

ANALYSIS OF STAKEHOLDERS COMMENTS ON THE DRAFT TECHNICAL AND OPERATIONAL GUIDELINES FOR DEPLOYMENT AND ROLL OUT OF COMMERCIAL INTERNET TELEPHONY SERVICES 2026 HELD FROM FEBRUARY 17TH TO MARCH 30TH 2026

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
1.	Wilken Telecommunications	General Comment	N/A	We respectfully recommend that the guidelines also consider: -Encouraging interoperability between VoIP platforms and existing telecom infrastructure.	None	This is already covered for in the ASP and NFP license conditions. (Ref license condition No. 10 of ASP license and Condition No. 5 of NFP license)	Before provision of commercial internet telephony services, one has to obtain ASP license which provides them with rights to interconnect with other service providers	None
				-Promoting fair access to broadband infrastructure to support VoIP service providers.	None	This will be catered for in the regulations currently under development	CA is currently developing fair competition and equality of treatment regulations that will promote fair access to broadband infrastructure	None
				Ensuring clear quality-of-service (QoS) standards to guarantee reliable voice communication over IP networks.	None	This is covered in clause 6.2 and 6.3 of the proposed guideline	The proposed guidelines have identified key QoS protocols needed to sustain the required QoS	None
				-Providing guidance on security and fraud prevention measures within Internet telephony platforms.	None	This is covered in clause 6.4 and 6.5 of the proposed guideline	Ability to trace IP address, identify the IMEI number and the need to display CLI are vital parameters used in security and fraud investigations	None
2.	Paul K. Rutto	8.3	Ensure registration of Subscribers in line with the set framework governing subscriber registrations, the Kenya Information and Communications (Registration of Telecommunications	I recommend that all users assigned VoIP numbers be subject to mandatory registration (KYC requirements), similar to traditional mobile and fixed-line services.	Enhance traceability and accountability of VoIP communications Support national security and fraud prevention efforts	This is already catered for in section 8.3	Compliance with the SIM registration framework entails mandatory KYC, maintaining records, verification via IPRS	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			Service Subscribers) Regulations		Ensure compliance with existing SIM registration frameworks Reduce misuse such as spam calls, fraud, and anonymous communications Additionally, VoIP service providers should be required to: • Maintain accurate subscriber records • Integrate with national identity verification systems where applicable • Provide lawful interception capability in compliance with regulatory requirements			
		General Comment	N/A	CPaaS (Communications Platform as a Service) and Infrastructure Sharing For CPaaS providers, I recommend the Authority enforces or strongly encourages **infrastructure sharing.	This will • Reduce duplication of network resources • Lower barriers to entry for new service providers • Promote innovation and competition in	This is covered for in condition 4 of the NFP License and in the infrastructure sharing guidelines under development	-The condition requires the NFP to take into account the need for equipment co-location and/or infrastructure sharing with other licensees when setting up telecom infrastructure. -The infrastructure sharing regulations will enforce sharing and co-location	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
					the VoIP and CPaaS ecosystem Improve service quality and coverage through optimized resource utilization Infrastructure sharing should include: interconnection frameworks between CPaaS and licensed operators Access to numbering resources under regulated conditions Fair and non-discriminatory access to core telecom infrastructure			
		General Comment	N/A	Additional Considerations -Quality of Service (QoS): Define minimum standards (latency, jitter, packet loss) for VoIP services	None	This is already catered for in clause 6.3 of the proposed guidelines	The proposed guidelines have identified key QoS protocols needed to sustain the required QoS	None
				-Number Portability: Allow VoIP numbers to be portable across providers	None	Not adopted	There is currently no framework for Fixed number portability. The existing framework only caters for mobile number portability	None
				-Ensure VoIP users can access emergency numbers (e.g., 999/112)	None	This is catered for in the ASP condition no.12	Before provision of commercial internet telephony services, one has to obtain ASP license whose condition 12 requires provision	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
							of emergency services via an Authority designated Emergency number	
				Anti-Fraud Measures: Mandate STIR/SHAKEN or equivalent caller ID authentication frameworks	None	Adopted	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8: The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR /SHAKEN) authentication framework for purposes of Caller ID authentication
		General Comment	N/A	Web phone to Web phone Calls (PC-to-PC / App-to-App) The 2005 guidelines recognize PC-to-PC VoIP communication as a non-commercial, self-provisioned service not subject to licensing requirements. However, with the evolution of OTT and CPaaS platforms, I recommend: -Clarifying the regulatory position for commercial web phone/app-to-app services	These measures will help create a secure, competitive, and scalable VoIP ecosystem in Kenya while aligning with global best practices. These measures will help create a secure, competitive, and scalable VoIP ecosystem in Kenya while aligning with global best practices.	This is catered for in the proposed guidelines in Clause 4 where the applicability of these guidelines has been limited to the hybrid model of internet telephony development	The hybrid model entails calls originating from the PSTN/PLMN network and the receiving party being on the IP network or vice versa, which is subject to regulation. The other models; trunk replacement and end-to-end are not subject to regulation and not covered in these guidelines	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				-Introducing light-touch regulation where monetization or large-scale service provision is involved	None	Not adopted	Regulation provides a level playing field for all service providers irrespective of the scale of service	None
				-Ensuring such platforms comply with security and lawful interception requirements where applicable	None	This is catered for in the existing legal and regulatory framework	Issues of interception for security concerns have been provided for in the relevant security laws	None
		General Comment	N/A	WhatsApp Calls, Chats, and Group Communications (OTT / App-to-App Services) VoIP communication is increasingly established through Over-The-Top (OTT) platforms such as messaging and collaboration applications, where users make voice and video calls, send messages, and participate in group chats using smartphones or computers. This form of communication typically occurs between users over the Internet (IP-based networks) and does not require traditional telecom numbering resources. It is generally offered at no additional cost beyond Internet connectivity and access charges. This model is comparable to the PC-to-PC (or app-to-app) VoIP classification, which has historically been treated as a self-provided (DIY) service with no regulatory requirements where no commercial service is being offered. However, given the evolution of OTT platforms, I recommend the following: -Maintain a light-touch regulatory approach for non-commercial, end-user communications such as: 1. One-to-one voice/video calls 2. Messaging (chat) services 3. Group chats and group calls	None	-These guidelines are limited to the hybrid model of commercial internet telephony services -currently there is no regulatory framework for OTTs	-The hybrid model entails calls originating from the PSTN/PLMN network and the receiving party being on the IP network or vice versa, which is subject to regulation. -The other models; trunk replacement and end-to-end are not subject to regulation and not covered in these guidelines	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				WhatsApp Calls, Chats, and Group Communications (OTT / App-to-App Services) VoIP communication is increasingly established through Over-The-Top (OTT) platforms such as messaging and collaboration applications, where users make voice and video calls, send messages, and participate in group chats using smartphones or computers. This form of communication typically occurs between users over the Internet (IP-based networks) and does not require traditional telecom numbering resources. It is generally offered at no additional cost beyond Internet connectivity and access charges. This model is comparable to the PC-to-PC (or app-to-app) VoIP classification, which has historically been treated as a self-provided (DIY) service with no regulatory requirements where no commercial service is being offered.				
				However, given the evolution of OTT platforms, I recommend the following: -Maintain a light-touch regulatory approach for non-commercial, end-user communications such as: 1. One-to-one voice/video calls 2. Messaging (chat) services 3. Group chats and group calls		-data protection and security issues are catered for in the Kenya information & Communications Act (KICA) and the Data Protection Act that all entities operating within Kenya are subjected to. -data protection is also catered for in the license conditions.		

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				-Where such platforms introduce commercial elements (e.g., business APIs, CPaaS integration, monetization), they should: 1. Support lawful interception capabilities where required by law 2. Align with data protection and security frameworks	None	-currently there is no regulatory framework for OTTs These guidelines are limited to commercial internet telephony services	Matters to do with whether or not to regulate OTTs is under discussion globally	None
				-The Authority may also consider 1. Providing clear definitions distinguishing OTT communication vs licensed VoIP services 2. Monitoring large-scale platforms for consumer protection, fraud, and misuse risks	None	Not adopted	These guidelines are limited to commercial internet telephony services	None
3.	Acacia Satlink	3	Scope	• Why is the "End-to-End" IP telephony model currently excluded from regulation? Are there plans to regulate these in the future as technology evolves?	None	Matters to do with whether or not to regulate end-to-end IP telephony are under discussion globally	None	None
				- How will the Authority distinguish between "commercial" and "non-commercial" internet telephony? Clarification on where the line is drawn for small-scale or private enterprise use could be helpful	None	Commercial Internet telephony services require numbering resources from the Authority. They also need to interconnect with other ASP service providers thus requiring an ASP license	None	None
		6.1	Deployment and roll-out of Internet Telephony services shall utilise Internet Protocol (IP) version 6 and any emergent latest technologies	-Is the mandatory transition to IPv6 feasible for all current providers? -Is there a timeline for the transition, and if there are provisions for providers still using IPv4	None	The IPv6 migration strategy states July 2023 as the deadline for type approval and use of IPv4 devices in the country.	CA adopted the IPv6 migration strategy in 2022	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			riding on IPv6, both at the network and end user levels.			Service providers currently using IPv4 equipment on their network will continue using them, however for any new equipment that needs type approval and importation into the country will have to be IPv6 capable		
		6.2	To sustain the required Quality of Service, internet telephony deployment shall utilize Key QoS protocols	-Are the Quality of Service (QoS) parameters too stringent or too lenient? -Were the benchmarks derived from local network performance data?	None	The identified QoS parameters are standard as defined by International Standards setting Organizations like the ITU	The ITU is the UN specialized agency responsible for Global standardization of Telecommunication infrastructure aimed at facilitating inter-operability.	None
		6.1	Deployment and roll-out of Internet Telephony services shall utilize Internet Protocol (IP) version 6 and any emergent latest technologies riding on IPv6, both at the network and end user levels.	How should providers handle "emergent latest technologies" riding on IPv6? Please provide a specific definition to ensure future proofing	None	Service providers are encouraged to adopt IPv6 emerging technologies like IPv6+ which offers additional benefits like IPv6 segment routing, network slicing, deterministic forwarding and path associated detection.	This is to ensure service providers harness the full benefits of IPv6	none
		5.1 & 5.2	For commercial internet telephony services within the country, the applicable license is an Application Service Provider (ASP). 5.2. For termination, transit, or origination of internet telephony calls out of the country, the applicable license is International	Can a single entity hold both ASP and IGSS licenses?	None	Yes, it is possible	The Authority encourages private investment in the Telecommunication sector and provision of international transit services by persons providing telecommunication services in Kenya. This therefore allows anyone to hold multiple licenses.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			Gateway Systems and Services (IGSS).					
		6.5	All calls made via VoIP platforms must display valid Caller Line Identifiers (CLI) information for purposes of distinction between international and local commercial internet calls.	What are the specific penalties for non-compliance with Caller Line Identifier (CLI) requirements?	None	Section 9.2. requires PSTN and PLMN operators to block all calls without CLI.	This is to curb the vice of terminating international calls disguised as local calls. A licensee who contravenes the requirement for CLI will be dealt with in accordance with KICA (83A).	None
		General Comment	N/A	What is the grace period or "safe harbor" provisions for accidental technical failures?	None	Matters related to technical failures shall be handled in line with ASP license conditions.	The license conditions provide a comprehensive list of terms/conditions to be adhered to by all service providers	None
		6.4.3	From the deployment, it should be possible to: View the International Mobile Equipment Identifier (IMEI) number as registered by the network for each number in use	-What are the data protection implications for tracking IMEI and airtime top-up patterns? -How does this align with the Data Protection Act regarding subscriber privacy?	None	The capability of the system to display IMEI does not mean there is tracking, the IMEI can only be accessible by authorized persons.	This is to facilitate investigations into possible fraud/crime that may occur via internet telephony.	None.
		6.4.1	Trace the IP address of the originating call, noting that different Regional Internet Registries (RIRs) have different IP address blocks.	How will the "traceability of IP addresses" be managed across different Regional Internet Registries (RIRs)?	Since different RIRs have different IP blocks, what are the technical standards on how this cross-registry tracing should be standardized?	All IP addresses are managed by ICANN which coordinates various RIRs.	This is to facilitate investigations into possible fraud/crime that may occur via internet telephony.	None
		7.4	International internet telephony calls shall be subjected to commercial interconnect rates.	How will the "local" vs. "international" call distinction affect roaming users?	None	Local calls will be identified on the basis of using Kenyan CLI while international calls	A roaming subscriber of a commercial internet telephony service provider does not connect to the networks of foreign service providers	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
						will use non-Kenyan CLI. This does not impact on the roaming capability.		
				You might ask how these impacts roaming agreements and billing for Kenyan subscribers travelling abroad.		Noting that the calls are made over the internet, roaming agreements are not applicable.		
		10.1	These Technical and Operational Guidelines for Deployment and Roll Out of Commercial Internet Telephony Services 2025, REPEAL, the Guidelines for the Implementation and Provision of Voice over Internet Protocol (VoIP) Services published on August 12th, 2005, via Gazette Notice No. 6394.	What is the expected impact of repealing the 2005 VoIP Guidelines?	None	The 2005 guidelines will no longer be operational.	N/A	None
4.	Elige	7.1 and 7.2	7.1. A subscriber of a Kenyan internet telephony provider calling a subscriber of another telephony service provider in Kenya, irrespective of their physical location, shall be considered to be making a local call. 7.2. Local internet telephony calls shall be subjected to local interconnect rates.	With regard to the draft technical and operational guidelines for commercial internet telephony services, could the Authority please clarify what license is required to run the services described under sections 7.1 and 7.2?	None	The ASP license.	The ASP license allows a service provider to offer services such as voice, data, Internet, mobile virtual network operator, vehicle tracking services.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
5.	Wananchi group (k) limited	5	Commercial internet telephony requires ASP license; IGSS required for international traffic	The requirement introduces regulatory rigidity for operators already licensed under multiple categories within the Unified Licensing Framework (ULF), potentially duplicating licensing obligations Clarify that existing ULF licensees with ASP and international gateway capabilities are deemed compliant without additional licensing requirements	Avoids regulatory duplication, reduces compliance burden, and ensures continuity for converged operators with existing authorizations	A service provider who has an ASP license under the ULF framework is allowed to provide local internet telephony services. Further, a service provider who has an IGSS license under the ULF framework is allowed to provide international internet telephony services	The ULF market structure allows a service provider to hold multiple licenses depending on the scope of their operation.	None
		6.3	Specifies strict QoS thresholds (latency, jitter, packet loss)	While aligned with global standards, strict enforcement without transition may create operational strain, especially where services depend on interconnection with third-party networks. Introduce phased implementation and allow for reasonable exceptions where QoS degradation is attributable to third-party interconnection.	Ensures practical implementation while maintaining service quality standards; mitigates unintended service disruptions.	A service provider offering commercial internet telephony services operates under the ASP license which requires them to comply with QoS obligations as set by the authority from time to time.	The level of QoS affects the service as experienced by customers, and therefore cannot be implemented in phases.	None
		3&4	Guidelines apply primarily to hybrid VoIP models; end-to-end IP remains unregulated	Partial regulatory scope risks arbitrage where operators or users migrate to unregulated channels, undermining policy objectives. Expand regulatory framework to include oversight principles for OTT/end-to-end VoIP services, at least on a light-touch basis.	Prevents regulatory arbitrage and ensures consistency in consumer protection and security standards.	Not adopted.	Matters to do with whether or not to regulate OTTs are under discussion globally.	None.
		General Comment	N/A	Lack of clarity on transition timelines and treatment of existing deployments. Introduce clear transition period and issue implementation guidelines for existing licensees and ongoing network configurations	Provides regulatory certainty, supports orderly compliance, and minimizes	Upon operationalization of these guidelines the Authority will communicate the transition period.	To allow operators to transition to the new guidelines.	None.

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
					disruption to existing services			
6.	Jamii Telecommunications Limited	3	Scope	The scope excludes end-to-end IP telephony, creating difficulty in distinguishing between regulated VoIP services and Over-the-Top (OTT) services such as WhatsApp that operate globally without physical presence.	None	These guidelines are intended for VOIP.	Matters to do with whether or not to regulate OTTs are under discussion globally.	None
		4	Internet telephony services.	Same comments as above on OTT services. The internet telephony services models as described will be against the technology-neutral approach as provided under the Unified Licensing Framework (ULF)	None	The type of license to provide commercial internet telephony services is the ASP license in line with the ULF framework	The ASP license allows a service provider to offer services such as voice, data, Internet, mobile virtual network operator, vehicle tracking services.	None
		5	Licensing Requirements	Might be difficult to enforce against foreign-based providers. Licensing for OTT services is not clearly provided under this provision. JTL does not interconnect with any OTT party offering telephony services for VoIP traffic exchange, as this traffic does not pass through any local ISP Switching Centre/Exchange. JTL holds a unified license from the CA that covers network infrastructure, and even with its ASP License, holds no legal authority to act as a defacto regulator for services operating at a different layer of the internet stack, e.g., against Meta	None	These guidelines are not for OTTs.	Matters to do with whether or not to regulate OTTs are under discussion globally.	None
		6.1	Deployment and roll-out of Internet Telephony services shall utilize Internet Protocol (IP) version 6 and any emergent latest technologies riding on IPv6, both at	The guideline mandates IPv6 at both the network and end-user levels. This could necessitate significant re-engineering of our VoIP stack, customer-premises equipment (CPE), and changes to any upstream peering partners still running IPv4-only. It also means our subscriber devices must be IPv6-capable, creating	None	The IPv6 migration strategy states July 2023 as the deadline for type approval and use of IPv6 devices in the country. Service providers currently using IPv4	CA adopted the IPv6 migration strategy in 2022	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			the network and end user levels	a hardware/support burden for existing customers already provisioned.		equipment on their network will continue using them, however for any new equipment that needs type approval and importation into the country will have to be IPv6 capable		
		6.3.3	Latency of less than 100 milliseconds.	The 100ms latency ceiling is below the ITU G.114 recommended 150ms, it's stricter than the international standard cited in the same clause. Over mobile or congested last-mile links (especially in underserved areas), consistently meeting 100ms latency may be operationally difficult.	None	Adopted.	To align with the standard.	Latency of less than 150 milliseconds.
		6.4	deployment should trace the IP address, view airtime top-up pattern, and view the International Mobile Equipment Identifier (IMEI number as registered by the network for each number in use.	Right to privacy concerns. Kenya's Data Protection Act 2019 and the Constitution (Article 31) create significant legal friction against surveillance-style compliance mandates. Need for alignment with the Data Protection Act on lawfulness and proportionality of data collection. IMEI visibility is unusual for internet telephony; it blurs the line between mobile and VoIP regulation. IMEI is fundamentally a mobile network concept.	None	The capability of the system to display IMEI does not mean there is tracking, the IMEI can only be accessible by authorized persons.	This is to facilitate investigations into possible fraud/crime that may occur via internet telephony.	None.
		6.5, 6.6 & 6.7:	Display of valid Caller Line Identifiers (CLI), assigned numbering resources restriction on use in different countries and Possibility to demonstrate the numbers used for	Measures are too Strick especially on CLI validation Enforcement might prove difficult for international VoIP traffic.	None	Section 9.2. requires PSTN and PLMN operators to block all calls without CLI.	This is to curb the vice of terminating international calls disguised as local calls. A licensee who contravenes the requirement for CLI will be dealt with in accordance with KICA (83A).	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			termination of commercial.					
		7	Local and international commercial internet telephony calls.	Complexity in determining call origin in IP-based networks Need for clarity on commercial interconnect rate determinations to avoid any disputes that may arise.	None.	The CLI of the originating network will determine the network originating the call and the respective country.	This is to curb the vice of terminating international calls disguised as local calls.	None
		8.3	Ensure registration of Subscribers in line with the set framework governing subscriber registrations, the Kenya Information and Communications (Registration of Telecommunications Service Subscribers) Regulations.	VoIP subscribers must be registered in line with the Kenya Information and Communications Regulations, the same framework as SIM registration. This is an elevated KYC burden for VoIP, which globally tends to operate with lighter registration requirements. It could create friction in onboarding and increase compliance overhead. This will also be difficult to implement, especially for OTT services.	None	It is a requirement under KICA 27A that before a service provider offers telecommunication services proper registrations of the subscribers be undertaken.	This is to curb/deter fraud/crimes perpetuated through telecommunications network.	None
		10	Repeal of 2005 VoIP guidelines	Repeal of 2005 VoIP guidelines without transition provisions. Need to provide transition provisions to ensure proper provision during the change in the regulations and to address retrospective application of the regulations.	None	Upon operationalization of these guidelines the Authority will communicate the transition period.	To allow operators to transition to the new guidelines.	None.
7.	Nurunet	1-10	As Proposed by CA	Remains same	Guidelines foster progress	Noted	Noted	None
8.	Geonet Kenya	7.4	International internet telephony calls shall be subjected to commercial interconnect rates.	This clause is Discriminatory, contravenes Article 34(5) (a) and (b), of the Constitution of Kenya, in that this clause does not reflect the interests of all sections of the society. Kenyans in the Diaspora are still Kenyans. They need to be protected from calling rates (price) gouging like other Kenyan. Under a ULF regulatory framework, the value of content should never dictate the rate charged. The transportation or	The purpose of licensing any service is to regulate provisioning of the service(s) offered under a particular license. In other words- to license is to regulate.	-Based on the displayed CLI during call termination the displayed CLI will determine whether the call is international or local. -For Kenyans in diaspora using Kenyan lines the	This is to curb the vice of terminating international calls disguised as local calls.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				processing of IP packet within the boundaries of Kenya should be the same for local or international content- See CAMAT Judgement APPEAL NO. 3 OF 2018. Guided by this principle The Authority (CA) in Determination Number 1 of 2018 (paragraph 3.2.5.2) directed service providers to adhere to International Telecommunications Union guidelines of international rates. It is GeoNet's view that, as long as ULF remains the CA regulatory standard, and as long as Kenya is a significant to the ITU charter, then, The Authority need to be bound by ITU rules and guidelines and its own Clause 12 (1) (a), (d) and (e) of regulation- THE KENYA INFORMATION AND COMMUNICATIONS (INTERCONNECTION AND PROVISION OF FIXED LINKS, ACCESS AND FACILITIES) REGULATIONS, 2010 (hereinafter, interconnect regulation).	International Gateway Systems and Services (IGSS) is not different. Therefore, The authority has the power to fairly regulate any service under IGSS, and thus set Commercial rates within the guidelines of ITU and its own interconnect regulations, which were meant to caution callers from outside the country and especially the KENYAN DIASPORA from price gouging	displayed CLI will be Kenyan, therefore local call rates will be applicable.		
9.	Airtel Networks Kenya Ltd	6.6	Assigned numbering resources are for use in Kenya and cannot be reassigned or transferred for use in a different country.	The enforcement mechanisms for detecting offshore use of Kenyan numbers are not specified. Assigned numbering resources are for use in Kenya and cannot be reassigned or transferred for use in a different country. Registration of new customers should only be enabled in Kenya.	This will address the abuse of Kenyan MSISDNs registered and controlled outside the country. Some ASPs allow new registrations to be done outside Kenya since the only requirement is an application downloadable from iOS and Android	The enforcement measures are contained in the legal and regulatory frameworks.	These guidelines are meant to provide technical and procedural guidelines for roll-out of commercial internet telephony.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
		7.1	A subscriber of a Kenyan internet telephony provider calling a subscriber of another telephony service provider in Kenya, irrespective of their physical location, shall be considered to be making a local call.	We request for more clarity on this statement	The area of clarity revolves around the statement “irrespective of their physical location” and how it affects enforcement, security and authenticity of the users.	Noting that internet telephony transit over the internet which is global, the calling subscriber’s location does not determine whether the call is local or international.	It is the displayed CLI that will determine whether the call is local or international.	None
		9.3	Flag and report internet calls with Calling Line Identifiers suspected to be invalid or manipulated.	We propose to expand this statement to allow PSTN and PLMN providers to follow the following procedure in handling suspected SIM boxing traffic. (i) Flag (ii) Block and then (iii) Report Flag, block and report internet calls with Calling Line Identifiers suspected to be invalid or manipulated.	This will mitigate revenue losses, QoS degradation and unfair competition when SIM boxing traffic is terminated into PSTN and PLMN networks. It would have been better to flag and report suspected traffic and then wait for investigation first but sometimes SIM boxing traffic is done at night and the delay might cause more damage and its better to block, investigate and implementing the resolution after the conclusion of the investigation	Noting that this are suspected and not confirmed the service provider is required to notify CA for investigation, and only after confirmation can the calls associated with that number be blocked	This is to avoid cases of unverified blockage.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
		General – Enforcement & Compliance	Not explicitly addressed.	The Guidelines lack clear consequences for non-compliance specific to VoIP abuses. Introduce graduated enforcement measures including audits, suspension of VoIP interconnection, and license sanctions for repeat offenders.	Strengthens deterrence and ensures the Guidelines are practically enforceable	Provision of internet telephony services is done upon getting a ASP license which has terms and conditions and consequences of not adhering to the terms and conditions.	The enforcement measures are contained in the legal and regulatory frameworks. These guidelines are meant to provide technical and procedural guidelines for roll-out of commercial internet telephony.	None
10.	Safaricom PLC	2.1	Provide an understanding of internet telephony services and the distinction for internet telephony services that are amenable to regulation and the associated regulatory constraints.	Provide an understanding of internet telephony services and the distinction for internet telephony services that are amenable to regulation and the associated regulatory constraints, and <i>a clear distinction between unregulated peer-to-peer services and commercial services that interconnect with licensed Public Land Mobile Networks (PLMN).</i>	The distinction must be based on the point of interconnect. Many VoIP providers claim they are self-provisioned/unregulated until the moment they hit the PSTN/PLMN. If the distinction is blurry, a provider can claim to be an unregulated OTT service while effectively operating as a commercial carrier.	Not adopted The usage of the term regulatory constraints implies need for interconnection, need for numbering resources and charging for the calls made by the subscribers.	Section 4 of the guidelines have stated the regulatory constraints associated with internet telephony services that are regulated which fall under the hybrid model.	None
		2.2	Provide for a fair and level playing field between internet telephony service providers and other telephony service providers	Provide for a fair and level playing field between internet telephony service providers and other telephony service providers <i>ensuring that Internet Telephony providers adhere to the same KICA Subscriber Regulations, termination fee structures as traditional MNOs.</i>	We advocate for Regulatory Parity because MNO pay for IGSS License, spectrum fee, and an Interconnect Fee, then VoIP provider shouldn't be allowed to	Not adopted Provision of fair and level playing field implies that all service providers will be subject to the requirements of KICA and the associated regulatory constraints	Section 5 of the guidelines requires that a service provider offering local commercial internet telephony services within the country, the applicable license is an Application Service Provider (ASP). For termination, transit, or origination of internet telephony calls out of the country, the	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
					bypass these costs by using a SIM Box or a cheap ASP license to terminate international traffic.		applicable license is International Gateway Systems and Services (IGSS)	
		2.3	Provide for obligations of internet telephony service providers to ensure compliance with the existing legal and regulatory documents on telephony services.	Provide for obligations of internet telephony service providers to ensure compliance with the existing legal and regulatory documents on telephony Services <i>specifically regarding Subscriber Registration, Anti-SIM Boxing measures, and the prohibition of unauthorized bypass of international gateways.</i>	The biggest threat is the violation of the Telecommunication Plan of Kenya by using mobile numbers for VoIP gateways. Fraudsters often claim VoIP is a new technology not covered by old subscriber registration laws.	Not adopted Compliance with legal and regulatory requirements covers all obligations required from the licensee like subscriber registration, obtaining the right license for the right service and refraining from obtaining service dishonestly.	Requirements with regards to subscriber reg are sufficiently provided in the Subscriber registration regulation of 2025. Further, Clause 8.3 of the guidelines requires commercial internet telephony service providers to register their subscribers. Clause 5.2 of the guidelines require commercial internet telephony service providers to acquire an IGSS license for termination, transit, or origination of internet telephony calls out of the country.	None
		2.4	Provide for best practice regarding deployment and rollout of internet telephony services	Provide for best practice regarding deployment and rollout of internet telephony services <i>focusing on technical transparency, ensuring that all deployments allow for the accurate identification of call origin (IP and CLI) and prevent signaling manipulation.</i>	Best practice must include Traceability. If a call cannot be traced then it is hard to bill and secure it. Deployments that use encryption to hide the origin of a call make it impossible for MNOs to detect if a call is local or international.	Not adopted. Best practice deployment of commercial internet telephony services spans beyond transparency, CLI and signal manipulation for it includes other aspects like QoS, prudent use of numbering resources, use of IPv6 and associated emerging technologies all	Clause 6.4, 6.5 and 6.6 have sufficiently addressed the concerns.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
						which cannot be stated on the objectives.		
		3.4	Local and International Commercial Internet Telephony Calls	Local and International Commercial Internet Telephony Calls <i>including the criteria for call classification and the prevention of international to-local bypass.</i>	The scope needs to explicitly include the classification and identification of what constitutes a "local" vs. an "international" call when IP networks are involved.	Not adopted.	Clause 7 of the guidelines on local and international commercial internet telephony calls sufficiently defines and distinguishes a local call from an international call. Further, Clause 6.4 and 6.5 of the guidelines spell out the deployment guidelines made to prevent international to local bypass.	None
		3.6	Obligations for Public Switched Telephone Network (PSTN) and Public Land Mobile Networks (PLMN) in relation to Internet telephony service providers.	Obligations for Public Switched Telephone Network (PSTN) and Public Land Mobile Network (PLMN) in relation to Internet telephony service providers <i>including the right of MNOs to filter, flag, or reject non-compliant or fraudulent traffic originating from Internet Telephony providers.</i>	This will explicitly allow MNOs to refuse traffic that doesn't meet security standards.	Not adopted. The ultimate decision to block suspected fraudulent calls is for the Regulator. However interim measures have been provided to secure MNOs networks against such fraudulent activities.	Clause 9 of the guidelines provides the obligations for PSTN and PLMN in cases of fraudulent traffic and calls terminating without valid CLI.	None
		3.7	General obligations for Commercial Internet Telephony Service Providers	General obligations for Commercial Internet Telephony Service Providers <i>regarding subscriber registration, billing integrity, and fraud prevention.</i>	Ensures that the scope covers the validation of subscriber identities and revenue assurance.	Clause 3 provides for the general scope of the guidelines. Matters to do with subscriber registration, billing integrity, and fraud prevention have been provided within the guidelines, the license conditions and KICA regulations.	Clause 3 provides for the general scope of the guidelines and need not provide for the specifics as proposed.	None.

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
		Proposal for addition in the scope (3.9)		Establishment of technical standards for interconnect security and signaling integrity, specifically requiring the mandatory preservation of transparent SIP headers and the validation of Calling Line Identifier (CLI) authenticity.	Prevents Header Manipulation. Fraudulent operators often strip or rewrite the original data in a SIP header to hide the call's international origin. By scoping signaling integrity, the regulator makes it a technical violation to alter these headers, ensuring that the metadata reaching the MNO is honest and billable. It provides the legal basis for mandating technologies like STIR/SHAKEN. This allows MNOs to verify that the person calling is who they say they are, effectively killing CLI Spoofing at the source.	Adopted. Added at clause 6.8	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8: The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR/SHAKEN) authentication framework for purposes of Caller ID authentication
		4	INTERNET TELEPHONY SERVICES (These guidelines are meant for the Hybrid model of commercial Internet Protocol telephony deployment. A zoomed-in	We propose that any model that interconnects with a PLMN/PSTN must follow this guideline, regardless of whether it is Hybrid or trunking.	We note that the draft guideline states that the guidelines are meant for the Hybrid model. Fraudsters often use a Trunk Replacement Model (Figure 1)	Not adopted. The trunk model depicted in the guidelines is an intra-network trunk where an operator transits its own traffic from one region of the	Under the ULF licensing regime there is no license issued for trunking services.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			architecture of the hybrid model with key components is depicted in Figure 4)		to run SIM boxes, claiming it's just transit. By excluding the other models, we might accidentally create a loophole where a provider says, "I'm not doing Hybrid, I'm doing trunking, so these fraud rules don't apply to me."	network to the other via IP trunking.		
		4	The functionalities of the various components are detailed in Table 1. Table 1: Functions of Internet telephony Architecture components 	Component 1: Signaling Gateway Controller (SGC) Manages call setup, routing, and teardown <i>while preserving the original signaling metadata (such as the OCN - Original Called Number) to ensure end-to-end traceability.</i> Session Border Controller (SBC). Protecting and regulating traffic, <i>performing mandatory CLI validation, and ensuring that no header manipulation (stripping or re-mapping) occurs at the network boundary across distinct network.</i> Media Gateway, converts voice between IP and traditional formats; <i>commercial deployments must ensure these gateways are hosted in secure,auditable environments and are not used to bypass international gateways.</i>	Adds a requirement for Signaling Integrity. The SBC is the security guard of the network. If a fraudster owns the SBC, they can manipulate headers before the traffic hits your network	The functions of the various components as provided are comprehensive.	Network components have various functionalities that keep evolving with advancement inn technology and therefore exhaustively listing all functions is not practical.	None
		5.2	For termination, transit, or origination of internet telephony calls out of the country, the applicable license is International Gateway Systems and Services (IGSS).	For termination, transit, or origination of internet telephony calls out of the country, the applicable license is International Gateway Systems and Services (IGSS). <i>IGSS holders are strictly prohibited from transiting international traffic through local ASP interconnect points; all such</i>	To provide a Technical Proof of Origin clause.	IGSS license obligates the holder to interconnect with other service providers for transit or termination of international traffic.	Offense related to dishonest service provision including interconnection are covered in section 28 of KICA.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				<i>traffic must be delivered via designated International Interconnect Exchange points and billed at the prevailing international termination rates.</i>				
		5.3	Suggested addition	All licensees providing commercial internet telephony must provide a Performance Bond or Bank Guarantee to the Authority. This guarantee shall be used to settle any outstanding interconnect debts or fines resulting from	This is to ensure that operators engaging in SIM Boxing do not vanish after committing fraud.	Not adopted. Interconnect debts arise out of commercial agreements and can only be dealt with under the existing Dispute resolution framework	Condition 22 of the NFP tier 1 provides for a mechanism for dispute resolution.	None
		6.1	Deployment and roll-out of Internet Telephony services shall utilize Internet Protocol (IP) version 6 and any emergent latest technologies riding on IPv6, both at the network and end user levels.	Deployment and roll-out of Internet Telephony services shall utilize Internet Protocol (IP) version 6 and any emergent latest technologies riding on IPv6, both at the network and end user levels. <i>Service providers must ensure that the originating enduser IPv6 address is preserved and visible in the signaling headers. The use of Carrier-Grade NAT (CGN) to obfuscate the identity of endpoints terminating traffic onto a PLMN is prohibited.</i>	Added a requirement for End-to-End IP Visibility. Fraudsters often use NAT (Network Address Translation) or IPv6-to-IPv4 Tunneling to hide their true identity. If a VoIP provider uses a single IPv6 address to mask a SIM Box containing 100 SIM cards, the traceability benefit of IPv6 is lost.	Not adopted This is catered for in Clause 6.4.1 which requires that from deployment it should be possible to trace the IP address of the originating call.	This is to curb the vice of terminating international calls disguised as local calls.	None
		6.4.1	Trace the IP address of the originating call, noting that different Regional Internet Registries (RIRs) have different IP address blocks.	Trace the actual originating IP address, <i>prohibiting the use of anonymizing proxies or VPNs that mask the true geographic source of the call</i> , noting that different Regional Internet Registries (RIRs) have different IP address blocks	To tighten the definition of originating IP.	Not adopted For an IP address to be traced to the origin it should not have been anonymized or masked.	Offense related to dishonest service provision with intent to avoid payment of any charge are covered in section 28 of KICA.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
		6.4.2	View the airtime top-up pattern of a given internet telephony number.	View the airtime top-up pattern of a given internet telephony number. <i>MNOs must implement automated triggers to flag numbers exhibiting machine-like recharge behavior associated with SIM boxing.</i>	To tighten the definition of originating IP	Implementation of automatic triggers is an operational issue for the MNO's.	Clause 6.4.1 of the guidelines has put in place deployment parameters that will enable detection of SIM boxing behaviors	None
		6.5	All calls made via VoIP platforms must display valid Caller Line Identifiers (CLI) information for purposes of distinction between international and local commercial internet calls.	All calls must display valid, <i>unaltered, and authenticated</i> CLI. <i>All VoIP-originated traffic must include a certified 'Attestation' level per STIR/SHAKEN standards to verify the relationship between the provider and the calling number.</i>	The current wording of a Valid CLI is too weak. A spoofed number can look valid but be a lie.	Adopted. Added at clause 6.8	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8: The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR/SHAKEN) authentication framework for purposes of Caller ID authentication
		6.7	It shall be possible to demonstrate that the numbers used for termination of local commercial internet telephony traffic within the country are configured on systems of Kenyan licensed commercial internet telephony providers	It shall be possible to demonstrate <i>via real-time signaling audits</i> that the numbers are terminated on locally hosted gateways within Kenya. <i>Any local number found to be terminating traffic from an International IP gateway without an IGSS license shall be immediately decommissioned.</i>	For clarity	Not adopted The statement is broad to allow for any form of demonstration whether real-time signaling or not.	Clause 5.2 of the guidelines require commercial internet telephony service providers to acquire an IGSS license for termination, transit, or origination of internet telephony calls out of the country. Further, Offense related to dishonest service provision with intent to avoid payment of any charge are covered in section 28 of KICA.	None
		7.1	A subscriber of a Kenyan internet telephony provider calling a subscriber of another telephony service provider in Kenya, irrespective of their physical location,	A subscriber of a Kenyan internet telephony provider calling a subscriber of another telephony service provider in Kenya, <i>shall be considered to be making a local call provided that the local call originates from a Kenyan-allocated IP address</i>	The draft as it is especially on irrespective of their physical location can allow a person in London or Dubai to use a Kenyan	All calls are terminated using mobile numbers which are assigned by local service providers.	Noting that internet telephony transit over the internet which is global, the calling subscriber's location does not determine whether the call is local or international.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			shall be considered to be making a local call.		VoIP app to call a Kenyan mobile number and have it treated as a local call. Consequently, the MNO loses the International Termination Rate (ITR), and the VoIP provider pockets the difference. This creates a legalized bypass.	IP addresses are assigned by AFRINIC.		
		7.2	Local internet telephony calls shall be subjected to local interconnect rates.	Add. 7.2. Local internet telephony calls shall be subjected to local interconnect rates. <i>Any traffic presented as local that is found to originate from a non-Kenyan IP or via an unauthorized gateway shall be reclassified as international and subjected to premium international termination rates plus a penalty surcharge.</i>	The draft as it is especially on irrespective of their physical location can allow a person in London or Dubai to use a Kenyan VoIP app to call a Kenyan mobile number and have it treated as a local call. Consequently, the MNO loses the International Termination Rate (ITR), and the VoIP provider pockets the difference. This creates a legalized bypass.	Clause 9.3 requires PSTN and PLMN to flag and report internet calls with Calling Line Identifiers suspected to be invalid or manipulated.	Offense related to dishonest service provision with intent to avoid payment of any charge are covered in section 28 of KICA.	None
		7.3	A subscriber of a non-Kenyan telephony provider calling a subscriber of a Kenyan	Any call entering the Kenyan ecosystem from an International SIP Interconnect or a foreign IP range shall be classified as an international internet call, regardless of the CLI displayed.	Same Justification as no 62 and 63	-All calls are terminated using mobile numbers which are assigned	Clause 6.4.1 of the guidelines has put in place deployment parameters that will enable detection of SIM boxing behaviors.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
			telephony service provider in Kenya, irrespective of their physical location, shall be considered to be making an international internet call.			by local service providers. -IP addresses are assigned by AFRINIC.	Further, Offense related to dishonest service provision with intent to avoid payment of any charge are covered in section 28 of KICA.	
			Proposed addition	Add: 7.5. Licensed providers are prohibited from tromboning or looping international traffic to make it appear as local. MNOs reserve the right to audit the P-Charge-Info and Via headers in the SIP signaling to verify the true path of the call.	To prevent the specific Hybrid fraud mentioned in Section 4, we propose to add this anti-arbitrage clause 7.5. For example, If a call starts in the US, goes to a Kenyan VoIP server, and then to your mobile network, it is International. Without this clause, the VoIP provider will argue it is "Local" because it came from their Kenyan server.	Not adopted. The guidelines have delineated the scope of operation for commercial internet telephony, with ASP for local operation and IGSS for international operation.	Clause 6.4.1 of the guidelines has put in place deployment parameters that will enable detection of SIM boxing behaviors	None
		8.1	Transit or deliver only internet calls with valid Calling Line Identifiers.	Transit or deliver only internet calls with authenticated and non-manipulated Calling Line Identifiers. The provider must ensure that the CLI corresponds to a registered subscriber on their network and that the P-Asserted-Identity (PAI) header matches the originating source.	The term Valid in the draft is a subjective term. A SIM boxer can present a valid local mobile format (e.g., 07XX...) that is actually spoofed or unauthorized.	Adopted. Added under section 6.	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8. The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR /SHAKEN) authentication framework for

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
								purposes of Caller ID authentication.
			Proposed addition	Add: 8.4. The provider shall implement automated Fraud Management Systems (FMS) capable of detecting and blocking machine-like calling patterns, high-frequency short-duration calls, and SIM-box signatures before they reach the interconnect point.	To further strengthen Section 8. This is to ensure that if a SIM box is discovered, the VoIP provider cannot say we didn't know. It makes it their legal obligation to have the technology to stop it before it hits your network.	Adopted. Added under section 6.	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8. The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR /SHAKEN) authentication framework for purposes of Caller ID authentication.
			Proposed addition	8.5 Providers are obligated to populate the Via and User-Agent SIP headers accurately. They must not use stripping or topology hiding techniques that obscure the original IP address or the geographic origin of the call.	To further strengthen Section 8. This is to ensure that if a SIM box is discovered, the VoIP provider cannot say we didn't know. It makes it their legal obligation to have the technology to stop it before it hits your network.	Adopted. Added under section 6.	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8. The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR /SHAKEN) authentication framework for purposes of Caller ID authentication.
			Proposed addition	8.6 The provider shall be held financially liable for any international traffic passed to an MNO as local traffic (Interconnect Bypass). MNOs shall have the right to back-bill such traffic at the International Termination Rate (ITR	To further strengthen Section 8. This is to ensure that if a SIM box is discovered, the VoIP provider cannot say we didn't know. It	Clause 9.3 requires PSTN and PLMN to flag and report internet calls with Calling Line Identifiers suspected to be invalid or manipulated.	Offense related to dishonest service provision with intent to avoid payment of any charge are covered in section 28 of KICA.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
					makes it their legal obligation to have the technology to stop it before it hits your network.			
		9.1	Ensure only internet calls with valid Calling Line Identifiers are terminated or switched through their networks	The PSTN and PLMN shall implement industry standard automated filtering to ensure only internet calls with valid and verifiable Calling Line Identifiers are terminated. MNOs shall not be held liable for terminating calls where the CLI has been fraudulently manipulated by the originating provider in a manner that bypasses standard detection.	The clause mandate that the MNO must ensure only valid CLIs are terminated. This is technically difficult if the originating provider is spoofing the CLI at the source. If an MNO fails to block an invalid call, then they could be held in regulatory breach for another provider's fraud.	Adopted. Added under section 6.	This is to ensure that calls are validated as legitimate by originating carriers and other interconnected networks before reaching consumers	6.8. The commercial internet telephony platforms shall implement the Secure Telephone Identity Revisited and Signature based Handling of Asserted Information using Tokens (STIR /SHAKEN) authentication framework for purposes of Caller ID authentication.
		9.3	Flag and report internet calls with Calling Line Identifiers suspected to be invalid or manipulated	Flag and report internet calls <i>exhibiting fraudulent signatures (e.g., high-volume short duration calls from a single IP or unauthorized range). Upon reporting such traffic, the MNO shall have the right to immediately suspend the interconnect link with the offending provider pending investigation.</i>	Suspected to be invalid is a high operational burden. It requires constant manual or expensive automated oversight.	Not adopted. The usage of the term suspected is meant to allow for PSTN and PLMN to apply various fraudulent signature for flagging suspicious calls. Further, the ultimate decision to block suspected fraudulent calls is for the Regulator. However interim measures have been provided	Advances in technology can create various fraudulent signatures which cannot be exhaustively listed in the guidelines.	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
						to secure MNOs networks against such fraudulent activities.		
			Recommended for addition	PSTN and PLMN providers reserve the unilateral right to refuse or drop any internet telephony traffic that fails to provide transparent signaling headers (as per Clause 3.9) or originates from blacklisted/unauthorized IP ranges.	None	Not adopted. The ultimate decision to block suspected fraudulent calls is for the Regulator. However interim measures have been provided to secure MNOs networks against such fraudulent activities.	Clause 9 of the guidelines provides the obligations for PSTN and PLMN in cases of fraudulent traffic and calls terminating without valid CLI.	None
			Recommended for addition	9.5 The PSTN/PLMN shall be indemnified by the originating Internet Telephony Provider against any loss of revenue, regulatory fines, or legal action arising from Interconnect Bypass or SIM Boxing activities originating from said provider's network.	None	Not adopted. Commercial internet telephony services operate under an ASP license which has obligations and any offenses committed under this license is their obligation.	These guidelines are technical and operational and therefore are not to resolve issues with indemnity.	None
11.	The Campaign Registry	General Comment	N/A	Extending Identity Principles Across Digital Communication Services While the consultation focuses on internet telephony, similar identity challenges are increasingly observed across other forms of digital communication services. Enterprise messaging services - including SMS and RCS for Business Messaging - are widely used by organizations to deliver business-to-consumer communications such as: • Service notifications • Authentication messages • Financial alerts	None	Noted	These guidelines are for commercial internet telephony, the issues of consistent identity transparency principles can only be addressed in the broader digital communication services regulatory framework	None

No.	Stakeholder	Section	Current Content	Proposed Content	Stakeholder Justification	CA Position	CA Justification	New Content
				Customer engagement communications. As with voice services, these communication pathways can be vulnerable to misuse if the identity of the originating entity is not clearly verified. Applying consistent identity transparency principles across both voice and messaging services can help create a more unified and trusted communications environment.				
		General Comment	N/A	The regulatory focus on CLI validation and traceability highlights the importance of establishing trust at the point where communications originate. In many communications ecosystems, governance approaches are being explored that introduce mechanisms to improve viability into enterprise communications activity <i>before</i> it enters a broader network. Such approaches are designed to: - Support identity transparency - Strengthen accountability - Enhance traceability across communications ecosystems. By aligning identity principles across both internet telephony and enterprise messaging services, regulators and operators can help establish a more consistent framework for trust across all digital communications.	None	Noted	These guidelines are for commercial internet telephony, the issues of consistent identity transparency principles can only be addressed in the broader digital communication services regulatory framework	None