calltower

TECHNOLOGY WHITE PAPER

CallTower Mobile Native Dialer

Enterprise-Controlled Mobile Identity at the Point of Origination

A technical overview for telecom, security, and compliance leaders

Published by CallTower, Inc.

Executive Summary

Mobile communications have become a primary channel for enterprise business, yet most mobile business calls originate outside or are otherwise disconnected from the enterprise's communications infrastructure. The result is a structural gap in identity, policy, and compliance that downstream platforms cannot close. This paper defines enterprise mobile identity, names the specific risks that flow from its absence, compares existing approaches to the problem, and describes how CallTower's Mobile Native Dialer addresses it at the network layer rather than at the application layer. The argument is narrow by design: what CallTower delivers is not a replacement for unified communications, mobile device management, or broader off-channel controls, but a mechanism for ensuring that every business call placed from a mobile device is, from the moment of origination, a call on the enterprise's own communications infrastructure.

1. The Problem Mobile Created

For most of the history of business telephony, enterprise identity was a byproduct of infrastructure. The desk phone, the assigned extension, the PBX, and the building's wiring all pointed to the same thing: a known business user, on a known business line, on a path the enterprise controlled end to end. Identity did not have to be asserted. It was inherent in how the call originated.

Mobile dissolved that alignment. A handset carried by an employee is provisioned by a mobile network operator under a consumer or small-business account, authenticated by a SIM tied to that subscriber, and routed through the carrier's core network before it touches anything the enterprise owns. When the employee places a business call, nothing in the origination path tells the receiving system — or the enterprise's own policy, recording, and compliance systems — that this is a business communication. The call is simply a mobile call that happens to be made by someone who works for the company.

This is not a gap that downstream platforms can close. It is a gap that has to be closed at the point where the call begins.

2. Defining Enterprise Mobile Identity

Before going further, the term must be defined, because it has been used loosely across the industry.

Enterprise mobile identity, as used here, means three specific conditions established at call origination:

First, the communication is associated with a corporate DID — a business number owned and administered by the enterprise — rather than a personal mobile number assigned by a carrier to an individual.

Second, the communication is authenticated against the enterprise's UC platform as an extension of that platform, not as an outside call that happens to be placed to or from an employee.

Third, the signaling path for the call transits enterprise-controlled infrastructure before it reaches the public network, so that policy, recording, and compliance systems see the call as a native business event rather than an external one.

A solution that provides only one or two of these does not establish enterprise mobile identity. It provides a partial signal that downstream systems still have to interpret.

3. What It Costs Not to Solve This

The gap in mobile identity is not a theoretical concern. It produces specific, measurable exposure across four categories, each of which is visible in enforcement records, litigation outcomes, or operational metrics that enterprises already track.

Regulatory recordkeeping exposure. Since late 2021, the SEC and CFTC have levied billions of dollars in combined fines against broker-dealers and investment advisers for failures to preserve business communications conducted on personal devices and through off-channel means. J.P. Morgan Securities alone paid a $200 million penalty for such violations. The enforcement pattern has extended across most of the major financial institutions, and the theory of the case is consistent: if a regulated employee conducted business on a mobile channel the firm did not capture, the firm failed its recordkeeping obligation. A mobile communications model in which business calls and texts routinely originate outside the UC platform does not simply create risk — it produces the exact evidentiary gap the enforcement actions target. Firms in financial services, healthcare, and other regulated industries cannot rely on employee discretion to close it.

Litigation and e-discovery exposure. Even outside regulated industries, mobile communications conducted on personal numbers become a legal liability when litigation arises. Courts have increasingly required production of communications from personal devices when business was conducted on them, which forces custodian interviews, device imaging, and preservation obligations that are expensive, invasive, and difficult to execute cleanly. A call that originates on the enterprise's communications infrastructure is captured, retained, and producible through the same processes the enterprise already uses for email and desk-phone records. A call that originates on a personal line is none of those things.

Identity spoofing and social engineering. When executives and employees conduct business from personal mobile numbers, the enterprise has no authoritative baseline against which to detect impersonation. Any attacker can spoof a personal number. Any recipient of a business call from an unfamiliar mobile number has no reliable way to verify it. Establishing a consistent business identity on outbound mobile calls — a verifiable corporate DID rather than a personal number — removes the ambiguity that social engineering attacks exploit.

Operational blind spots. Enterprises invest heavily in tooling that depends on communications being visible to the UC platform: call analytics, CRM integration, workforce quality management, compliance monitoring, and increasingly, AI-powered conversational intelligence. Mobile calls that bypass the UC platform are invisible to all of it. The enterprise is paying for insight, it is not getting on a growing share of

its communications, and the share is growing because mobile work is growing. The tooling is not underperforming; it is starved of data.

The common structure across all four categories is the same: each risk is a consequence of business communications originating outside the enterprise's communications infrastructure. Addressing the origination point addresses all four.

4. Why the Obvious Alternatives Fall Short

Three approaches to mobile business communications are widely deployed. Each addresses part of the problem while leaving the identity question open.

UC mobile apps (Teams mobile, Webex, Zoom Phone, and similar softphone clients). These apps place business calls over the data network through an application on the device. They do establish enterprise identity when used, because the call originates inside the UC platform. The weakness is behavioral and technical: users frequently place business calls from the native dialer instead of opening the app, which defeats the identity control entirely; and VoIP over cellular data is less reliable than native voice, particularly in areas with weak data coverage, which drives users back to the native dialer. The identity model is sound in principle and leaks in practice.

Mobile device management and work-profile containers (Intune, Android Work Profile, Samsung Knox, iOS managed configurations). These separate business and personal data on the device, but they do not originate calls through enterprise infrastructure. A call placed from the work profile still leaves the device as an ordinary mobile call on the carrier's network, presenting the user's personal mobile number unless a UC app is in the path. Containerization solves the data problem; it does not solve the voice identity problem.

Native mobile integrations offered directly by UC vendors. These move closer to the right model by pairing the mobile subscription with the UC platform so the business number can ring on the native dialer. The constraint is that these offerings are typically tied to specific carrier relationships and specific geographic footprints. An enterprise with a multi-carrier environment, international users, or a mix of BYOD and corporate-liable devices often cannot standardize on a single direct offering. A unified solution requires a provider that sits between the mobile network and the UC platform and can deliver the integration across the full enterprise footprint.

That is the role CallTower Mobile Native Dialer occupies.

5. What CallTower Mobile Native Dialer Is

CallTower has operated as a cloud communications provider for enterprise UC since 2002, delivering PSTN connectivity and platform integration for Microsoft Teams (through Operator Connect and Direct Routing), Cisco Webex Calling, and Zoom Phone. CallTower Mobile Native Dialer extends that role into

mobile by establishing an enterprise-controlled path between the mobile device and the UC platform at the network layer, not the app layer.

The user's mobile device is provisioned with an enterprise eSIM issued by CallTower. The eSIM can be installed on a corporate-liable device as the primary SIM, or on a personal BYOD device as a second line alongside the user's personal SIM. After installation, the device connects to CallTower's mobile core as a VoLTE subscriber on the enterprise business line. In certain countries, this connection may utilize GSM or 2G networks.

The enterprise assigns a corporate DID to that SIM — typically a user's existing Microsoft Teams number, Webex Calling number, or another business DID already administered in the UC platform. CallTower's role as a Microsoft Teams Operator Connect provider and a Cisco Certified Mobile Calling Provider means the DID is not a parallel number layered onto the mobile; it is the same business number, provisioned onto the mobile through the same control plane the enterprise already uses for its desk phones and softphones.

From that point forward, every call placed or received on the business line transits CallTower's infrastructure, which connects directly into the UC platform via the same PSTN and session border controller relationships CallTower operates for the enterprise's fixed communications. The mobile is not an outside caller routed into the UC platform. It is an endpoint of the UC platform. The contrast with the conventional mobile model is shown in Figure 1.

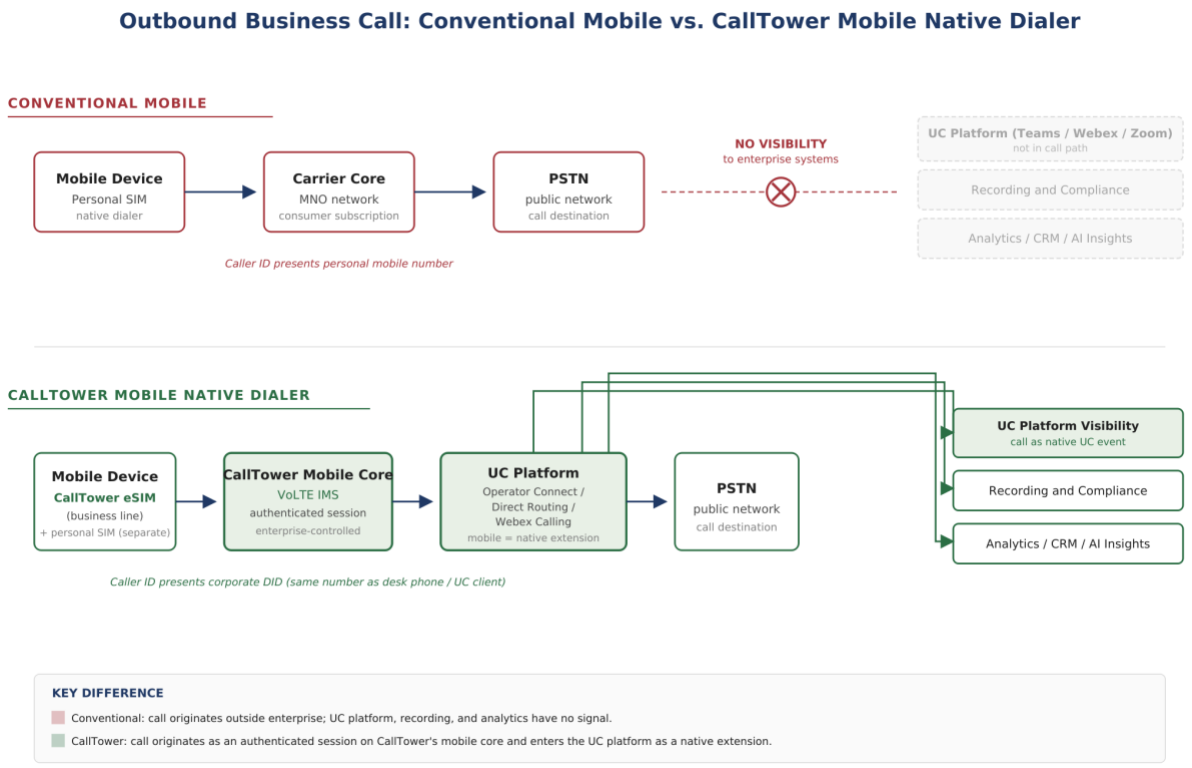

Figure 1. *Outbound business call, conventional mobile path versus CallTower Mobile Native Dialer path.*

Three implications follow from this architecture.

The call never enters the public mobile network as an anonymous consumer call. It originates as an authenticated session on a mobile core that CallTower operates under a commercial and signaling relationship with the enterprise.

Persona separation is enforced at the device level, before the network and app layer. On a BYOD device, the business eSIM and the personal SIM are two independent mobile subscriptions on the same device. The native dialer shows the user which line is active. There is no app to forget to open, and no path by which a business line call can accidentally leave the device on the personal line.

The UC platform sees the mobile as an extension. Call recording, compliance logging, presence, voicemail, call transfer, and short-code dialing work on the mobile because the UC platform is treating it exactly as it treats a desk phone. The blind spot that MDM and UC apps leave — mobile calls that occur outside the UC platform's visibility — does not exist, because there is no path for a business call to be placed outside that platform.

6. The Three Questions, Answered Mechanically

The definition in Section 2 raised three questions about what constitutes enterprise mobile identity. With the mechanism now on the table, each has a concrete answer. The identity chain that binds them is shown in Figure 2.

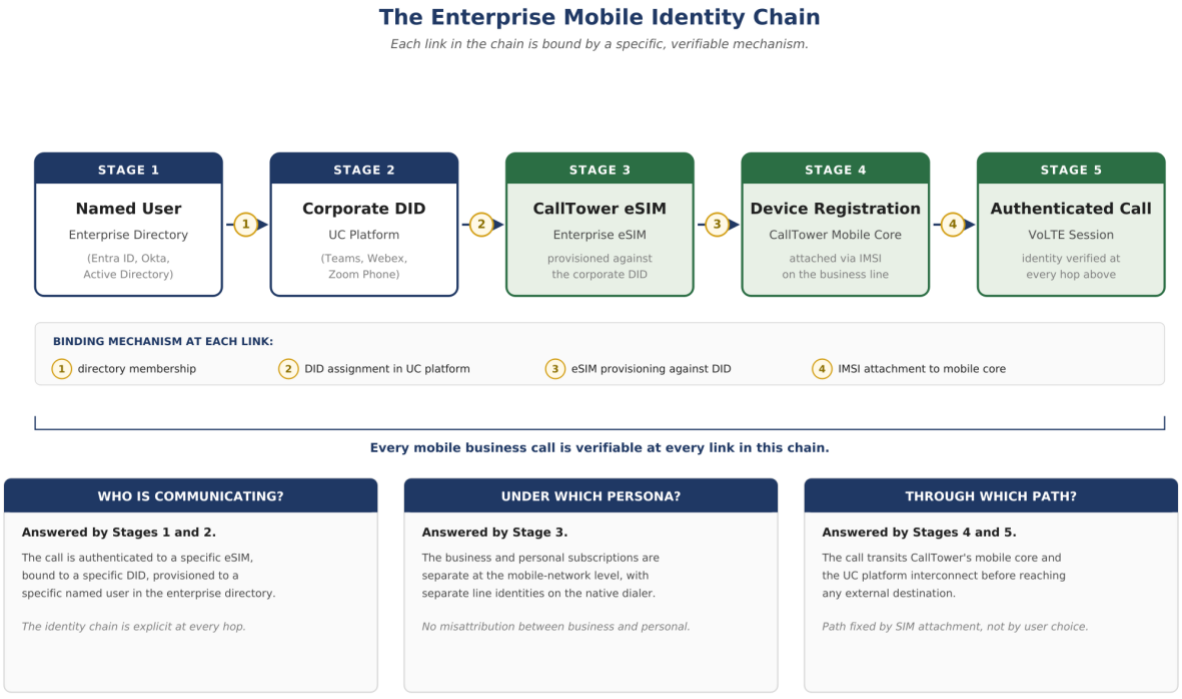

Figure 2. *The identity chain from named user to authenticated mobile session.*

Who is communicating? The call is authenticated to a specific enterprise eSIM, which is bound to a specific DID in the UC platform, which is provisioned to a specific named user in the enterprise directory. The identity chain is explicit at every hop.

Under which persona? On a BYOD device, the business and personal subscriptions are separate at the device level, with separate line identities exposed to the native dialer. The persona is determined by which line the user selects; there is no mechanism by which a call on the business line can be misattributed to the personal line or vice versa.

Through which path? The call transits CallTower's mobile core and the enterprise's existing UC platform interconnect before reaching any external destination. The path is fixed by the SIM's network attachment, not by app selection.

7. Why This Matters for Compliance and Security

The identity argument maps directly to the risks named in Section 3.

For regulated firms, every business call on a mobile becomes a call on the UC platform by construction. The same recording, retention, and supervisory controls the firm already applies to desk phones and softphones apply to the mobile without modification. The recordkeeping gap that produced the SEC enforcement actions is structurally closed, not administratively managed.

For security teams, the enterprise now has a consistent, verifiable business identity on outbound mobile calls. Zero-trust architectures and identity-based access controls gain a mobile signal they did not previously have. Impersonation attacks that rely on the absence of an authoritative business number lose their footing.

For operational tooling, the UC platform regains visibility into mobile communications. Analytics, CRM logging, quality management, and conversational AI operate on mobile calls the same way they operate on any other call the platform handles.

8. What CallTower Mobile Native Dialer Is Not

The case for the solution is stronger when it is clear about its limits.

It is not a replacement for a UC platform. It integrates with Teams, Webex, and Zoom Phone; it does not compete with them. An enterprise without a UC platform has no use for it.

It is not a mobile device management solution. It governs the communications path, not the device itself. Organizations that need to manage the device — encryption, app installation, remote wipe — still need MDM alongside.

It is not a universal answer to off-channel communications risk. Employees can still use personal messaging apps, personal email, and other channels that sit entirely outside enterprise infrastructure.

What the solution eliminates is the specific case in which a voice or SMS business communication on a mobile handset escapes enterprise visibility.

9. Conclusion

The enterprise mobile identity problem is specific: mobile calls originate in a network context the enterprise does not control, with an identity that cannot be reliably tied to enterprise systems after the fact. UC apps partially solve this but leak through user behavior. MDM solves an adjacent problem. Direct-from-vendor mobile integrations solve it within narrow carrier and geographic boundaries.

CallTower Mobile Native Dialer solves it at the network layer, by inserting CallTower's enterprise-controlled mobile core into the call path, attaching the device to that core through an enterprise eSIM, and presenting the mobile to the UC platform as a native extension using the same Operator Connect, Direct Routing, and Webex Calling integrations CallTower already provides for the fixed environment. The result is that a mobile business call is, from the moment of origination, a call on the enterprise's communications infrastructure — with the identity, policy, and compliance properties that implies.

That is a narrower claim than "mobile identity, solved." It is also a claim that can be verified, specified in an architecture diagram, and tested against a deployment. Those are the properties that make an argument worth putting to a buyer.

About CallTower

CallTower delivers Microsoft Teams, Cisco Webex Calling, Zoom Phone, and AI-driven contact center solutions, all backed by a 24/7/365 global service operation. With deep platform integrations, high-availability voice architecture, and global number management expertise, CallTower allows organizations to standardize on their collaboration tools while relying on a single partner for voice continuity worldwide. CallTower Mobile Native Dialer further extends these integrations into the mobile experience, delivering consistent enterprise calling across devices and locations.