conditioning and exclusive dealing, including but not limited to a declaratory judgment that these exclusive-dealing practices

are unlawful and injunctive relief requiring carriers to cease conditioning native privileges on bundle affiliation.

COUNT IV — CLAYTON ACT § 7 (VERTICAL FORECLOSURE)

189. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Four. Plaintiff brings this Count against the Platform Provider Defendants for acquisitions the effect of which "may be substantially to lessen competition, or to tend to create a monopoly" in any line of commerce or section of the country in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18. Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

190. The Platform Provider Defendants entered into an agreement to combine (the "Vertical Integration") OS-level restraints imposed by Apple and Google, reinforced by Samsung's firmware enforcement and validated through carrier entitlements, pursuant to which Platform Provider Defendants created a vertical stack that locks the native lane to carrier-validated lines. Evidence of the Vertical Integration is attached hereto as Appendix B.

191. The Platform Provider Defendants' integrated conduct constitutes unlawful vertical foreclosure across platforms, devices, and carrier entitlements to combine two (or more) firms that compete in the relevant market and will result in: (a) a significant increase in concentration in the relevant market; (b) the elimination of vigorous, head-to-head competition between the parties; and (c) increased ability and incentive to engage in anticompetitive conduct, including but not limited to raising prices, reducing output, reducing service quality, degrading innovation, and increasing entry barriers.

192. The Vertical Integration has materially increased the concentration in the relevant market (e.g., as measured by the Herfindahl-Hirschman Index (HHI)). These concentration levels and the increase are presumptively likely to enhance market power and to have anticompetitive effects under Department of Justice and Federal Trade Commission merger guidelines.

193. The Vertical Integration will (or has) eliminated competition on price, service, innovation, and other dimensions. On information and belief, the parties previously competed aggressively for customers through promotional programs and product features as described in Appendix C. The Vertical Integration will (or has) removed those competitive incentives.

194. The Vertical Integration is further evidenced by the Platform Provider Defendants coordinating interaction among the Carrier Co-Conspirators (by reducing the number of effective competitors and enabling tacit coordination). The Vertical Integration creates or enhances barriers to entry and expansion in the relevant market because the unified Lock–and–Key system by which the Platform Provider Defendants have conditioned access to the tying product — native Wi-Fi calling — on the purchase of a tied product, carrier bundles, effect a market-wide device-level mandate that forecloses stand-alone competition.

195. As a direct and proximate result of the Acquisition, Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered antitrust injury, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

196. The Acquisition is likely to result in substantial and irreparable injury to competition and to Plaintiffs unless enjoined. Plaintiffs will be unable to be made whole by money damages alone because the combined firm's exercise of enhanced market power will cause long-term structural

harm to the competitive process.

197. Plaintiffs have exhausted such administrative remedies as are required (if applicable) or – alternatively – reserves the right to seek administrative relief before the appropriate enforcement authorities. Plaintiffs brings this action to enjoin the Acquisition and to obtain damages and other relief under the Clayton Act.

198. Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass have been injured by reason of Defendants' violations of Section 7 of the Clayton Act and is entitled to recover damages, injunctive relief, costs of suit, and reasonable attorneys' fees pursuant to 15 U.S.C. § 15, including but not limited to conduct relief in the form of parity injunctions and no re-locking provisions, and if such relief proves insufficient, structural remedies tailored to restore stand-alone competition.

COUNT V — RICO § 1962(C) (ENTERPRISE; PATTERN OF RACKETEERING ACTIVITY)

199. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Five. Plaintiffs bring this Count under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c). Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

200. For purposes of this Count, the "Enterprise" is an association-in-fact enterprise. The Enterprise is an ongoing organization with members and associates consisting entirely, or in part, by the Platform Provider Defendants that functions as a continuing unit for the purpose of carrying out the alleged illegal activities. The Enterprise's activities affect interstate commerce by:

- Designing/shipping/maintaining OS/firmware gating mechanisms (platforms).
- Conditioning access on bundled cellular and validation approvals (carriers).
- Transmitting uniform half-truth messaging concealing gating and bundle conditions.
- Defendants engaged in a pattern of mail and wire fraud, in violation of 18 U.S.C. §§ 1341 and 1343, as described above.

201. Alternatively (or in addition), the Enterprise consists of in part the Carrier Co-Conspirators who, by common purpose or coordination, formed an association-in-fact Enterprise to carry out the unlawful scheme described herein.

202. Defendants were associated with and employed by or participated in the affairs of the Enterprise and, through that association, conducted and participated, directly and/or indirectly, in the conduct of the Enterprise's affairs through a pattern of racketeering activity, in violation of 18 U.S.C. § 1962(c).

203. The racketeering activities (predicate acts) of the Enterprise include, but are not limited to, the repeated commission of the following offenses (each constituting a "predicate act" under 18 U.S.C. § 1961(1) and § 1962(c)): Wire fraud, 18 U.S.C. § 1343 (by use of interstate wire communications, including emails, as described in Exhibits B–D).

204. Each of the predicate acts alleged above was committed knowingly and intentionally by the Platform Provider Defendants and/or Carrier Co-Conspirators for the purpose of effectuating the Enterprise's scheme to mislead customers and monopolize the Wi-F-Calling market.

205. The predicate acts alleged above are related to one another (by common scheme, shared participants, similar methods, or the same victims) and amount to, and pose a threat of continuing criminal activity. Specifically: a. from at least 2015 through the present, b. repeated or continuous (e.g., wires, releases), c. a common purpose (to e.g., mislead subscribers and maintain unlawful

control over the Wi-Fi Calling market), demonstrating both the relationship and continuity elements of a "pattern."

206. By reason of the foregoing, the Platform Provider Defendants' conducted and participated, directly and indirectly, in the conduct of the Enterprise's affairs through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c).

207. As a direct and proximate result of the Platform Provider Defendants violation of 18 U.S.C. § 1962(c), Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered injury by reason of the racketeering activities alleged herein, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

208. Plaintiffs have incurred and will incur additional expenses as a result of the Platform Provider Defendants conduct, including attorneys' fees, investigative costs, and other litigation expenses.

209. Plaintiffs are entitled to treble damages and the recovery of costs and reasonable attorneys' fees under 18 U.S.C. § 1964(c), and requests injunctive relief under 18 U.S.C. § 1964(a) to prevent further racketeering activity by the Platform Provider Defendants and the Enterprise.

COUNT VI — RICO § 1962(D) (CONSPIRACY)

210. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Six. Plaintiffs bring this Count under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(d). Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and

the Shareholder–Consumer Subclass.

211. Beginning on or about 2015, and continuing through at least the present, the Platform Provider Defendants (and Carrier Co-Conspirators) knowingly and willfully conspired and agreed with one another to violate 18 U.S.C. § 1962 by: a. agreeing to commit and/or to cause to be committed multiple predicate acts (including, without limitation, mail fraud, 18 U.S.C. § 1341 and wire fraud, 18 U.S.C. § 1343; and b. agreeing to participate, directly or indirectly, in the conduct of the affairs of the Enterprise through a pattern of racketeering activity. The purpose and object of the conspiracy was to mislead consumers and to obtain and maintain monopoly power in the market for Wi-Fi Calling.

212. The Enterprise's hub-and-spoke structure is apparent: platforms/OEMs are the hub (entitlements/privileges/allow-lists), and carriers are the spokes (bundle conditioning and validation). Coordinated deployment across OS/firmware cycles manifests shared purpose and agreement. The predicate acts and overt acts described above were committed by the Platform Provider Defendants and co-conspirators knowingly, intentionally, and for the purpose of advancing the conspirators' common unlawful objectives.

213. The conspiracy was ongoing and posed a threat of continued racketeering activity. The predicate acts alleged were related to one another (by common participants, shared scheme, similar methods, and the same victims) and together constituted a pattern of racketeering activity under 18 U.S.C. § 1961(5).

214. As a direct and proximate result of the Platform Provider Defendants' conspiracy in violation of 18 U.S.C. § 1962(d), Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered injury by reason of the racketeering activities alleged herein, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-

Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

215. Plaintiffs have incurred and will incur additional damage and expenses as a result of the Platform Provider Defendants' unlawful conduct, including reasonable attorneys' fees and investigative costs.

216. Plaintiffs are entitled to recover treble damages, costs, and reasonable attorneys' fees under 18 U.S.C. § 1964(c), and seeks injunctive relief under 18 U.S.C. § 1964(a) to prevent further racketeering activity by the enterprise and its participants

COUNT VII — RICO § 1962(A) (USE OR INVESTMENT OF RACKETEERING INCOME)

217. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Seven. Plaintiffs bring this Count under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(a). Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

218. Beginning on or about 2015, and continuing through at least the present, the Platform Provider Defendants participated in, conducted, or otherwise engaged in the affairs of the Enterprise by using, investing, or acquiring income derived from a pattern of racketeering activity, in violation of 18 U.S.C. § 1962(a).

219. The racketeering activities (predicate acts) giving rise to the racketeer income include, without limitation, the repeated commission of the following offenses (each a predicate act under 18 U.S.C. § 1961(1)): Wire fraud, 18 U.S.C. § 1343 — by interstate wire communications identified in Exhibits B-D].

220. The Platform Provider Defendants obtained income, directly or indirectly, from the racketeering activity described above.

221. The Platform Provider Defendants used, invested, or otherwise disposed of those racketeer-derived proceeds in the conduct of the Enterprise's affairs.

222. The use and investment of racketeer income were not merely peripheral or tangential to Defendants' business; they were integral to the Enterprise's ability to continue and expand the unlawful conduct. By investing illicit proceeds into the Enterprise, the Defendants materially facilitated the Enterprise's operations and perpetuated the pattern of racketeering activity. The Platform Provider Defendants and Carrier Co-Participants used and reinvested racketeering proceeds from the "no-additional-charge" scheme to finance, expand, and enforce the OS/firmware gating infrastructure (iOS entitlements/validation; Android hasCarrierPrivileges() and CarrierConfig(); Samsung CSC/allow-lists) and to run coordinated OS-level messaging that normalized the omission. Each platform enterprise reinvested in code, tooling, or firmware to maintain the Lock.

223. The predicate acts and the investment of their proceeds were related and constituted a pattern of racketeering activity under 18 U.S.C. § 1961(5) because: a. The predicate acts were repeated and continuous (e.g., numerous mailings, repeated wire transfers, repeated fraudulent invoices), not isolated incidents; c. The predicate acts shared a common purpose and participants — to mislead subscribers and siphon proceeds into controlled entities to maintain market control over Wi-Fi Calling.

224. As a direct and proximate result of the Platform Provider Defendants' violation of 18 U.S.C. § 1962(a), Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered injury by reason of the racketeering activities alleged herein, including but not limited to: paying

for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

225. Plaintiffs have incurred and will incur additional expenses as a result of the Platform Provider Defendants' conduct, including attorneys' fees, investigative costs, and other litigation expenses.

226. Plaintiffs are entitled to treble damages and the recovery of costs and reasonable attorneys' fees under 18 U.S.C. § 1964(c), and seeks injunctive relief under 18 U.S.C. § 1964(a) to prevent further investment of racketeer income into the Enterprise.

COUNT VIII — RICO § 1962(B) (ACQUISITION OR MAINTENANCE OF CONTROL)

227. Plaintiffs repeat and reallege each and every foregoing paragraph as if fully stated here in this Count Eight. Plaintiffs bring this Count under the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(b). Plaintiffs Ray Leon, Richard Inza, and Michael Inza bring this Count on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass. Plaintiff VoIP-Pal brings this Count on behalf of the Device-Owner Class and the Shareholder–Consumer Subclass.

228. Beginning on or about 2015, and continuing through at least the present, the Defendants knowingly acquired and/or maintained, directly or indirectly, an interest in and/or control of the Enterprise by means of a pattern of racketeering activity or through the proceeds derived from such racketeering activity, in violation of 18 U.S.C. § 1962(b).

229. The racketeering activities (predicate acts) giving rise to the racketeer income and control include, without limitation, the repeated commission of the following offenses (each a predicate act under 18 U.S.C. § 1961(1)): Wire fraud, 18 U.S.C. § 1343 — by interstate wire

communications (emails, telephone calls, electronic transfers) identified in Exhibits B-D].

230. The Platform Provider Defendants derived income and proceeds from the racketeering activity described above. The Platform Provider Defendants used those racketeer-derived proceeds to acquire or maintain an interest in and/or control of the Enterprise. The acquisition and/or maintenance of the interest and control were central to the Enterprise's operations and allowed the Platform Provider Defendants to direct, influence, and profit from the Enterprise's ongoing unlawful activities. The Platform Provider Defendants control [Apple (iOS entitlement pipelines); Google (Android policy/privilege frameworks); Samsung (CSC/firmware policies)] was not merely passive or peripheral; rather, it materially frustrated competitive conditions and enabled the Enterprise to continue and expand the racketeering scheme.

231. The predicate acts and the acquisition/maintenance of control were related and constituted a pattern of racketeering activity under 18 U.S.C. § 1961(5).

232. As a direct and proximate result of the Platform Provider Defendants' violation of 18 U.S.C. § 1962(b), Plaintiffs, the Device-Owner Class, and the Shareholder–Consumer Subclass suffered injury by reason of the racketeering activities alleged herein, including but not limited to: paying for bundle premiums to unlock native calling (including Wi-Fi Calling) on their own phones or suffered functional degradation when they declined the tie and other damages in an amount to be proved at trial.

233. Plaintiffs have incurred and will incur additional expenses as a result of the Platform Provider Defendants' conduct, including attorneys' fees, investigative costs, and other litigation expenses.

234. Plaintiffs are entitled to treble damages and the recovery of costs and reasonable attorneys' fees under 18 U.S.C. § 1964(c), and seeks injunctive relief under 18 U.S.C. § 1964(a) to divest the

Defendants of illicitly acquired interests, to prevent further investment of racketeer proceeds into enterprises, and to enjoin the Defendants and their agents from exercising further control over the Enterprise.

DEMAND FOR JURY TRIAL

235. Pursuant to Rule 38 of the Federal Rules of Civil Procedure and Local Rule 38(a), Plaintiffs hereby demand a trial by jury on all issues so triable as of right by a jury.

PRAYER FOR RELIEF

236. Plaintiffs, on behalf of themselves, the Device-Owner Class, and the Shareholder–Consumer Subclass have been injured by reason respectfully request judgment in its favor and against the Defendants, jointly and severally, and pray for the following relief:

Monetary Relief (Damages)

Class Antitrust Damages (Single & Trebled): Entry of judgment for classwide single damages and treble damages under Clayton Act § 4, proved at trial using the per-phone, per-month class model for Apple iPhone, (iOS and iPhone firmware), Samsung Galaxy (Android (Galaxy and Samsung firmware), and Google Pixel (Android and Pixel firmware) devices sold in the United States from 2018–2024, together with pre- and post-judgment interest as allowed by la. Exemplar floor (three cohorts only; full period higher):

- Single damages subtotal: $22,891,200,000
  - iPhone-2020: $13,320,000,000; Galaxy-2020: $7,584,000,000; Pixel-2021: $1,987,200,000.
- Treble damages subtotal: $68,673,600,000.

Joint and Several Liability: A finding that Apple, Google, and Samsung are jointly and severally liable for the full measure of class antitrust damages to the extent permitted by law.

Non-Duplication and Netting: An order directing that any monetary recovery here be netted against recoveries in related proceedings addressing the same transactions, to avoid double counting, without limiting the Device-Owner Class's right to the full antitrust recovery available here.

Reservation of Rights: Leave to revise and supplement damages computations as discovery proceeds, including by reference to certification/entitlement logs, parity KPIs, adoption and pricing data, offload/retention impacts, and other technical or financial records.

Conduct-Based Injunctive Relief

Parity Injunction: An order requiring nondiscriminatory, certification-based inbound-native access, without bundle validation, to non-replicable telephony surfaces necessary for native operation on Apple iOS/iPhone firmware, Google Android/Pixel firmware, and Samsung Galaxy firmware, including: (a) main-number binding; (b) push-free inbound wake and ring; (c) system call-log read/write; (d) E911 and emergency hooks; (e) Quality of Service prioritization; and (f) identity/continuity features where implemented—for any qualified provider meeting the same safety, E911, and lawful-access criteria applied to carrier lines.

No Re-Locking: An injunction prohibiting re-imposition of parity-defeating restrictions through OS releases, (Apple iOS; Google Android), entitlement/CarrierConfig changes, (Google/Android; Samsung firmware), review-rule edits, or firmware/boot policies; (Samsung/Pixel/iPhone firmware); and requiring published criteria, change-management notice, telemetry, and KPIs, subject to oversight by a Rule 53 Special Master with authority to audit, require corrective measures, and resolve parity appeals.

API & Entitlement Transparency and Governance: An order requiring Defendants Apple, Google, and Samsung to publish the APIs, entitlement criteria, configuration endpoints, and objective pass/fail standards governing native access; to issue reasoned written denials; and to provide a rapid appeal process to the Special Master. Retaliation or degradation against certified providers is prohibited.

Non-Discrimination: An order prohibiting exclusive-dealing terms or technical defaults that condition native access on purchase or retention of a carrier bundle or affiliated branding.

Fees And Costs

An award of reasonable attorneys' fees, expert fees, and litigation costs pursuant to Clayton Act § 4.

Structural Relief (If Necessary)

If conduct remedies and monitorship fail to secure durable parity and compliance, entry of narrowly tailored structural relief sufficient to restore and preserve competition in native-quality Wi-Fi Calling across Apple, Google, and Samsung devices.

Retained Jurisdiction And Enforcement

An order retaining jurisdiction to supervise the parity program, enforce no-relock obligations, and oversee Special Master processes, together with authority to enforce remedial orders.

Additional Relief

Such other and further relief as the Court deems just and proper to end the device-level tie, restore competitive access to native telephony surfaces on owner devices, remedy Defendants' systematic exclusion of stand-alone native Wi-Fi Calling, and restore fair competition in mobile

telecommunications.

Respectfully submitted,

/s/ Travis Pittman

Travis Pittman (D.C. Bar No. 1016894)
Local Counsel for Plaintiff
HOLMES, PITTMAN & HARAGUCHI, LLP
1140 3rd St. NE
Washington, DC 20002
(202) 329-3558
jpittman@hphattorneys.com

Sean Parmenter
(Pro Hac Vice to be submitted)
Bar Card No. 233,144 (California)
PARMENTER INTELLECTUAL PROPERTY LAW, PLLC
1401 21st St, Suite #10724
Sacramento, CA 95811
(925) 482-6515
sean@parmenterip.com
ATTORNEYS FOR PLAINTIFFS

Filed: September 21, 2025