

Compliance and Enforcement Notice of Consultation CRTC 2026-132

Call for Comments: Review of the Unsolicited Telecommunications Rules

Submitted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Filed with the Secretary General of the CRTC | Public Record: 1011-NOC2026-0132

1. About M³AAWG

The Messaging, Malware and Mobile Anti-Abuse Working Group ([M³AAWG](#)) is the largest global industry organization focused on addressing online abuse across messaging, mobile, and infrastructure ecosystems. M³AAWG was founded in 2004 and brings together more than 200 member organizations spanning internet service providers, telecommunications carriers, cloud service providers, security vendors, and technology companies. Collectively, M³AAWG members handle the majority of the world's email, messaging, and voice traffic.

M³AAWG works to develop industry best practices, technical standards, and policy frameworks that reduce abuse across all communications channels. This includes sustained work on email authentication (DMARC, DKIM, SPF), robocall mitigation, STIR/SHAKEN caller authentication, SMS abuse prevention, botnet remediation, and anti-spam enforcement cooperation.

M³AAWG is a founding and active participant in the STIR/SHAKEN ecosystem and has published widely adopted best practices on robocall mitigation and call authentication. Members include major North American telecommunications carriers and service providers who are directly subject to or operationally engaged with the Canadian Unsolicited Telecommunications Rules (UTRs) framework. M³AAWG also maintains active engagement with the CRTC on anti-abuse policy.

M³AAWG submits this intervention from technical, privacy, and public policy perspectives.

2. Executive Summary

M³AAWG strongly supports the Commission's initiative to modernize the Unsolicited Telecommunications Rules (UTRs). The UTRs framework has not undergone substantive revision since 2014 and the telecommunications abuse landscape has changed materially in the intervening decade. Artificial intelligence (AI)-generated voice technologies, software-defined calling platforms, and algorithmic number targeting have fundamentally altered the tools available to bad actors. As such, the rules as currently drafted are not designed for this environment.

M³AAWG recommends the following core modifications:

- The Automatic Dialing-Announcing Device (ADAD) Rules definition should be updated to be technology-neutral and outcome-focused, capturing AI-generated voice, software-defined calling systems, and future automation technologies, regardless of the underlying mechanism.
- Disclosure requirements should mandate that recipients are informed, at the outset of the call and without any required recipient interaction, when a call is not initiated or conducted by a live human.

- Regulatory modernization should explicitly reinforce, rather than inadvertently undermine, the STIR/SHAKEN caller authentication ecosystem and related anti-abuse infrastructure.
- Personal-use exemptions for AI-driven calling technologies must be carefully scoped to prevent exploitation as a compliance “escape hatch.”
- The distinction between sequential and random dialing is a technical anachronism that should be retired in favor of outcome- and volume-based regulatory standards.
- Consent frameworks should be harmonized across voice, SMS, email, and emerging communications channels to prevent regulatory arbitrage and reduce confusion for both consumers and compliant organizations.
- Privacy-By-Design (PbD) principles should be incorporated, particularly regarding caller identity, data minimization, and the intersection of AI-generated communications with biometric and voice data privacy.
- Caller authentication alone is insufficient to mitigate modern telecommunications abuse. The Commission should preserve the ability of service providers to employ reputation systems, traffic analytics, and other risk-based mitigation tools alongside STIR/SHAKEN authentication.
- Effective enforcement increasingly depends upon timely traceback and information sharing among telecommunications providers, authentication ecosystem participants, and anti-abuse organizations. The Commission should encourage such cooperation and remove barriers to good-faith abuse reporting.
- The Commission should ensure that modernized rules address cross-border telecommunications abuse and encourage international cooperation to address accountability gaps for foreign-originated traffic entering Canadian networks.
- Regulatory obligations should increasingly follow the function of the communication rather than the underlying transport technology, recognizing the convergence of voice, messaging, AI agents, and emerging communications platforms.

3. Priority Issues and Responses to Commission Questions

3.1 ADAD Definition: AI-Generated and Software-Defined Calling (Q2)

Q2 *With today's technology and available applications, is the definition sufficient to capture software, applications, or technologies that use synthesized voices, recordings, artificial intelligence, or other methods of non-human-generated voice messages?*

The current ADAD definition, which reads as “any automatic equipment incorporating the capability of storing or producing telecommunications numbers used alone or in conjunction with other equipment to convey a pre-recorded or synthesized voice message,” was drafted in an era when robocalls required dedicated physical hardware. It is no longer adequate.

Today, a bad actor can initiate thousands of AI-generated voice calls using nothing more than a cloud API subscription, a language model, and a list of telephone numbers. The current definition’s equipment-centric framing creates a structural gap that sophisticated abusers are already exploiting. This will only widen as AI voice generation becomes cheaper and more accessible.

M³AAWG recommends replacing the current hardware-centric definition with a technology-neutral, outcome-focused standard. The Commission should regulate the function of automated,

non-human-initiated or non-human-conducted voice telecommunications rather than the mechanism by which that function is accomplished.

M3AAWG proposes a revised definition:

"ADAD" means any system, software, application, platform, or technology, including but not limited to artificial intelligence, machine learning, voice synthesis, predictive dialing, or cloud-based calling services, that initiates, conducts, or facilitates telecommunications to one or more recipients through automated means, without meaningful human intervention in the initiation and placement of each individual call, regardless of whether the voice content is pre-recorded, synthesized, generated, or otherwise delivered through automated means.

For purposes of this definition, "meaningful human intervention" should not include purely ministerial, repetitive, or mechanical actions that merely enable or trigger automated communications. The Commission should evaluate the substance of human involvement, rather than its mere presence, to ensure that trivial actions, such as approving batches of calls or initiating automatically generated communications with a single click, do not remove otherwise automated systems from the scope of the UTRs.

This definition accomplishes three objectives. First, it captures AI-generated voice calls that do not rely on "stored" recordings in the traditional sense. Second, it encompasses software-as-a-service (SaaS) calling platforms that lack a physical equipment component. Third, it is forward-compatible, meaning future voice automation technologies remain within scope without requiring further amendment.

M³AAWG also recommends that the Commission explicitly clarify that the use of a human voice actor's recorded audio, fed into an AI system for playback or synthesis at scale, does not remove a call from ADAD scope. The rules are intended to address the outcome of automated mass telecommunications. Whether a system qualifies as an ADAD should be determined by its functional capabilities and how it is used, rather than its specific technical architecture or a caller's knowledge of its internal operation. A person or organization should not avoid application of the UTRs simply because the automated functionality is provided by a third-party platform or occurs within a proprietary or "black box" system. The Commission may also wish to consider whether the volume, frequency, and pattern of telecommunications activity provide evidence that a system is operating in an automated manner. These factors may be considered alongside the system's functional capabilities when determining whether the UTRs apply, without requiring the Commission to prescribe specific numerical thresholds.

3.2 Mandatory Disclosure of AI and Automated Calling Technologies (Q10)

Q10 Should *the identification requirements be expanded to require telemarketers to tell consumers that the call is using this sort of technology (i.e., it is not a live person making the call)?*

Yes. M³AAWG strongly recommends that any caller using automated, AI-generated, or synthesized voice technology be required to disclose this fact to the recipient at the outset of the call, prior to the delivery of any substantive content and without requiring the recipient to take any action to receive that disclosure.

Where other disclosures are already required under the UTRs or other applicable requirements, such as identification of the calling party or the nature of the communication, the Commission

should ensure that disclosure obligations are presented in a clear, logical, and consistent manner. AI disclosure should complement, rather than conflict with or obscure, existing identification and consumer information requirements.

The objective should be to provide recipients with sufficient information, at the beginning of the interaction, to understand who is calling, the nature of the communication, and whether they are interacting with an automated or AI-assisted system before engaging in any substantive conversation.

In addition to improving consumer transparency, a clear disclosure requirement establishes an objective compliance obligation that may simplify enforcement. Whether an AI disclosure was provided is generally easier to verify than assessing the caller's underlying intent or the technical operation of a communications platform.

This recommendation is grounded in both anti-abuse and privacy principles. From an anti-abuse standpoint, the inability of consumers to distinguish AI-generated voices from human voices is already enabling large-scale fraud, including voice impersonation of government officials, financial institutions, and family members. Mandatory disclosure is a foundational trust mechanism. From a privacy standpoint, consumers have a legitimate interest in knowing when they are interacting with an automated system, particularly when the call may involve eliciting personal information or consent.

The disclosure requirement should meet the following standards:

- Occur at the beginning of the call, before any solicitation or information collection.
- Be delivered without requiring any key press, voice prompt, or other interaction from the recipient.
- Clearly identify the nature of the calling technology (e.g., "This call is being made using an automated or AI-generated system.").
- Apply regardless of whether the automated system delivers a one-way message or is capable of conducting an interactive, two-way conversation.

M³AAWG further recommends that, where an AI system is capable of conducting extended or highly interactive conversations, the Commission considers whether additional disclosure requirements are appropriate. For example, periodic reminders that a recipient is interacting with an automated system may be appropriate when the nature or duration of the conversation could reasonably lead a recipient to believe they are interacting with a human.

This recommendation aligns with emerging international regulatory trends. Several jurisdictions are actively developing or have already enacted requirements for AI-generated communications disclosure. Modernizing the UTRs now to include this requirement positions Canada ahead of the regulatory curve, rather than behind it.

3.3 Personal-Use Exemptions for AI-Driven Calling (Q11)

Q11 Should the UTRs apply to instances where individuals initiate telecommunications strictly for personal use?

M³AAWG recognizes that certain uses of automated or AI-assisted communications by individuals may be appropriate and should not necessarily be subject to the same requirements that apply to large-scale or organizational automated communications. Examples may include an individual using

an AI assistant to schedule a medical appointment, contact a restaurant, communicate with a school, or conduct other limited personal activities.

However, the Commission should exercise caution in creating or expanding personal-use exemptions for automated or AI-driven calling technologies. The concern is not the individual consumer making a single automated appointment call. Rather, it is that broadly drafted exemptions may create opportunities for abusive actors to characterize organized or large-scale telecommunications activity as personal use to avoid compliance obligations. M³AAWG also cautions that the absence of a commercial purpose should not, by itself, qualify a communication for a personal-use exemption. Automated communications that are intended to harass, intimidate, repeatedly contact, or otherwise abuse recipients can cause substantial consumer harm regardless of whether they are undertaken for commercial gain. The Commission should therefore evaluate both the nature and the effect of the communications activity, rather than rely solely on the caller's stated motive.

In assessing whether activity exceeds the scope of legitimate personal use, the Commission should consider objective factors such as the number of recipients, the frequency and duration of the calling activity, the extent to which communications are systematic or recurring, the use of telephone numbers generated or obtained from third-party sources, and whether the activity provides a direct or indirect commercial, organizational, or financial benefit. No single factor should be determinative; rather, the overall nature and scale of the activity should guide the analysis.

M³AAWG recommends that the Commission distinguish between personal and non-personal telecommunications activity based on the purpose, scale, relationship, and economic benefit associated with the communication.

Personal-use communications generally exhibit the following characteristics:

- Initiated by an individual acting solely on their own behalf.
- Directed to a specific person or organization for a legitimate personal purpose.
- Not intended to promote commercial goods or services, generate revenue, or otherwise form part of an organized, systematic, or abusive communications campaign.
- Occurs on a limited basis and is consistent with ordinary personal activity.

Conversely, communications should generally be considered non-personal when one or more of the following factors are present:

- Promotes commercial, political, religious, advocacy, fundraising, marketing, or lead-generation activities.
- Conducted on behalf of a business, organization, campaign, association, religious institution, or other entity.
- Involves multiple recipients, systematic outreach, or repeated calling activity.
- Utilizes purchased, harvested, generated, or third-party telephone number lists.
- Results in direct or indirect economic benefit to the caller or another party.
- Forms part of an organized campaign or coordinated communications effort, regardless of whether the activity is commercial or non-commercial.

The distinction between personal and non-personal use has historically been difficult to enforce in telecommunications contexts. AI tools now allow individuals to conduct large-scale calling campaigns that may appear personal while exhibiting characteristics traditionally associated with commercial or organized telecommunications activity.

If a personal-use exemption is adopted, M³AAWG recommends the following safeguards:

- The exemption should be explicitly limited to single-recipient calls initiated for a specific, identifiable non-commercial purpose.
- It should include a volume threshold, above which the personal-use classification no longer applies regardless of stated intent.
- The exemption should not apply to calls that involve harvested, purchased, or algorithmically generated telephone number lists for the purpose of mass outreach. This limitation should not preclude authorized public safety or emergency communications, such as geographically targeted emergency notifications issued by or on behalf of authorized governmental or emergency management authorities.
- The Commission should retain authority to investigate exemption abuse and should not permit the personal-use exemption to serve as a default defense against enforcement.

M³AAWG further recommends that the Commission evaluate claims of personal use based on the totality of the circumstances, including the purpose, scale, recipient relationship, and economic benefit associated with the communications activity, rather than rely solely on the caller's characterization of the activity as personal.

3.4 Calling Chain Identification: Service Provider and Client (Q13)

Q13 Should *the requirement include both the calling service provider and the client in the identification?*

Yes, unambiguously. M³AAWG recommends that identification requirements capture both the calling service provider and the end client on whose behalf the call is made.

This mirrors the accountability model underlying STIR/SHAKEN, which requires that both the originating provider and the entity responsible for the communication be traceable through the authentication chain. Applying the same logic to consumer disclosure requirements is both consistent with the broader anti-abuse ecosystem and practically necessary for effective enforcement.

Abusive calling operations frequently rely on intermediary service providers, cloud calling platforms, and telecommunications resellers to obscure the identity of the ultimate calling party. If identification requirements capture only the client, intermediary platforms may avoid accountability. If they capture only the service provider, the entity benefiting from the calls may remain concealed. Both participants in the calling chain should therefore be identifiable through information sufficient to distinguish them from similarly named entities and to enable consumers and regulators to determine who is responsible for the communication.

M³AAWG further recommends that providers of automated or large-scale calling services implement reasonable customer verification and onboarding practices. Effective customer verification practices support accountability, improve traceback capabilities, facilitate enforcement activities, and reduce opportunities for abusive actors to exploit telecommunications platforms through anonymous or inadequately vetted accounts.

These practices are conceptually similar to “Know Your Customer” programs used in other industries, although the Commission should avoid prescribing a specific verification framework. Rather, providers should retain flexibility to implement risk-based customer verification procedures that are appropriate to the services offered and the level of abuse risk presented.

Emerging trusted communications frameworks increasingly rely on verification not only of the caller identity presented to consumers, but also the organizational identity and rights associated with the use of telephone numbers.

While the appropriate level of verification may vary based on the nature and scale of the services provided, providers should maintain sufficient information to identify customers, investigate complaints, respond to regulatory inquiries, and support traceback efforts where appropriate.

M³AAWG recommends that identification requirements include:

- The legal name or registered trade name of the entity on whose behalf the call is being made.
- The identity of the calling service provider, platform, or intermediary responsible for originating or facilitating the communication, where distinct from the client.
- Contact information sufficient to enable consumers or regulators to reach a responsible representative within a reasonable time. This may include a telephone number, website, email address, or other reliable point of contact.
- Sufficient customer information maintained by service providers to permit investigation of abusive activity, support lawful regulatory inquiries, and facilitate traceback efforts where appropriate.

For higher-risk or high-volume automated calling customers, providers should consider implementing enhanced, risk-based customer verification practices that are proportionate to the nature of the services offered and the potential abuse risks presented. Such practices may include validating organizational identity, business purpose, contact information, and the intended nature of the calling activity.

M³AAWG does not recommend that the Commission prescribe a single verification framework. Rather, providers should retain flexibility to implement reasonable, risk-based procedures appropriate to their business models and customer populations.

The Commission may also wish to consider whether providers that implement and consistently follow reasonable customer verification procedures in good faith should receive appropriate consideration when evaluating compliance efforts. Recognizing good-faith due diligence can encourage broader adoption of effective customer verification practices while acknowledging that even well-designed onboarding processes cannot eliminate all abusive activity.

These recommendations reinforce the accountability and traceability architecture established by STIR/SHAKEN by extending similar principles from the network layer to the customer and consumer disclosure layers. Improved visibility into both the service provider and the end client enhances enforcement, supports traceback efforts, and reduces opportunities for abusive actors to conceal their identity through intermediaries.

3.5 Sequential and Random Dialing: A Distinction That No Longer Serves Its Purpose (Q19)

Q19 Are *the rules regarding sequential and random dialing still necessary?*

No. M³AAWG recommends that the Commission retire the sequential versus random dialing distinction entirely.

The sequential dialing restriction was designed to address a specific 1990s-era abuse pattern: auto dialers that worked through telephone exchange prefixes in numerical order. This was detectable and addressable with a rule based on the pattern of number selection. That world no longer exists.

Modern abuse operations do not select telephone numbers sequentially or randomly in the traditional sense. They use predictive generation models, harvested consumer datasets, algorithmically curated calling lists, AI-assisted targeting based on demographic or behavioral signals, and purchased lead databases. None of these techniques is captured by rules that distinguish sequential vs. random dialing. A definition anchored to that distinction is not just outdated; it creates affirmative loopholes that sophisticated bad actors can and do exploit by demonstrating that their calling pattern was nonsequential.

M³AAWG recommends replacing this distinction with outcome-based standards that focus on:

- The volume of unsolicited calls initiated over a given time period, regardless of the number selection methodology.
- Whether the caller has obtained valid, documented consent or otherwise has a lawful basis for initiating the communication, and whether the telephone numbers were obtained through legitimate means rather than harvested, purchased for unsolicited outreach, or algorithmically generated.
- Whether the calling activity is associated with a legitimate business relationship with the recipients.

The existence of valid, documented consent should remain an important factor in assessing compliance with the UTRs. However, the method by which telephone numbers are selected or dialed should not, by itself, determine whether automated-calling technologies fall within the scope of the rules.

This approach is more durable, enforceable, and harder to circumvent than a definition that depends on the technical pattern of number selection.

3.6 Authentication and Reputation-Based Call Assessment

M³AAWG strongly supports the continued expansion of STIR/SHAKEN caller authentication. However, authentication alone does not establish that a call is trustworthy, wanted, or non-abusive.

STIR/SHAKEN verifies aspects of call origination and caller identity. It does not evaluate the content, intent, volume, or behavioral characteristics of a calling campaign. A properly authenticated call may nevertheless be fraudulent, deceptive, or unwanted. Modern abuse operations increasingly utilize legitimate service providers, authenticated calling infrastructure, and properly attested telephone numbers.

For this reason, M³AAWG recommends that the Commission explicitly recognize that caller authentication and caller trust are distinct concepts.

Service providers increasingly employ traffic analytics, reputation systems, anomaly detection, consumer complaint signals, and behavioral analysis to identify abusive calling campaigns that may otherwise satisfy technical authentication requirements. These systems have become an important component of modern anti-abuse programs.

The Commission should avoid adopting requirements that would discourage carriers from employing reasonable analytics-based mitigation measures or that would create an expectation that authenticated calls should automatically be treated as trusted calls.

M³AAWG recommends that the Commission:

- Recognize that authentication is necessary but not sufficient for consumer trust.
- Preserve the ability of carriers and service providers to employ reputation, analytics, and risk-based call assessment tools.
- Encourage the use of consumer-facing warning labels and call categorization technologies, where appropriate, to provide recipients with additional context regarding the nature or potential risk of a communication. Examples may include caller identification labels such as “Spam Risk,” “Suspected Fraud,” “Likely Telemarketing,” or other similar designations based on reasonable analytics and reputation-based assessment.
- Ensure that modernized rules do not unintentionally restrict legitimate anti-abuse mitigation practices.

Such consumer-facing indicators should complement, rather than replace, caller authentication mechanisms by providing recipients with additional information that supports informed decisions about whether to answer or trust a communication.

3.7 Telephone Number Reassignment and Consent Validity

Telephone numbers are routinely disconnected and reassigned to new subscribers. As a result, valid consent from one individual may subsequently become associated with a different person.

Modern automated and AI-assisted communications systems frequently rely upon historical customer records, previously collected consent, and long-lived contact databases. Without appropriate safeguards, these systems may direct calls or messages to individuals who have not provided consent and have no relationship with the caller.

M³AAWG recommends that the Commission recognize that consent is fundamentally associated with an individual rather than indefinitely with a telephone number.

The United States has addressed this issue through the FCC’s Reassigned Numbers Database (RND), which enables callers to determine whether a telephone number has been permanently disconnected and potentially reassigned after consent was obtained. Such mechanisms help reduce wrong-party contacts, protect consumers, and improve the accuracy of legitimate communications.

The Commission should consider encouraging reasonable measures to identify reassigned numbers, particularly for high-volume automated communications. Such measures may include periodic validation of telephone numbers, use of reassigned number databases, or other reasonable practices designed to confirm the continued validity of previously obtained consent.

M³AAWG further recommends that organizations conducting large-scale automated communications periodically review and validate consent records, particularly where the underlying consent is longstanding or there is reason to believe that a telephone number may have changed ownership.

The Commission may also wish to consider whether organizations that employ reasonable reassigned-number validation practices should receive appropriate consideration when evaluating compliance efforts. Encouraging the use of reasonable validation measures may help reduce wrong-party communications, improve consumer protection, and promote proactive compliance practices without prescribing a specific technical solution.

As AI-driven communications systems increasingly operate at greater scale and speed, maintaining accurate recipient information becomes an important component of consumer protection and abuse prevention.

The Commission may draw upon lessons from other jurisdictions that have adopted reassigned-number validation mechanisms to reduce unintended communications.

4. Privacy and Public Policy Considerations

4.1 AI Voice Technologies and the Privacy Dimension

The modernization of the UTRs presents an important opportunity to address the intersection of AI-generated communications with established privacy principles.

AI voice generation and voice-cloning technologies raise privacy concerns that extend beyond the traditional unsolicited telecommunications framework. Specifically:

- Voice biometric data. AI voice systems that interact with consumers in real time may capture, process, or retain voice recordings and voice biometric information without the consumer's knowledge or meaningful consent. The UTRs currently contain no provisions addressing the collection or use of voice data generated during automated calls.
- Consent laundering. Some AI-driven calling operations claim prior express consent based on consent obtained through channels that consumers do not associate with subsequent phone calls. The modernized framework should require that consent obtained for one communications channel not be automatically transferable to a materially different channel, particularly when that channel involves AI-generated voice communication.
- Impersonation and deepfake-enabled consumer deception. AI voice cloning and other deepfake technologies can replicate the voices of identifiable individuals with increasingly high fidelity, enabling callers to impersonate government officials, financial institutions, healthcare providers, employers, family members, or other trusted parties. Such communications are already being used in fraud campaigns to deceive consumers and facilitate financial and identity-related crimes. The modernized UTRs framework should explicitly recognize the unauthorized use of AI-generated voice technologies to impersonate identifiable individuals and ensure that AI-enabled impersonation is addressed, regardless of the underlying technology used to generate the communication.

M³AAWG recommends that the Commission consider incorporating privacy-by-design principles into the modernized UTRs framework, including the following requirements:

- Data minimization. Automated calling systems should collect and retain only the voice data, call content, and consumer-generated information reasonably necessary to fulfill the purpose of the communication; satisfy applicable legal, regulatory, contractual, or recordkeeping obligations; support legitimate audit and dispute resolution requirements; and protect against fraud or abuse. Information should not be retained longer than reasonably necessary for those purposes.

- Transparency. Where an automated system records, retains, analyzes, or otherwise uses a consumer's voice, or information derived from the consumer's voice, beyond what is reasonably necessary to conduct the immediate interaction, the caller should clearly disclose that practice at an appropriate point in the interaction. However, the Commission should seek to balance meaningful transparency with the need to avoid excessive or repetitive disclosures that diminish consumer understanding.
- Purpose limitation. Consent obtained for one communications purpose should not extend to materially different uses without fresh, informed consent.

4.2 CASL Alignment and Cross-Channel Consent Harmonization (Q3)

Q3 Should *the Commission align the definitions found in the UTRs with those in CASL?*

M³AAWG supports the principle of cross-channel definitional harmonization and encourages the Commission to pursue greater consistency between the UTRs and CASL terminology where this can be accomplished without undermining the legal integrity of either regime.

M³AAWG members operate across email, SMS, voice, and emerging communications channels simultaneously. When consent definitions, commercial activity thresholds, and opt-out requirements differ materially between the UTRs and CASL, compliant organizations bear disproportionate compliance burdens while bad actors find arbitrage opportunities between regimes.

However, the Commission's own footnote in this consultation correctly observes that the two regimes are legally distinct by design. Any harmonization effort must proceed carefully to avoid creating unintended interactions between the regimes, particularly with respect to the express consent model under CASL and the existing consent structures under the UTRs.

M³AAWG takes the following position:

- Harmonization of terminology and concepts is desirable where the underlying policy intent of both regimes is the same.
- Harmonization should not result in the less protective standard prevailing in either regime.
- Any harmonization of consent definitions should be accompanied by a clear articulation that consent obtained under one regime does not automatically satisfy the requirements of the other, absent explicit consumer authorization for multi-channel use.
- The Commission and the relevant CASL enforcement authorities should pursue ongoing coordination to ensure that modernization of either framework does not inadvertently create gaps in the other.

4.3 Voice Mail Broadcasting (Q6)

Q6 Should *Part II of the UTRs continue to apply to voice mail broadcasting, or should it be excluded?*

M³AAWG recommends that voice mail broadcasting remain subject to the UTRs and not be removed from scope.

Voice mail broadcasting, which involves the delivery of pre-recorded messages directly to voicemail without the recipient's telephone ringing, is functionally equivalent to any other automated unsolicited voice communication from the recipient's perspective. The fact that it does not cause a ring is not a meaningful distinction from a consumer protection or anti-abuse standpoint. Excluding it from the UTRs framework would create a readily exploitable loophole for operators seeking to conduct mass unsolicited voice campaigns while avoiding the rules.

M³AAWG further notes that the absence of enforcement history for voice mail broadcasting does not mean the practice is not occurring or causing consumer harm. It may reflect detection and attribution challenges rather than the absence of abuse. Removing the practice from the UTRs scope would extinguish any regulatory authority to address future abuse in this area, which M³AAWG considers unwise given the direction of voice technology development.

4.4 Fictitious Names and Accountability (Q16)

Q16 Should *the UTRs require that fictitious names may only be used when the telemarketer can determine the identity of the individual making the telecommunication?*

Yes. M³AAWG supports the Commission's proposed approach and recommends that the use of fictitious names be conditional on the ability to link that name to a specific, identifiable individual upon regulatory request.

The use of untraceable fictitious names is a well-documented tactic in abusive calling operations. Requiring traceability does not eliminate the privacy protections or reasonable business practices associated with the use of professional names, preferred names, or pseudonyms by front-line calling staff. For example, to facilitate communication, customer service representatives may legitimately use a more easily understood name when interacting with consumers. Such practices should not, by themselves, be considered deceptive. Rather, the objective is to ensure that the use of professional or alternate names cannot be used to shield responsible individuals or organizations from regulatory accountability. The individual's legal identity need not be disclosed to consumers, but it should be ascertainable by the Commission or other authorized authorities in the context of a lawful enforcement investigation.

4.5 Information Sharing, Traceback, and Collaborative Enforcement

Modern telecommunications abuse frequently involves multiple service providers, intermediaries, and jurisdictions. Effective enforcement increasingly depends upon cooperation among carriers, service providers, authentication ecosystem participants, and anti-abuse organizations.

Traceback efforts have demonstrated that collaborative investigation significantly improves the ability to identify abusive calling operations, attribute responsibility, and mitigate ongoing harm. The timely sharing of abuse indicators, complaint information, traffic patterns, and authentication data can substantially improve both industry and regulatory responses. Such information should be shared as promptly as practicable, consistent with applicable legal requirements, privacy obligations, and the operational needs of effective incident response and abuse mitigation.

M³AAWG recommends that the Commission encourage voluntary information sharing among telecommunications providers and anti-abuse stakeholders for the purpose of identifying and mitigating unlawful telecommunications activity.

The Commission should also consider whether additional protections or guidance are appropriate to support good-faith sharing of abuse indicators, traceback information, and related investigative information.

Effective anti-abuse programs increasingly rely upon collaborative approaches. No single provider typically possesses sufficient visibility to identify complex or distributed abuse operations independently.

The Commission should therefore view traceback, collaborative investigations, and information sharing as important components of the modern telecommunications enforcement ecosystem.

4.6 Cross-Channel Communications and Technology Convergence

Consumers increasingly interact with organizations through multiple communications channels, including voice, SMS, rich messaging platforms, AI agents, web-based communications interfaces, and emerging conversational technologies.

The distinctions between these channels continue to narrow. AI systems may initiate voice calls, conduct text conversations, transition between communications channels, or coordinate multi-channel campaigns that combine voice, messaging, and digital interactions.

M³AAWG recommends that the Commission adopt technology-neutral principles wherever possible. Regulatory obligations should increasingly follow the function and impact of the communication rather than the underlying transport technology.

This approach promotes consistency, reduces opportunities for regulatory arbitrage, and improves the durability of the rules as communications technologies continue to evolve.

The Commission should therefore consider the interaction of the UTRs with SMS, rich messaging services, AI agents, and future communications platforms when modernizing the framework.

5. Coordination with STIR/SHAKEN and Caller Authentication Infrastructure

M³AAWG urges the Commission to ensure that UTRs modernization is developed in explicit coordination with the STIR/SHAKEN framework and related caller authentication infrastructure. These are not separate regulatory environments. They are complementary layers of the same anti-abuse ecosystem.

STIR/SHAKEN establishes a technical chain of accountability for call origination at the network level. The UTRs establish a legal framework for the substantive content and conduct of those calls. A modernized UTRs framework that creates definitional gaps, for example, by exempting AI-generated calling systems from ADAD scope or allowing mass calling operations to claim personal-use status, would undermine the accountability architecture that STIR/SHAKEN provides by removing the regulatory consequences that give that architecture meaning.

Conversely, the UTRs modernization process presents an opportunity to strengthen the connection between technical authentication and regulatory accountability. M³AAWG recommends that the Commission consider:

- Requiring that ADAD-regulated callers operating at scale be registered with the relevant STIR/SHAKEN ecosystem stakeholders, and that their attestation level be disclosed or made accessible to carriers for call screening purposes.
- Treating calls that fail STIR/SHAKEN authentication or are originated by unregistered entities as presumptively high-risk from a UTRs enforcement standpoint, and prioritizing them for investigation.
- Ensuring that new definitions introduced through UTRs modernization, particularly any revised ADAD definition, do not create categories of calling activity that fall outside both the

UTRs framework and the STIR/SHAKEN registration requirements, thereby leaving them entirely unaccountable.

M³AAWG notes that several of our member organizations are directly involved in the technical operation of the STIR/SHAKEN ecosystem in Canada. As such, they can provide additional technical detail on this intersection in a supplemental submission, if that would assist the Commission.

5.1 International and Cross-Border Telecommunications Abuse

A significant portion of abusive telecommunications traffic originates outside the jurisdiction in which consumers receive calls. International calling providers, gateway operators, and intermediary service providers frequently participate in complex call paths that obscure the true origin of unlawful activity.

The Commission should ensure that modernization of the UTRs does not create accountability gaps for foreign-originated telecommunications traffic entering Canadian networks.

Requirements relating to identification, authentication, and accountability should apply consistently regardless of whether a call originates domestically or internationally.

M³AAWG further encourages continued cooperation among Canadian regulators, international counterparts, and relevant telecommunications anti-abuse stakeholders to address cross-border abuse operations that frequently target consumers in multiple jurisdictions simultaneously.

Modern abuse campaigns increasingly operate globally. Effective consumer protection therefore requires both domestic enforcement and international cooperation.

5.2 Emerging Trusted Calling Frameworks

M³AAWG recognizes that caller authentication technologies continue to evolve beyond traditional network-layer authentication mechanisms.

While STIR/SHAKEN provides important assurances regarding caller identity and call origination, additional industry efforts are exploring methods to provide consumers with greater confidence regarding the identity of the organization behind a communication and its authorized use of telephone numbers.

For example, emerging industry initiatives such as the GSMA's Open Verifiable Calling (OVC) project seek to enhance trust in voice communications by combining verified organizational identity, rights to use telephone numbers, and cryptographic validation mechanisms. These approaches may ultimately provide consumers with additional information regarding the identity of the calling entity and the legitimacy of the communication.

M³AAWG believes that future trusted communications frameworks may increasingly combine several elements, including:

- Network-level authentication.
- Verification of the identity of the calling organization.
- Validation of the right to use specific telephone numbers.
- Customer verification and onboarding practices.

- Consumer-facing presentation of verified identity information.

The Commission should avoid prescribing any particular technical framework. However, modernization efforts should remain sufficiently technology-neutral to accommodate future developments in trusted communications, identity verification, and caller authentication.

As AI-generated communications, voice impersonation, and cross-border calling continue to increase, flexible and interoperable trust frameworks may become an increasingly important component of consumer protection.

6. Record Keeping and Compliance Infrastructure (Q9, Q18, Q20)

M³AAWG supports the Commission's efforts to modernize and consolidate record-keeping requirements. The current framework's dispersed record-keeping obligations, spread across Parts II, III, and VI of the UTRs, create unnecessary complexity and increase the risk that compliant organizations inadvertently fail to maintain records required under one part while fully complying with another.

M³AAWG recommends the following with respect to record keeping:

- Calling records should be maintained for a reasonable period that supports effective enforcement and consumer protection. A minimum retention period of 24 months would generally satisfy these objectives.
- Record-keeping requirements should be format-neutral, allowing organizations to maintain records in any business-standard format, but should specify minimum required data elements clearly enough to prevent disputes about compliance.
- For AI-driven and automated calling systems, records should include the parameters of the automated system used (e.g., the model or platform, the calling list source, and the consent basis for each called number) in addition to call disposition data.
- Voice mail broadcasting records, if voice mail broadcasting remains within UTRs scope as M³AAWG recommends, should be subject to the same retention requirements as other ADAD records, given the potential for this channel to be used for large-scale abuse.
- Records associated with automated or AI-driven systems should include sufficient information to identify the platform, service provider, or automated technology employed, including version or system information when reasonably available.

Retained records should be maintained in a manner that reasonably supports oversight, complaint investigation, and regulatory enforcement. Providers should be capable of locating and producing relevant records within a reasonable time using commonly available identifiers, such as the called or calling telephone number; date and time of the communication, campaign or customer identifier; or other appropriate search criteria. The Commission should establish performance objectives for record accessibility without prescribing specific technical implementation requirements.

6.1 Measuring Effectiveness

The modernization of the UTRs presents an opportunity to evaluate the effectiveness of telecommunications protections through objective indicators and measurable outcomes.

M³AAWG recommends that the Commission periodically assess:

- Consumer complaint trends.
- Authentication adoption and effectiveness.
- Complaint volumes associated with AI-generated communications.
- Enforcement outcomes and compliance trends.
- The effectiveness of mitigation measures employed by service providers.

Collecting and evaluating such information can assist the Commission in identifying emerging abuse trends and determining whether additional regulatory adjustments may be warranted.

Given the rapid evolution of communications technologies, periodic assessment will help ensure that the modernized framework remains effective over time.

7. Additional Comments

7.1 Express Consent and Evolving Technology (Q15)

M³AAWG recommends that the Commission update the express consent framework to explicitly address consent obtained through digital and automated interfaces. As AI-driven interfaces become more prevalent, including AI chat agents, automated web forms, and interactive voice systems, the quality and meaningfulness of consent obtained through these channels is a legitimate question.

The Commission should consider whether consent obtained through an AI-mediated interface, particularly one that the consumer may not have recognized as automated, satisfies the express consent standard. M³AAWG takes the position that consent obtained without clear disclosure of the automated nature of the interface should be treated with heightened scrutiny and should not be presumed to constitute valid express consent for unsolicited telecommunications purposes.

7.2 Business Consumer Definition (Q1)

M³AAWG supports the adoption of a formal definition for "business consumer" but recommends that the Commission ensure the definition is not so broad as to capture organizations that receive automated calls in a consumer capacity, such as small businesses receiving unsolicited telemarketing on their primary business lines. The intent of differentiating business consumers from individual consumers should be to reflect a realistic difference in the nature of the relationship and the harm caused by unsolicited calls, not to reduce the protections available to smaller entities.

7.3 Sequential Dialing Definition (Q1)

If the Commission proceeds with formally defining "sequential dialing," M³AAWG recommends that the definition be explicitly accompanied by a statement that the rules applicable to sequential dialing apply with equal force to any other systematic or algorithmic method of generating or selecting telephone numbers for unsolicited telecommunications, regardless of the pattern of selection. A definition limited to numerically sequential patterns could be interpreted by sophisticated operators as excluding their algorithmic or AI-assisted number-selection methodologies.

7.4 Bill C-36 (Protecting Privacy and Consumer Data Act)

M³AAWG is aware that Bill C-36 is currently before Parliament and would materially alter the institutional framework for private-sector privacy enforcement in Canada. The Commission should be cognizant that several of the privacy-related obligations M³AAWG recommends incorporating into the modernized UTRs, including voice biometric transparency, consent quality for AI-mediated interfaces, and cross-channel consent harmonization, will operate within a regulatory landscape

whose institutional architecture is actively in flux. M³AAWG recommends that the Commission explicitly coordinate with the incoming Digital Safety and Data Protection Commission on any UTRs provisions with privacy implications, and that the modernized rules be drafted with sufficient flexibility to accommodate the incoming C-36 framework without requiring immediate amendment. M³AAWG further recommends that the Commission flag this intersection in its final decision and invite comment from the incoming Commission on any implementation questions that arise at the boundary of the two regimes.

7.5 Accessibility and Consumer Understanding

Disclosure obligations associated with automated and AI-generated communications should be designed to maximize consumer understanding.

Certain populations, including older adults and individuals with hearing impairments, cognitive disabilities, limited digital literacy, or limited proficiency in the language used for the communication, may face additional challenges in recognizing automated communications or understanding disclosure statements.

As automated and AI-driven communications become increasingly capable of conducting natural conversations in multiple languages, the Commission should encourage disclosure practices that are clear, understandable, and appropriate to the language in which the communication is conducted. Consumers should receive equivalent transparency regarding the use of AI regardless of the language of the interaction.

M³AAWG recommends that required disclosures be presented in clear, concise, and understandable language and delivered at the beginning of the communication before any substantive interaction occurs. Disclosure statements should be designed so that an average consumer can readily understand the identity of the caller, the nature of the communication, and whether they are interacting with an automated or AI-assisted system. The Commission should encourage plain-language disclosures that are appropriate to the language of the communication without prescribing a specific readability formula or metric.

Where automated systems engage in extended or interactive conversations, the Commission should consider whether periodic reminders of the automated nature of the interaction may further support informed consumer decision-making.

Accessible and understandable disclosures strengthen both consumer protection and trust in legitimate communications systems.

8. Conclusion

M³AAWG appreciates the Commission's commitment to modernizing the Unsolicited Telecommunications Rules and respectfully submits that the questions posed in this consultation reflect a serious and well-framed effort to address a rapidly evolving landscape. The abuse community is sophisticated, well-resourced, and quick to exploit definitional and jurisdictional gaps. The Commission has an opportunity with this modernization to close gaps before they are exploited, rather than after.

The core thread running through M³AAWG recommendations is this: the rules should be defined by outcomes, not mechanisms. The question is not what technology a caller used to reach a consumer. The question is whether that consumer received an unsolicited automated

communication without meaningful consent, disclosure, and accountability. Rules built around this principle will remain relevant and enforceable as technology continues to evolve. Rules built around specific technical mechanisms will require updating in another decade.

M³AAWG is committed to supporting the Commission's work in this area and is prepared to provide technical expertise, member perspectives, and supplemental comments on any of the issues raised in this intervention. We respectfully request party status to participate in the reply phase of this proceeding.

We appreciate the opportunity to submit feedback and welcome further engagement as needed to answer any questions during this process. Please address any inquiries to M³AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director

Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

P.O. Box 9125, Brea, CA 92822, USA

www.m3aawg.org

Filed: July 24, 2026

End of document