Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	
Dismissal of Outdated or Otherwise Moot Robocalls Petitions	)	CG Docket No. 25-307

COMMENTS OF INCOMPAS

INCOMPAS
Christopher L. Shipley
Executive Director of Public Policy
1100 G Street NW, Suite 800
Washington, DC 20005
cshipley@incompas.org

January 5, 2026

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	
Dismissal of Outdated or Otherwise Moot Robocalls Petitions	)	CG Docket No. 25-307

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submit these comments in response to the Federal Communication Commission's ("Commission") *Further Notices of Proposed Rulemaking and Public Notice* ("*FNPRM*" or "*Notice*") addressing call authentication, caller identity information, Rich Call Data ("RCD"), and the origination of robocalls from outside the United States.[1]

I. INTRODUCTION AND EXECUTIVE SUMMARY

INCOMPAS, the competitive communications and Artificial Intelligence ("AI") infrastructure association, commends the Commission for taking this important step toward

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, *Dismissal of Outdated or Otherwise Moot Robocalls Petitions*, CG Docket No. 17-59, WC Docket No. 17-97, CG Docket Nos. 02-278, 25-307, Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97, Further Notice of Proposed Rulemaking in CG Docket No. 02-278, Public Notice in CG Docket No. 25-307, FCC 25-76 (rel. Oct. 29, 2025) ("*FNPRM*" or "*Notice*").

restoring consumer trust in the public switched telephone network ("PSTN") through enhanced capabilities, particularly caller identity ("caller ID") information verification through the inclusion of RCD. Consumers still lack the information they need to make informed decisions about which calls to answer. As the Commission correctly recognizes, STIR/SHAKEN has made significant progress in enhancing transparency and accountability throughout the call path, and the *Notice* appropriately seeks to build upon the STIR/SHAKEN framework's foundation to provide additional and enhanced verified caller identity information that empowers consumers while supporting legitimate business communications, leading to increased restored trust in the PSTN.

As recently noted in joint comments the association submitted with the Cloud Communications Alliance ("the Alliance") on the Triennial Assessment of the STIR/SHAKEN framework ("*STIR/SHAKEN Triennial Review*"), INCOMPAS and our members strongly support the expansion of the STIR/SHAKEN framework to include verified caller identity information through RCD.[2] But the success of any caller identity verification mandate depends on addressing legacy TDM network infrastructure that persists in the call path and adopting a flexible and competitively neutral approach.

As a threshold matter, INCOMPAS urges the Commission to prioritize universal IP interconnection and a complete transition to an IP-based PSTN. Without the Commission actively leading a transition to an all-IP PSTN and closing the persistent time-division multiplexing ("TDM") "gap" that currently strips STIR/SHAKEN authentication information

[2] *See* Joint Comments of INCOMPAS and the Cloud Communications Alliance, WC Docket No. 17-97, 6-7 (filed Nov. 18, 2025) ("INCOMPAS-Alliance Comments") (urging the Commission to support non-proprietary RCD solutions in order to better facilitate caller ID authentication and further the goals of the TRACED Act).

from approximately 61% of signed calls,[3] enhancements to caller identity verification and branding will remain incomplete and unreliable, fundamentally undermining the Commission's goals with its reopening of the record in this proceeding. Second, the Commission should require support for RCD based on STIR/SHAKEN while also permitting optional proprietary solutions that are fully interoperable with these standards. Providing this kind of flexibility will protect innovation and competition. Third, the Commission must ensure interoperability of call presentation solutions. Any caller identity solution, whether proprietary or standardized, must securely interoperate with STIR/SHAKEN protocols in all-IP ecosystems to ensure that authenticated information reaches consumers regardless of which providers are in the call path. Fourth, industry and the Commission must work in concert to avoid creating false consumer expectations with call presentation. The Commission should preserve STIR/SHAKEN as a network-level authentication tool and use RCD for consumer-facing caller identity display, and it is critical not to conflate network authentication with caller "trustworthiness."

Finally, while INCOMPAS shares the Commission's concerns about illegal robocalls originating from outside the United States, INCOMPAS suggests that international gateway traffic should be addressed appropriately without harming legitimate communications. Any gateway solutions that mark traffic as internationally originated should not undermine receipt of legitimate calls or result in disproportionate blocking of lawful international traffic. To tackle the problem of foreign originated illegal robocalls, the Commission should focus on encouraging the adoption of STIR/SHAKEN in other countries and implementation of cross-border frameworks, like the Cross Border Call Authentication ("CBCA") framework,[4] for tracebacks and trusted

[3] *See* INCOMPAS-Alliance Comments at 3.

[4] *See* Alliance for Telecommunications Industry Solutions *Ex Parte* Notice, WC Docket No. 17-97 (filed July 12, 2025).

calling at the network level, regardless of country of origin. Such proposals will address the Commission's security concerns while preserving legitimate international business communications and avoiding fee-based verification schemes that would impose unnecessary and likely discriminatory costs on service providers.

These principles are essential to achieving the Commission's goal of empowering consumers while maintaining the competitive and innovative global communications services market. Members of INCOMPAS stand ready to work with the Commission to implement the future of caller identity information transmission in a way that serves American consumers, legitimate U.S. businesses, and the competitive communications marketplace.

II. IP INTERCONNECTION IS A PREREQUISITE FOR EFFECTIVE CALL PRESENTATION

The *FNPRM* quite correctly concludes that current call presentation solutions today are not safe and effective. However, the *FNPRM* fails to adequately highlight the fact that the persistent presence of legacy TDM interconnection undermines STIR/SHAKEN's effectiveness by stripping IP-based authentication information from calls, effectively breaking the end-to-end authentication that the STIR/SHAKEN framework is designed to provide. IP networks are necessary infrastructure for STIR/SHAKEN, RCD, and future presentation and authentication capabilities. INCOMPAS welcomes the Commission's efforts to address the lack of end-to-end IP interconnection[5] and supports an affirmative mandate for such interconnection for numbered voice services. As explained further below, any effort to incorporate caller identity information

(filed July 12, 2025) ("The CBCA initiative, a collaborative effort between ATIS, iconectiv, and its founding members, will allow calls to be verified end-to-end, even if they originate in a country that has not yet deployed SHAKEN.").

[5] *See Advancing IP Interconnection, Accelerating Network Modernization, Call Authentication Trust Anchor*, WC Docket Nos. 25-304, 25-208, 17-97, Notice of Proposed Rulemaking, FCC 25-73 (rel. Oct. 29, 2025) ("*IP Interconnection NRPM*").

using RCD or other industry standards will ultimately be unsuccessful without a comprehensive regulatory framework, Commission oversight, and robust industry participation.

A. STIR/SHAKEN and RCD Efficacy are Undermined by the Persistence of TDM in the PSTN.

Recent data demonstrates the severity of the problem that remaining TDM networks create for STIR/SHAKEN effectiveness. As INCOMPAS and the Alliance noted in recent joint comments on the *STIR/SHAKEN Triennial Review*, TransNexus data shows that, as of October 2025, only 38.8% of signed calls arrive at the terminating end with SHAKEN information intact.[6] This represents minimal improvement from the 24% rate observed in 2023. The obvious culprit here is the on-going presence of TDM switching equipment in the call path. This "TDM gap" has significant implications for consumers and overall trust in the PSTN. Larger carriers with end-to-end IP networks can successfully convey SHAKEN information across their networks or through interconnections with other major IP-enabled providers. But smaller providers frequently send traffic through networks that at least partially contain TDM, which ultimately "breaks" STIR/SHAKEN by dropping the authentication it provides. Specifically, just as SHAKEN authentication data is lost when calls traverse TDM networks, RCD information,

[6] *See* INCOMPAS-Alliance Comments at 3 (quoting *STIR/SHAKEN statistics from October 2025*, TRANSNEXUS (Nov. 4, 2025), *available at* https://transnexus.com/blog/2025/shaken-statistics-october/ ("This makes four consecutive months in which the percentage of signed calls at termination has hovered around 38%. *We believe that this statistic reflects calls being routed over non-IP segments in the call path*, where the SHAKEN call authentication information is lost. We suspect that perhaps some authentication providers are deliberately routing calls over non-IP call segments to launder their identity from the calls they authenticated." (emphasis added)).

which is also conveyed in SIP headers,[7] will be stripped from calls that pass through legacy TDM networks.

This persistent TDM gap that continues to "break" STIR/SHAKEN means that any mandate to provide RCD-based verified caller identity information without first ensuring the transition to an IP-based PSTN is complete will be similarly incomplete and fall short of its intended goal.

B. The Commission Should First Mandate Universal IP Interconnection

To ensure that STIR/SHAKEN and RCD can function as intended, the Commission should use its authority to establish a national IP interconnection policy with firm deadlines for universal IP-based call routing. Building on our advocacy in the *STIR/SHAKEN Triennial Review* proceeding and the Commission's recent *IP Interconnection NPRM*, we urge the Commission to require all voice providers to support IP-based call routing and signaling. An IP interconnection mandate for numbered voice services would ensure that call authentication data, including both STIR/SHAKEN tokens and RCD, is preserved from origination to termination—essential not only for the caller identity proposals in this proceeding but also for enabling future capabilities that will further restore trust in voice communications.

Without robust PSTN IP interconnection, the Commission's caller identity proposals will create a patchwork system where some consumers receive verified caller information while others do not—not because of choices made by their providers, but because of infrastructure

[7] *Signature-based Handling of Asserted Information Using toKENS (SHAKEN): Calling Name and Rich Call Data Handling Procedures*, ATIS-100094.2, April 30, 2025 ("This specification expands the SHAKEN framework, introducing mechanisms for authentication, verification, and transport of calling name as well as other enhanced caller identity information (e.g., images, logos) and call reason, and describes how they are handled in various call origination and termination scenarios.").

limitations beyond those providers' control. This outcome would undermine consumer trust and create competitive disparities that disadvantage providers serving markets with persistent TDM interconnection. The Commission should act now to establish clear requirements to eliminate the TDM gap that currently prevents these technologies from operating effectively.

III. RCD IMPLEMENTATION SHOULD BE INTEROPERABLE, LEVERAGE EXISTING STIR/SHAKEN INFRASTRUCTURE, AND BE VOLUNTARY FOR CALLERS

Assuming the Commission establishes universal IP interconnection, INCOMPAS supports the use of RCD to provide consumers with verified caller identity information. RCD represents a natural and necessary evolution of the STIR/SHAKEN framework that can help restore consumer trust in the PSTN while enabling legitimate businesses to identify themselves to consumers in the US and globally through interoperable standards.

A. Call Presentation Solutions Should Build on STIR/SHAKEN and Remain Rooted in Open Interoperable Technology Standards

To provide verified caller identity information to consumers, it is critical that any RCD implementation leverage existing STIR/SHAKEN infrastructure and maintains the interoperability that has made the framework successful. To accomplish this, INCOMPAS proposes that the Commission adopt a three-part framework for RCD implementation.

First, RCD data should be made available under protocols based on non-proprietary standards that are honored across the PSTN, regardless of provider. As the Commission recognizes,[8] IETF and ATIS have developed RCD standards that build directly on STIR/SHAKEN, using the same authentication and verification mechanisms that providers have already implemented. By requiring implementation of RCD based on these open standards, the

[8] *See FNPRM* at para. 12.

Commission can ensure rapid, cost-effective deployment that maintains interoperability across the voice ecosystem.

Second, the Commission should allow providers to use existing infrastructure so that all voice providers on IP networks can accept and transmit RCD. Providers have already invested heavily in STIR/SHAKEN implementation. RCD represents a natural evolution of this framework rather than a wholesale replacement, allowing providers to build on existing investments rather than starting from scratch.

Third, any proprietary solutions that may also leverage RCD and STIR/SHAKEN protocols cannot be allowed to supplant the critical fundamentals of non-discrimination and competitive neutrality of the Telecommunications Act. Authenticated caller identity information must be honored and made available on a non-discriminatory basis across the PSTN. This requirement is essential to prevent market fragmentation, barriers to entry and existence, and ultimately ensure that consumers receive verified caller identity information regardless of which providers are in the call path or which RCD-based call presentation solutions providers have chosen to implement.

B. The United States Should Lead Global STIR/SHAKEN Adoption

As an originating participant in the Secure Telephone Identity—Governance Authority ("STI-GA"), INCOMPAS and its members believe that the STIR/SHAKEN framework is a critical component in the fight against illegal robocalls. The United States has been a leader in STIR/SHAKEN implementation, with Canada and other countries following its example. The Commission should bolster continued U.S. leadership by encouraging the adoption of open standard RCD built on STIR/SHAKEN so that it can be used globally, demonstrating benefits to U.S. providers and improving calling experiences for U.S. consumers.

In this quest for continued U.S. leadership, and as cross-border authentication is becoming increasingly important as voice communications become more global, the Cross Border Call Authentication ("CBCA") organization is in the process of obtaining approval from the STI-GA to interoperate with the U.S. system. The CBCA framework includes key elements such as vetting systems for legitimacy and enforcement procedures at the network level, including traceability. Supporting cross-border RCD deployment built on cross-border authentication frameworks like CBCA will enable legitimate international calling while providing tools to combat illegal robocalls that originate overseas.

C. RCD Should Empower Callers to Voluntarily Identify Themselves

An important use case for RCD is enabling callers to transmit their identity when they choose to share it with terminating providers and called parties. This voluntary nature is critical as RCD should empower callers to identify themselves for legitimate business and personal communications while respecting privacy interests when callers have legitimate reasons to withhold identifying information. This approach recognizes that caller identity verification serves different purposes in different contexts. A business calling a customer may want to present its brand and establish trust, while an individual calling from a domestic violence shelter, however, has compelling privacy interests that must be protected. RCD's flexibility allows the framework to accommodate both scenarios.

IV. PROPRIETARY CALL BRANDING SOLUTIONS WILL FURTHER ENTRENCHMENT OF PAY-TO-PLAY INTEROPERABILITY STRUCTURES

A. The Commission Can Avoid Discriminatory Outcomes by Adopting Interoperability Requirements

The *FNPRM* discusses various proprietary call branding solutions currently in the marketplace. While INCOMPAS supports innovation and does not oppose the development of

such solutions, the Commission must ensure that proprietary approaches do not discriminate against competitive providers. Industry's past experience with centralized databases can be instructive as the Commission seeks to incorporate caller identity information into the call authentication framework. Legacy CNAM databases suffer from the structural inaccuracies that the Commission has previously identified in that they are often outdated, incomplete, and subject to manipulation. Creating a new regime of proprietary, non-interoperable caller identity solutions would repeat these mistakes while adding new problems.

The messaging industry provides a cautionary example. The Campaign Registry ("TCR") for 10-digit long code ("10DLC") enacted discriminatory and onerous terms and conditions for competitive providers, creating barriers to entry and raising compliance costs significantly for providers who lack the market power to negotiate favorable terms all while having proven relatively ineffective at preventing bad actors from taking advantage.[9] In that context, the absence of uniform standards for vetting and oversight of how those standards are implemented leads to unequal treatment and anti-competitive harms. Given the importance of caller identity information to the survival of voice services, the market cannot afford a similar situation where a few proprietary solutions become gatekeepers controlling access to caller identity verification.

B. Optional Third-Party Solutions with Mandatory Interoperability

INCOMPAS supports the optional use of third-party caller identity solutions, provided that any such solution is fully interoperable with STIR/SHAKEN protocols. This balanced approach would first permit innovation in caller identity verification while preventing market

[9] *See* INCOMPAS Notice of *Ex Parte* Communications, CG Docket Nos. 17-59, 21-402, 02-278, WC Docket No. 17-97, 1-2 (filed Mar. 10, 2023) (expressing concerns regarding the competitive implications of The Campaign Registry and 10DLC system in the mobile wireless industry and urging the Commission to extend the non-discriminatory and competitively neutral treatment it has applied in the call blocking context to voluntary text blocking).

fragmentation. Next, it would ensure that no single solution becomes a mandatory bottleneck or gatekeeper and preserve competitive markets for caller identity solutions rather than creating winner-take-all dynamics. Finally, it would protect smaller providers who may lack the resources to implement multiple proprietary solutions.

Third-party solutions must operate according to several key requirements. Providers must be able to implement caller identity verification using open standards without being required to use proprietary third-party solutions. Any solution that a provider chooses to use must also work seamlessly with the open STIR/SHAKEN framework to ensure end-to-end authentication. Critically, the framework should ensure that no single provider or solution can block or degrade caller identity information for competitive reasons. Finally, to preserve competitive neutrality and overall integrity of the PSTN, any rules adopted by the Commission should not favor particular business models or advantage incumbent providers over competitive entrants.

V. THE COMMISSION SHOULD NOT MANDATE CALLER NAME WITH A-LEVEL ATTESTATION

While INCOMPAS supports RCD as a mechanism for voluntary caller identity transmission, we strongly oppose the Commission's proposal to require terminating providers to transmit verified caller identity information whenever they transmit an indication that a call has received an A-level attestation.[10] This proposal fundamentally misunderstands the purpose and design of STIR/SHAKEN and would create dangerous false impressions about call legitimacy.

[10] *See FNPRM* at para. 9 (asserting that providers may apply an A-level attestation only "when (1) it is responsible for the origination of the call onto the IP network, (2) has a direct authentication relationship with its customer and can identify the customer, and (3) has established a verified association between its customer and the telephone number used for the call); ATIS & SIP Forum, *Joint ATIS/SIP Forum Standard—Signature-Based Handling of Asserted Information Using toKENs (SHAKEN)*, 12-13 (2022), https://access.atis.org/higherlogic/ws/public/download/67436. (ATIS-1000074v.003).

A. STIR/SHAKEN is a Network-Level Provider Tool, Not a Consumer-Facing Trust Indicator

The Commission proposes to require terminating providers to transmit verified caller name whenever they transmit an indication that a call has received A-level attestation.[11] INCOMPAS respectfully opposes this proposal because it conflates network-level authentication with consumer-facing trust indicators in ways that could mislead consumers and undermine the integrity of the STIR/SHAKEN framework. STIR/SHAKEN was designed as a network-level tool to enable tracebacks, authenticate number authorization, and support analytics. Critically, STIR/SHAKEN does not determine whether a caller is trustworthy or whether the intent of the caller is legitimate. An A-level attestation simply means the originating provider has verified that its customer has the right to use the number—it says nothing about whether that customer intends to commit fraud or violate the law.

B. Mandatory Caller Name Display Tied to A-Level Attestation Creates A False Sense of Security for Consumers and Will Undermine the Commission's Goals

Forcing A-level attestations to include verified caller name will create a false sense of security for consumers who receive these calls. In other words, it will lead consumers to believe that a fraudster with illegal intent is a trusted caller simply because the call carries an A-level attestation and displays a name. Recent data underscores this concern. As noted in the Numeracle *Ex Parte* filing cited in the *Notice*, 93.4% of robocall traffic from the most prolific robocall signers now carries A-level attestations, and 48% of illegal calls are A-attested.[12] These numbers

---

[11] *See FNPRM* at para. 30.

[12] *See* Letter from Keith Buell, General Counsel and Head of Global Public Policy, and Rebekah Johnson, Founder and Chief Executive Officer, Numeracle to Marlene Dortch, Secretary, FCC, CG Docket 17-59, WC Docket 17-97, CG Docket 02-278, CG Docket 25-307 at 2 (filed Oct. 21, 2025).

demonstrate that bad actors have learned to obtain A-level attestations for their calls, whether through fraud, identity theft, or exploiting gaps in provider vetting. Requiring caller name display with A-level attestation would give these illegal calls an unwarranted veneer of legitimacy.

Consumers who see both a checkmark indicating A-level attestation and a displayed caller name are likely to incorrectly conclude that the call is legitimate and trustworthy. This could actually increase the success rate of scam calls rather than reduce it.

C. RCD Provides the Appropriate Mechanism for Caller Identity Display

INCOMPAS supports providing verified caller identity information to consumers, but this should be accomplished through RCD rather than by mandating caller name display with A-level attestation. RCD enables transmission of comprehensive caller identity information, including name, logo, and call reason, in a framework specifically designed for consumer-facing display. Under this approach, STIR/SHAKEN remains at the network level, serving its intended purposes of enabling tracebacks, authenticating number authorization, and supporting analytics. RCD then provides the mechanism for verified caller identity display to consumers, conveying rich information that helps consumers make informed decisions. Working together, the two frameworks serve distinct purposes, avoiding the confusion and false sense of security that would result from conflating network authentication with caller trustworthiness.

This approach also provides flexibility for future evolution. As RCD standards and deployment mature, providers can enhance the caller identity information they provide without being constrained by requirements tied to A-level attestation display.

VI. CALLER IDENTITY DEFINITIONS REQUIRE FLEXIBILITY FOR LEGITIMATE BUSINESS USE CASES

The Commission proposes to define "caller identity information" as having the same meaning as "caller identification information" in existing rules, but excluding the originating telephone number, billing number, and certain other elements. INCOMPAS has serious concerns about this definition and urges the Commission to adopt a more flexible approach.

A. Specific Aspects of the Proposed Definition of "Caller Identity Information" Raise Concerns

The Commission's proposed definition of caller identity information raises several specific concerns. First, including "location" as a required element is impractical for nomadic and cloud-based VoIP services where users may place calls from anywhere with internet connectivity.[13] It also risks misleading consumers about the caller's actual physical location, particularly for mobile and cloud communications services that are inherently location-independent. Second, the Commission should avoid imposing non-uniform or caller-type-based verification regimes. Differentiating rules by caller category (i.e. government, non-profit, business, individual) would add significant complexity, invite evasion by bad actors who could falsely claim to fall into categories with lighter requirements, and provide little consumer benefit given that consumers care about whether the caller is legitimate regardless of category. A better approach is to establish uniform principles for caller identity verification, such as requiring that originating providers take reasonable steps to verify the accuracy of transmitted information,

[13] *See Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, WC Docket No. 03-211, Memorandum Opinion and Order, 19 FCC Rcd 22404 (27), para. 23 (2004) (finding "the significant costs and operational complexities associated with modifying or procuring systems to track, record and process geographic location information as a necessary aspect of the [VoIP] service would substantially reduce the benefits of using the Internet to provide the service, and potentially inhibit its deployment and continued availability to consumers").

while allowing flexibility in how providers implement those principles based on the type of caller and the nature of the relationship.

Finally, INCOMPAS urges the Commission to forgo retroactive verification obligations on existing customers. Applying new vetting or documentation requirements to legacy accounts would be operationally unmanageable for providers and economically harmful to both providers and their customers. Voice service providers have millions of existing customers whose accounts were established under previous requirements. Many of these customers signed up years ago, and the provider may have limited documentation about the customer's identity or business operations. Requiring providers to go back and re-verify all existing customers, collect new documentation, and potentially suspend service for customers who cannot provide required documentation would be extraordinarily disruptive and costly.

The Commission should apply any new caller identity verification requirements prospectively only, to new customers or customers seeking to add or modify caller identity information. Existing customers should be grandfathered under previous requirements unless they choose to participate in caller identity verification by transmitting RCD information.

B. Flexible Principles with Interoperability Requirements Should be Developed for Caller Identity Information

Rather than prescriptive caller identity definitions and verification requirements, the Commission should establish flexible principles that accommodate legitimate business needs and modern communications architectures. These principles could include:

- **Establish a General Reasonableness Standard**—Require originating providers to take reasonable steps to verify the accuracy of caller identity information they transmit, but allow flexibility in what constitutes "reasonable" based on the provider's relationship with the customer, the type of caller, the nature of the information being verified, and industry best practices.

- **Any "Vetting" Must be Aligned with Existing Industry Standards** —The ATIS RCD standard contains provisions related to vetting of RCD information. With regards to any "vetting" of RCD information, the Commission should reference this standard as an example of reasonable vetting practices and should refrain from mandating specific procedures or vendors (*e.g.*, BCID and its vendors) be used to "vet" RCD.
- **Provide Safe Harbors**—The Commission should establish safe harbors for certain types of verification that would be deemed presumptively reasonable.

C. One-Size-Fits-All Requirements Undermine Legitimate Needs for and Privacy Interests Served by Caller Identity Flexibility

INCOMPAS urges the Commission not to adopt prescriptive measures that limit flexibility in how caller identity information is defined or provided. Modern communications architectures and legitimate business practices require flexibility that rigid definitions would eliminate. Our members serve diverse customers with varied needs. A prescriptive approach that fails to account for this diversity would harm competition by advantaging providers with uniform customer bases while disadvantaging those serving customers, particularly business or enterprise customers, with more complex needs. It could also make the U.S. an outlier internationally if our requirements are incompatible with practices in other countries, which will fundamentally undermine U.S. leadership in tackling issues of global illegal robocalling.

Several common and legitimate business practices require flexibility in caller identity. Large enterprises with distributed operations and other major businesses have thousands of employees making calls on behalf of the company. The customer of record may not be the actual caller, or individual callers may share common numbers. These businesses need flexibility to present appropriate caller identity information—such as the company name rather than individual employee names—that accurately represents the calling entity while maintaining operational efficiency. Similarly, multi-location businesses, including those that operate 24/7/365 support, need flexibility to present caller identity information that accurately represents the

business regardless of which location or call center is placing the call. Furthermore, there are companies with industry-specific privacy considerations that must be considered. For example, healthcare providers often need to call patients using numbers that do not expose the doctor's personal number. Privacy considerations require flexibility to present the medical office rather than individual practitioners while complying with the Health Insurance Portability and Accountability Act and other industry-specific information privacy requirements and best practices. Consumer-facing services, such as those provided via rideshare platforms, also facilitate communications between users while protecting the privacy of both parties. These intermediate communications services need flexibility to present appropriate identity information without exposing personal details of either party to ensure consumer safety and security.

VII. INTERNATIONAL GATEWAY TRAFFIC CONSIDERATIONS

A. Balance Security Concerns with Legitimate International Calling

The Commission proposes requiring providers to identify calls originating from outside the United States and to transmit that information over the entire call path. While INCOMPAS recognizes the Commission's legitimate concern about illegal robocalls originating overseas, any requirements in this area must balance security concerns with the need to preserve legitimate international business communications. For example, U.S. businesses operate call centers outside the United States for both inbound customer service and outbound customer contact. Also, domestic companies with international operations need to communicate with U.S. customers and partners. Marking these calls as foreign-originated could inappropriately stigmatize legitimate business communications. Gateway solutions that mark traffic as internationally originated should not undermine user receipt of legitimate calls.

INCOMPAS also submits that new requirements should not inappropriately burden legitimate international personal communications. Many U.S. residents maintain close connections with family members overseas. Additionally, users of nomadic VoIP services may place calls using their U.S. numbers while traveling abroad. The Commission should exempt these calls from foreign-origination marking.

B. Cross Border Call Authentication ("CBCA") Framework

Rather than focusing primarily on marking international traffic, the Commission should encourage the adoption of STIR/SHAKEN in other countries and support implementation of cross-border frameworks for tracebacks and trusted calling at the network level. This approach addresses security and traceback concerns while preserving legitimate international business communications.

CBCA participants, including ATIS, iconnectiv, Google, Microsoft, Ring Central, and Bandwidth are actively working to establish interoperability with the U.S. STIR/SHAKEN system. As participants noted in a meeting with the Commission in July of 2025, instead of adopting broad prohibitions and limitations on calls originating from outside the U.S., the Commission should support these efforts and work with international partners to expand STIR/SHAKEN adoption globally.[14] CBCA enables end-to-end authentication for international calls while maintaining the enhanced security benefits for American consumers from foreign-originated illegal robocalls that the Commission seeks to achieve.

[14] *See* ATIS *Ex Parte* Notice at 1. Alliance for Telecommunications Industry Solutions *Ex Parte* Notice, WC Docket No. 17-97 (filed July 12, 2025).

C. Avoid Fee-Based Verification Schemes

Should the Commission insist on marking traffic as "international," in no case should this labeling result in payment schemes that assess fees on service providers to verify their traffic as legitimate and route it to its final destination. Such fee-based "verification" would create barriers to entry, disadvantage smaller providers, and ultimately function as a toll on international communications—resulting in decreased competition and possible "breaking" of the PSTN as providers see themselves forced to retreat from markets altogether due to unsustainable costs. If gateway providers or other entities should choose to offer verification services, those services should be optional rather than mandatory and no preferential treatment should be given to calls that are delivered after having gone through any such pay-for-play verification services. To put it plainly, providers acting in good faith should be able to establish the legitimacy of their international traffic through participation in standardized authentication frameworks like STIR/SHAKEN and CBCA rather than being required to pay fees to third-party verification services.

D. The Commission's Foreign Spoofing Prohibition is Overly Broad

The Commission seeks comment on whether to prohibit foreign spoofing of U.S. numbers even in cases where the caller is authorized to use the spoofed number. INCOMPAS believes this approach is overly broad and would harm legitimate business communications. Speculative assumptions about labor "reshoring" tied to foreign-origin spoofing rules are unfounded. Prohibiting foreign spoofing is highly unlikely to bring call center jobs back to the U.S., as labor outsourcing decisions are in large part driven by other considerations, such as labor economics and operational efficiencies, not exclusively by voice call numbering regulation. The

more effective approach to enhancing security is for the Commission to focus on robust authentication and traceback mechanisms that work internationally and are competitively neutral.

Moreover, many legitimate businesses have valid and positive reasons for presenting U.S. numbers for calls that originate overseas. For example, and as noted above, companies with offshore operations want to present their main U.S. contact number for customer convenience and assurance to consumers that their calls are legitimate. Rather than instituting a blanket prohibition on all foreign spoofing of U.S. numbers, the Commission should focus on ensuring that such foreign-originated calls are properly authenticated.

VIII. CONCLUSION

The Commission's proposals to enhance caller identity verification through RCD and other measures represent an important evolution of the STIR/SHAKEN framework. To succeed, however, these proposals must be implemented in ways that address foundational infrastructure gaps by requiring IP interconnection for the PSTN as a prerequisite for caller identity mandates. At the same time, the Commission must preserve competitive markets to ensure that abusive gatekeeping does not take root in the call presentation ecosystem as we've seen previously. The interoperable competitively neutral technology standards of STIR/SHAKEN and RCD standards should be advanced to avoid such outcomes. These solutions must maintain appropriate distinctions between network-level authentication (STIR/SHAKEN) and consumer-facing caller identity (RCD) to avoid creating false expectations about call legitimacy, accommodate legitimate business needs through flexible definitions and verification requirements that account for modern communications architectures, and protect international communications by balancing security concerns with the need to preserve legitimate business and personal calling.

INCOMPAS and its members stand ready to work with the Commission to implement a framework that restores consumer trust, supports legitimate businesses, and maintains vibrant competition in the communications marketplace.

Respectfully Submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
Executive Director of Public Policy
INCOMPAS
1100 G Street NW, Suite 800
Washington, DC 20005
cshipley@incompas.org

January 5, 2025