# THE STATE OF DOMESTIC AND INTERNATIONAL STIR/SHAKEN ADOPTION AND CALL AUTHENTICATION AND ENFORCEMENT

Philip J. Macres
Principal
KLEIN LAW GROUP PLLC
1250 Connecticut Avenue N.W.
Suite 700
Washington, D.C. 20036
(202) 289-6956
pmacres@kleinlawpllc.com

September 18, 2024

# PRELIMINARY DISCLAIMER

- This presentation is provided in my individual capacity, and the views expressed do not necessarily reflect the views of Klein Law Group or its clients.
- This communication is not intended to provide legal advice addressed to a particular situation, and prior results do not guarantee a similar outcome.

# AGENDA

- **Caller ID Authentication and Robocall Mitigation Plan***
  - 47 C.F.R. § 64.6300 *et seq.*
- **Call Blocking***
  - 47 C.F.R. § 64.1200(k), (n), & (o)
- **Reassigned Numbers Database***
  - 47 C.F.R. §§ 64.1200(l), 52.15(f)(1)(ii), & 52.103(d)
- **Snapshot of International Adoption of STIR/SHAKEN**

*** These Rules Continue to Evolve**

# STIR/SHAKEN: CALLER ID AUTHENTICATION

- Obligations of **Voice Service Providers with IP Networks**
  - Unless they have an extension, Voice Service Providers must have implemented the STIR/SHAKEN caller ID authentication framework in the Internet Protocol (IP) portions of their networks
  - **3 Obligations in Handling Calls:**
    1. Authenticate & Verify (originating and terminating call)
    2. Authenticate (originating call)
    3. Verify (terminating call)
  - **3 Attestations**
    1. Full Attestation (A)
    2. Partial Attestation (B)
    3. Gateway Attestation (C)

# STIR/SHAKEN: CALLER ID AUTHENTICATION

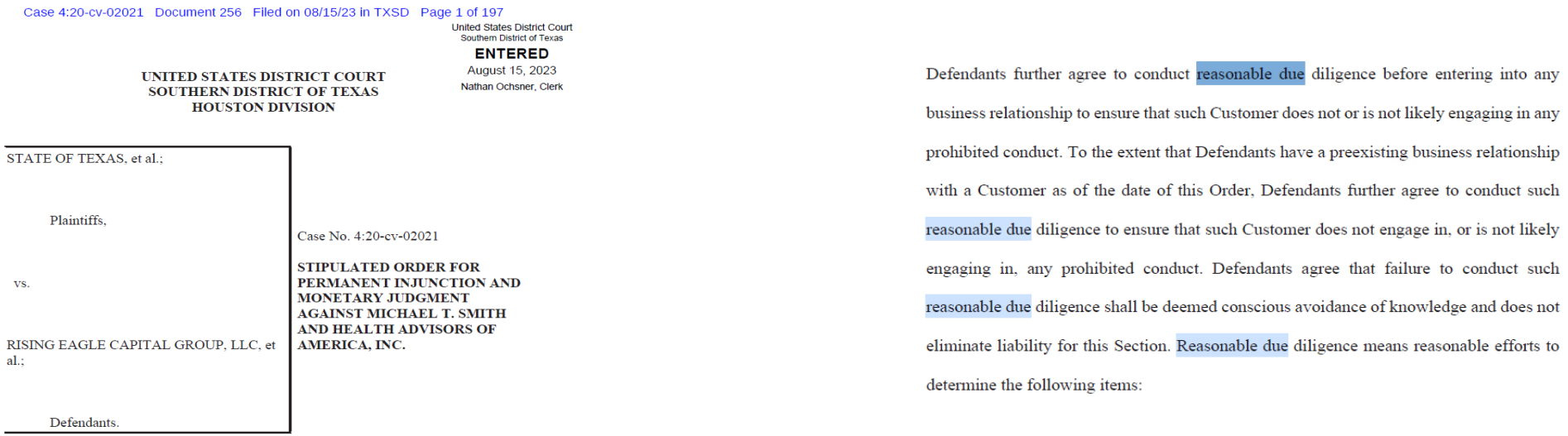
- **August 21, 2024: FCC's EB Settles NAL via and Order and Consent Decree**
  - In Short, NAL was based on A-level attestations provided on call traffic sent from the customer of its apparent reseller, where the reseller's customer did not have the authorization to use the telephone number in the caller-ID field.
  - The $2M NAL was reduced to $1M and Lingo is subject to a Compliance Program that includes an "**ATTACHMENT 1: OPERATING PROCEDURES"** which the FCC apparently supports on:
    1) **When to provide an A attestation (i.e., only when a provider has provided the number to the calling party);**
    2) **What the FCC expects in Knowing Your Customer;**
    3) **What the FCC expects for Knowing Your Customer for Upstream Providers; and**
    4) **What the FCC disapproves of for payment for transmitting and originating calls (no cyptocurrency, gift cards, or cash).**

# STIR/SHAKEN: CALLER ID AUTHENTICATION

- **August 21, 2024: FCC's EB Settles NAL for $1M via and Order and Consent Decree (cont'd)**
  - **No Safe Harbor:** Rules are still a moving target as the "Attachment 1: Operating Procedures" have a **disclaimer**:
    - "[P]rovisions are **not** a comprehensive robocall mitigation plan and are designed to **supplement**, rather than replace, existing caller ID authentication and robocall mitigation measures Lingo currently has in place or may implement in the future." (emphasis added)
    - "Compliance with these measures is **not** a defense to future violations of state or federal law or Commission Rules." (emphasis added)

# STIR/SHAKEN: CALLER ID AUTHENTICATION

- **What is KYC Reasonable Due Diligence?**
  - **Perhaps what the State AGs have expressed in the Aug. 15, 2023 stipulated order with Defendants Michael T. Smith and Health Advisors of America, Inc.**



Case 4:20-cv-02021 Document 256 Filed on 08/15/23 in TXSD Page 1 of 197

United States District Court
Southern District of Texas
**ENTERED**
August 15, 2023
Nathan Ochsner, Clerk

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF TEXAS**
**HOUSTON DIVISION**

STATE OF TEXAS, et al.;

Plaintiffs,

vs.

RISING EAGLE CAPITAL GROUP, LLC, et al.;

Defendants.

Case No. 4:20-cv-02021

**STIPULATED ORDER FOR PERMANENT INJUNCTION AND MONETARY JUDGMENT AGAINST MICHAEL T. SMITH AND HEALTH ADVISORS OF AMERICA, INC.**

Defendants further agree to conduct reasonable due diligence before entering into any business relationship to ensure that such Customer does not or is not likely engaging in any prohibited conduct. To the extent that Defendants have a preexisting business relationship with a Customer as of the date of this Order, Defendants further agree to conduct such reasonable due diligence to ensure that such Customer does not engage in, or is not likely engaging in, any prohibited conduct. Defendants agree that failure to conduct such reasonable due diligence shall be deemed conscious avoidance of knowledge and does not eliminate liability for this Section. Reasonable due diligence means reasonable efforts to determine the following items:

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order**
  - Requires ALL providers, regardless of their STIR/SHAKEN implementation status, to:
    1. Submit a detailed RMP in the FCC's RMD.
    2. Take "reasonable steps" to mitigate illegal robocall traffic.
       - "Reasonable steps" means for a provider to mitigate illegal robocall traffic via its RMP.
         - RMP is "**sufficient if it includes detailed practices that can reasonably be expected to significantly reduce**" illegal robocalling and provider "**must comply with the practices**";
         - RMP is insufficient if provider "**knowingly or through negligence**" routes or originates unlawful robocall campaigns; and
         - Must respond to tracebacks and be cooperative.
         - Rule effective August 21, 2023
    2. Submit a certification in the FCC's RMD.
  - **January 26, 2024** was the deadline to file and submit certifications in the RMD

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - What is detailed? Requires ALL providers, regardless of their STIR/SHAKEN implementation status, to
    - "describe with particularity" their robocall mitigation techniques,
      - Voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to **prevent "new and renewing customers" from originating illegal calls**;
      - Non-gateway intermediate providers and voice service providers must, like gateway providers, describe any **"know-your-upstream provider"** procedures in place designed to mitigate illegal robocalls;
      - To comply with the new requirements to describe their "**new and renewing customer**" and "**know-your-upstream provider**" procedures, providers **must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls**; and
      - All providers **must describe any call analytics systems they use to identify and block illegal traffic**, including whether they use a third-party vendor or vendors and the name of the vendor(s).

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Requires all providers to submit additional information with their certifications to the FCC's RMD.
  - FCC requires all providers:
    1. To submit additional information regarding their "**role(s) in the call chain**" and must indicated whether it is:
       - A voice service provider with a STIR/SHAKEN implementation obligation serving end-users,
       - A voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls,
       - A voice service provider without a STIR/SHAKEN obligation,
       - A non-gateway intermediate provider with a STIR/SHAKEN obligation,
       - A non-gateway intermediate provider without a STIR/SHAKEN obligation,
       - A gateway provider with a STIR/SHAKEN obligation,
       - A gateway provider without a STIR/SHAKEN obligation, and/or
       - A foreign provider.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - FCC requires all providers (cont'd):
    2. Asserting they do not have an obligation to implement STIR/SHAKEN because of an extension or because it **lacks the facilities necessary to implement** STIR/SHAKEN to explicitly state the rule that exempts it from compliance and **explain in detail why the exemption applies to the filer**;
    3. To certify that they (including their principals, affiliates, subsidiaries, and parent companies) **have not been barred** from filing in the RMD, **removed** from the RMD, **precluded** from filing in RMD unless deficiencies are cured, or whose **authorizations have been revoked** due to continued violations of the FCC's robocall mitigation rules; and
    4. To state whether they are **subject to a formal** FCC, law enforcement, or regulatory agency **action or investigation during the prior two (2) years** due to suspected unlawful robocalling or spoofing or deficient RMD certification or program and provide a description concerning any such actions or investigations.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - FCC requires all providers (cont'd):
    - In reporting formal action or investigations, the FCC clarified that providers **are not required to submit information concerning mere inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing**.
      - "[F]or example, traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement would not trigger this obligation **because they are not accompanied by findings of actual or suspected wrongdoing**." (emphasis added)
  5. To **submit their OCN if they have one**.
    - An OCN is a prerequisite to obtaining an SPC token, so this information allows the FCC to more easily determine whether a provider is meeting its requirement to diligently pursue obtaining a token in order to authenticate its own calls and provides an additional way to determine relationships among providers.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - FCC requires all providers (cont'd):
    - **Feb 26, 2024 Compliance Deadline for Nos. 1-5, above**: Providers newly subject to the FCC's RMD filing obligations and existing Providers must submit a certification and RMP in the RMD
      - Submissions may be made subject to existing confidentiality rules.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - By May 28, 2024, downstream providers were prohibited from accepting traffic from **non-gateway intermediate providers** that do not "affirmatively" list themselves in the FCC's RMD.
    - Stated differently, **downstream providers may not rely upon any non-gateway intermediate provider RMD registration that was imported from the FCC's "intermediate provider registry**."
  - At this time, **downstream providers are prohibited from accepting any traffic** from any domestic voice service providers, non-gateway intermediate providers, and gateway providers along with Foreign providers with US NANP numbers in caller-ID field that are:
    - **Not listed in the FCC's RMD with an RMP filed, or**
    - **Have otherwise been de-listed pursuant to an enforcement action.**

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Requires Intermediate Providers that receive unauthenticated IP calls directly from originating providers to authenticate those calls using STIR/SHAKEN.
  - Compliance Deadline: December 31, 2023.
  - **Note Prior Existing Obligations for Intermediate Providers:**
    - Not Alter Caller ID Information (except to remove the authenticated caller ID info. Tech. reasons or imminent threat).
    - Perform caller ID authentication for unauthenticated calls:
      - Required for Gateway providers and first intermediate providers in call chain
      - Other intermediate providers can be excused from authenticating if they cooperate with ITG and timely & fully respond to traceback requests

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Establishes **new enforcement tools to hold illegal robocallers accountable for violations of the FCC's rules**, including additional penalties for noncompliance and an expedited removal procedure for **facially deficient Robocall Mitigation Database filings**. Specifically, the FCC:
    1. Adopts a per-call forfeiture penalty **ranging from $2,500 to $23,727 per call for failure to block traffic** in accordance with the FCC's rules;
    2. Requires the removal of non-gateway intermediate providers from the RMD for violations of the FCC's rules, consistent with the standard applied to other filers;
    3. Establishes an expedited process for provider removal for "**facially deficient**" certifications and RMPs in the RMD.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Clarifies that a certification is **"facially deficient"** where the provider fails to submit a RMP within the meaning of its rules. **That is, it fails to submit any information regarding the "specific reasonable steps" it is taking to mitigate illegal robocalls. Examples include, without limitation, instances where the provider only submits:**
    1. A request for confidentiality with no underlying substantive filing;
    2. Only non-responsive data or documents (e.g., a screenshot from the Commission's website of a provider's FCC Registration Number data or other document that does not describe robocall mitigation efforts);
    3. Information that merely states how STIR/SHAKEN generally works, with no specific information about the provider's own robocall mitigation efforts; or
    4. A certification that is not in English and lacks a certified English translation.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Where a "willful" violation has occurred, the provider's RMD certification may be removed without a separate notice prior to the initiation of an "agency proceeding" to remove the certification.
  - A **two-step expedited procedure is established for removing a "facially deficient"** certification:
    1. Issuance of a notice by the Enforcement Bureau to the provider explaining the basis for its conclusion that the certification is facially deficient and **providing an opportunity for the provider to cure the deficiency or explain why its certification is not deficient within 10 days**; and
    2. **If the deficiency is not cured or the provider fails to establish that there is no deficiency within that 10-day period, the Enforcement Bureau will issue an order removing the provider from the database**.
  - Entities with **continued violations of robocall mitigation rules would result in revocation of Section 214 operating authority or for non-common carriers, other FCC authorizations and/or certifications.**
    - May prevent individual company owners, directors, officers, and principals of such entities from getting future FCC authorizations, licenses, or certifications.

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 Sixth Report and Order (cont'd)**
  - Addressed the application of STIR/SHAKEN obligations to Satellite Providers:
    - Concluded that satellite providers **that do not use NANP numbers to originate calls or only use such numbers to forward calls to non-NANP numbers are not "voice service providers"** under the TRACED Act and therefore do not have a STIR/SHAKEN implementation obligation.
    - **Grants an ongoing STIR/SHAKEN implementation extension for satellite providers that are small service providers using NANP numbers to originate calls**.
  - **Dec. 15, 2023**: Held that the two remaining STIR/SHAKEN implementation extensions granted by the Commission on the basis of undue hardship:
    - The extension for **small voice service providers originating calls via satellite** using U.S. North American Numbering Plan (NANP) numbers, and
    - The extension for providers that **cannot obtain an Service Provider Code (SPC) token**—and finds that they do not require revision

# LATEST RMP REQUIREMENTS IMPLEMENTING STIR/SHAKEN

- **FCC's Mar. 17, 2023 FNPRM**
  - Seeks comment on:
    - The **use of third-party caller ID authentication solutions** and whether any changes should be made to the FCC's rules to permit, prohibit, or limit their use.
  - Comments filed on June 5, 2023 and reply comments filed July 5, 2023 – Three General Camps:
    - Camp 1 - **Does not Support** 3rd Party Caller-ID Authentication.
    - Camp 2 - **Supports** 3rd Party Caller-ID Authentication, **so Long as Originating Provider's Token is Used.**
    - Camp 3 - **Supports** 3rd Party Caller ID Authentication, **without Requiring that the Originating Provider's Token be Used**.

# FCC EFFORTS TO ENSURE ACCURACY OF RMD

- **FCC's Aug. 7, 2024 NPRM on RMD**
  - FCC proposes on **procedural** measures to promote accurate information in the RMD, **technical validation** solutions to identify data discrepancies in filings, and **accountability measures** to ensure and improve the overall quality of submissions in the RMD.
  - Proposes and seeks comment on additional steps filers should be required to affirmatively take to ensure the accuracy of information submitted to the RMD, and to ensure that such information **remains accurate and up-to-date over time**, including:
    - Requiring providers to update information they have submitted to the FCC in **CORES within 10 business days of any changes**, to ensure that the information automatically populated into RMD submissions from that system is current.
    - Requiring **multi-factor authentication** each time a provider accesses the RMD.
    - Requiring providers to obtain a **unique PIN** that must be provided before the RMD will accept a submission.
    - Require a **$100.00 RMD per filing fee** and **technical solutions to flag and have discrepancies resolved** before RMD filings are accepted.

# FCC EFFORTS TO ENSURE ACCURACY OF RMD

- **FCC's Aug. 7, 2024 NPRM on RMD (cont'd)**
  - NPRM does the following, among other things (cont'd):
    - Proposes to establish a separate **base forfeiture amount of $10,000 for submitting false or inaccurate information to the RMD** or failing to keep information up-to-date.
      - The FCC also proposes a $1,000 forfeiture for **failure to update the RMD within 10 business days** and asks if it should establish this forfeiture as a continuing violation for every day inaccurate information remains in the RMD. It also asks should the FCC establish separate base and maximum forfeiture amounts for failing to update a filing within 10 business days.
    - Propose to authorize downstream providers to **permissively block traffic by RMD filers** that have been given notice that their robocall mitigation plans are **facially deficient** and **that fail to correct those deficiencies within 48 hours**.
    - Seek comment on additional procedural steps the FCC could require to encourage providers to submit **accurate and complete information to the RMD and CORES and keep that information current.**
  - Initial comments due Oct. 15, 2024 with reply comments due Nov. 12, 2024.

# RECENT ENFORCEMENT ACTIONS ON RMP FILINGS

# RECENT NOTABLE ENFORCEMENT ACTIONS - DEFICIENT RMP FILINGS

- **Failure to File Sufficient RMP**
  - **May 27, 2024:** Removed BPO Innovate from RMD (DA 24-283)
  - **Feb. 22, 2024:** Removed 13 providers from the RMD (DA 24-152, DA 24-153)
  - **Jan. 9, 2024:** Threatened to remove BPO Innovate from RMD (uploaded EIN) (DA 24-20)
  - **Oct. 16. 2023:** Reinstated Global UC into RMD with robust compliance plan. (DA 23-956)
  - **Oct. 16, 2023:** Threatened to remove 20 non-compliant providers from RMD for deficient RMP filings, response due 14 days later. (e.g., DA 23-960)
  - **Nov. 22, 2022:** Removed Global UC from RMD (DA 22-1219)
  - **Oct. 3, 2022:** Threatened to remove 7 providers from RMD for deficient RMP filings, response due 14 days later. (e.g., DA 22-1032)

# RECENT NOTABLE ENFORCEMENT ACTIONS - INITIAL AND FINAL BLOCKING ORDERS

- **Initial Determination Orders Issued**
  - **July 8. 2024: Veriwave (DA 24-645), Original Notice of Suspected Illegal Robocall Traffic (NSIRT) - April 4, 2024**
  - **Sep. 19, 2023: One Owl (DA 23-866), Original NSIRT Aug. 1, 2023**
  - **April 3, 2023: One Eye (DA 23-279), Original NSIRT Feb. 15, 2023**
- **Final Determination Order**
  - **May 11, 2023: One Eye (DA 23-389)**
- See Listing of Orders in EB Docket No. 22-174

# FCC ENFORCEMENT BUREAU'S ESTABLISHMENT OF C-CIST CLASSIFICATION

- **Consumer Communications Information Services Threat ("C-CIST") classification**
  - **May 13, 2024:** The Bureau classifies a party as a C-CIST when the party's misconduct—in either nature or scope—**poses a significant threat to consumers' trust in, and ability to use, communications information services.**
  - The Bureau applies this classification to **heighten awareness of these threat actors among our law enforcement partners and industry stakeholders**.
    - The objective is to ensure that these threat actors are readily detected and blocked from perpetuating potentially unlawful schemes that compromise our communications information services and harm consumers.
    - This notice will provide industry stakeholders with information to **enhance their "Know Your Customer" ("KYC") and "Know Your Upstream Provider" ("KYUP") processes**.

# FCC ENFORCEMENT BUREAU'S ESTABLISHMENT OF C-CIST CLASSIFICATION

- The Bureau classified a group of individuals and entities it is identifying as "Royal Tiger" as the first designated C-CIST.
  - **Royal Tiger is led by:** Prince Anand and his associate Kaushal Bhavsar.
  - **Royal Tiger's U.S-Based Providers**: Illum Telecommunication Limited; PZ Telecommunication LLC; and One Eye LLC.
  - **Royal Tiger's Associated United Kingdom-Based Entities**: PZ Telecommunications (UK) LTD; UK Tell Ltd.; and Opulix Digital Limited.

# FCC ENFORCEMENT BUREAU'S ESTABLISHMENT OF C-CIST CLASSIFICATION

- **Royal Tiger's Clients**: The Bureau identified the following as clients of Royal Tiger's U.S.-based voice service providers that initiated apparently illegal traffic that was transmitted through or originated on Royal Tiger's networks, as set forth in the Bureau's cease and desist letters to Illum, PZ Telecom, and One Eye. **Bureau listed the entities below to aid industry stakeholders in connection with KYC processes:**

| | |
|---|---|
| • Mavtel Voip<br>• Clevertel<br>• Edoro Technologies<br>• Q2Serves<br>• Spinning Mantra Communications Pvt. Ltd.<br>• Cyber Futuristics Pvt. Ltd.<br>• Iqbri Telecom Pvt. Ltd.<br>• Globalite Collaboration Pvt. Ltd. | • RD INFOTECH<br>• AARV Services Pvt. Ltd.<br>• Coequence<br>• Go4Customer/CyFuture<br>• SAGA<br>• Max Solutions<br>• LINTECH SOLUTIONS |

# Call Blocking

# CALL BLOCKING

(1) A voice service provider "**may" [to MUST] block** a voice call when the subscriber to which the originating number is assigned has requested that calls purporting to originate from that number be blocked because **the number is used for inbound calls only.**

- **Do Not Originate Lists**

(2) A provider **may block** a voice call purporting to originate from any of the following NANP number:

- **Not Valid**
- **Not Allocated**
- **Unused**
- **One-Ring Scam**

- **However, Gateway Providers "Must" Block Calls on a "reasonable DNO list" (which may also include not valid, not allocated, and unused NANP numbers).**
  - **FCC Sep. 6, 2024 Draft Eighth Report and Order on FCC's Sep. 26, 2024 agenda expands this mandate to all providers, with no safe habor DNO list.**
  - **DNO list needs to be reasonable**: "A DNO list so limited in scope that it leaves out obvious numbers that could be included with little effort may be deemed unreasonable."

# CALL BLOCKING

(3) **Terminating Provider ("TP") Blocking Calls without Liability**

- **Using Reasonable Analytics (considering Caller ID, if available)**
  - Consumer is informed and may opt out of blocking.
- **Highly Likely to be Illegal**
  - **Requires Human Oversight of Network Monitoring.**
    - Sufficient to ensure that calls blocked are highly likely to be illegal, and
    - Must include a process that **reasonably determines** that the **particular call pattern is highly likely to be illegal before initiating blocking** of calls that are part of that pattern.
  - **Discloses to consumers** that it is engaging in such blocking.
  - **Ceases blocking** calls if likely lawful**.**

# CALL BLOCKING

## (4) TP Blocking Calls without Liability (cont'd)

- **Requirements applicable to both**
  - Applies blocking in a **non-discriminatory, competitively neutral manner**;
  - Provide blocking with **no additional line-item charge** to consumers; and
  - **Offer redress via a Single Point of Contact (SPOC).**

# CALL BLOCKING

(5) **Blocking Calls without Liability - Non-Compliant Providers:**

- When the originating or intermediate provider, after being notified by the FCC:
  - Fails to **effectively mitigate illegal traffic within 48 hours;** or
  - Fails to **implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.**
- Prior to initiating blocking, the provider shall notify the FCC and summarize why the originating or intermediate provider meets **one or more** of these two conditions for blocking.

# CALL BLOCKING

(6) **If 911 Call – No Blocking:** A provider may **not block** a voice call if the call is an emergency call placed to 911.

(7) **No Blocking Gov. Emergency or PSAP #s**: A provider **may not** block calls unless the provider makes all reasonable efforts to ensure that calls from public safety answering points and government emergency numbers are not blocked.

(8) **Can Rely on Caller ID:** A provider may rely on Caller ID information to determine the purported originating number **without regard to whether the call in fact originated from that number.**

# CALL BLOCKING

(9) **TP Single Point of Contact ("SPOC") Requirements - Blocking Calls or Using Caller ID to Determine How to Deliver Calls:**

- SPOC on terminating provider's **public-facing website** for:
  - Receiving call blocking error complaints, and
  - Verifying the authenticity of the calls of a calling party that is adversely affected by information provided by caller ID authentication.
- **Dispute Resolution:**
  - Resolve disputes in reasonable time and provide update within 24 hours,
  - Promptly Stop Blocking if Error, and
  - No Charges.

# CALL BLOCKING

## (9) TP Realtime Blocking Transparency – Notification Code:

- Applies to blocking calls based analytics programs (by the TP or a 3rd party blocking services)
- All voice service providers in the call path **must immediately transmit** the certain blocking response codes to **the originating point of the call (i.e. the caller):**
- For a call terminating on an IP network - SIP code 603, 607, or 608 (FCC to replace 603, 607, or 608 with 603+)
- For a call terminating on an non-IP network – ISUP code 21 with cause location "user"
- Transmitting from IP to non-IP network SIP code 603 and 608 must map to ISUP code 21 (FCC to replace 607 and 608 with 603+ mapping to ISUP code 21)
- Transmitting from non-IP to IP network, ISUP code 21 must map to SIP Code 603, 607, or 608 where the cause location is "user". (FCC to replace ISUP 607 and 608 mapping with 603+)
- Per FCC's **Draft Eighth Report and Order**, on FCC's Sep. 26, 2024 Open Meeting Agenda
  - 12 months to implement from Federal Register publication.

# CALL BLOCKING

(10) **TP Conditions to Blocking Based on Analytics Program**:

- Subscriber inquiries on blocking
  - Must provide **within 3 business days of a subscriber's request;**
  - List of calls blocked, including the date and time of the call, going back 28 days; and
  - Provide such information at no additional charge.

# CALL BLOCKING

- **Other Key Ongoing Obligations that Apply to All Voice Service Providers Under TCPA**
  - Prevent Illegal Calls from Customers:
    - Take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including:
      - **Knowing your customers**, and
      - **Exercising due diligence** in ensuring that your services are not used to **originate illegal traffic.**
  - **Not Process High Volume Illegal Traffic** on US Network from other Providers.
  - Fully Respond to Traceback Requests within 24 hours.
  - Effectively Mitigate Illegal Traffic Upon Receiving and Per EB Notice.

# CALL BLOCKING

- **Overview of FCC's September 6, 2024 Draft Eighth Report and Order (Addresses 7th R&O FNPRM)**
  - **Expands** requirement to block calls based on a reasonable **DNO list to include all U.S.-based providers** in the call path.
  - Following FCC notification to a provider when its upstream entity cannot be identified, enhances existing requirements for such providers to block **"substantially similar traffic."**
    - Ensures that bad actors operating multiple entities cannot shield each other and circumvent the requirement.
  - **Establishes SIP code 603+** as the exclusive code to notify callers when calls on IP networks are blocked based on reasonable analytics to better correct erroneous blocking.
  - Establishes a **base forfeiture of $11K** (per customer, not per call) for providers that fail to take affirmative, **effect. measures to prevent customers from using their networks to originate illegal calls**
  - Adopts add. rules applicable to **mobile wireless providers concerning texts**:
    - Requires originating mobile wireless providers to block text messages following FCC notification of suspected illegal texts or ultimately have all of their text messages blocked by FCC direction
    - Requires mobile wireless providers to make email-to-text an opt-in service to better protect consumers.

# CALL BLOCKING

- **FCC's September 6, 2024 Draft Eighth Report and Order (cont'd)**
  - **Declined** to adopt a **safe harbor DNO list**.
  - **Declined** to adopt rules requiring **all terminating providers to offer analytics-based blocking** to consumers.
    - Imposing a mandate at this time could lead to over blocking or other problems.
  - **Declined** to require the **display of caller name information when caller ID has been authenticated**.
    - Record indicates both that CNAM databases are insufficient to provide a consumer with reliable information, and
    - A mandate requiring the use of other, newer, technologies is premature.
  - .

# Reassigned Numbers Database (RND)

# REASSIGNED NUMBERS DATABASE

- **Reporting Disconnections:**
  - Beginning April 15, 2021 and recurring on the 15th day of each month thereafter, service providers **must report permanent disconnections of their subscribers.**
  - The report must contain data for **numbers newly and permanently disconnected** (numbers that were not submitted in the service provider's prior reports).
  - Small service providers (those providers with 100,000 or domestic retail subscriber lines) had six additional months (**until October 15, 2021)** to begin reporting this information to the Reassigned Numbers Database Administrator.

# REASSIGNED NUMBERS DATABASE

- **Aging Numbers**
  - **Aging**: Numbers to be aged are disconnected numbers that are not available for assignment to another end user or customer for a specified period of time.
  - **Residential:** Numbers previously assigned to residential customers may be aged for no less than 45 days and no more than 90 days.
  - **Business**: Numbers previously assigned to business customers may be aged for no less than 45 days and no more than 365 days.

# REASSIGNED NUMBERS DATABASE ENFORCMENT

- **RND Non-Compliance**
  - **Dec. 12, 2022:** FCC proposed fines against 12 phone companies ranging from $33K to $93K that apparently failed to submit timely phone number disconnection information to the RND. This is an implicit FCC reminder that it takes RND reporting seriously.
- **Jan. 25, 2024**: FCC reiterated that the permanent disconnection reporting rule requires every service provider to file a monthly report in the RND, **even if it does not have permanent disconnections to disclose.**

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **Canada**
  - Regulator implemented STIR/SHAKEN.
  - Nov. 30, 2021: STIR/SHAKEN became effective (CRTC 2021-123) - Telecom. Service Providers (TSPs) are required to implement the STIR/SHAKEN to authenticate and verify caller-ID for IP-based voice calls as a condition of offering and providing telecommunications services.
  - **TSPs must submit an implementation status reports every six months, by May 31 and Nov. 30.**
- **France**
  - Regulator implemented STIR/SHAKEN.
  - Jan. 1, 2023: Automated dialed calls must come from a designated number block.
  - June 1, 2024: All operators required to have deployed STIR/SHAKEN and upload statistics to the MAN platform, a call authentication mechanism.
  - As of October 1, 2024, **all operators must start blocking unauthenticated calls** and calls that fail SHAKEN verification. See Transnexus blog and webinar.
- **Brazil**
  - Regulator implemented a variant of STIR/SHAKEN, Voluntary adoption.

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **Ireland**
  - Regulator did NOT implement STIR/SHAKEN.
- **United Kingdom**
  - Regulator did NOT implement STIR/SHAKEN, February 1, 2024 decided to not adopt call authentication (STIR/SHAKEN).
  - Guidance that providers are urged to follow to address illegal robocalling:
    - Tackling scam calls- Updating out CLI Guidance to expect providers to block more calls with spoofed numbers. (Pub. July 29, 2024)
    - CLI Guidance – Guidance on the provision of Calling Line Identification facilities and other related services. (Pub. July 29, 2024, applies Jan. 29, 2025)
- **Australia**
  - Regulator did NOT implement STIR/SHAKEN.
  - Australia blocks inbound international calls that spoof a domestic number.

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **India**
  - Regulator did NOT implement STIR/SHAKEN.
  - Telcom Regulatory Authority of India ("TRIA") implemented Distributed Ledger Technology (DLT) platform/framework to minimize unlawful robocalling.
  - **Aug 6, 2024:** TRIA seeks input from service providers:
    - **Asked Access Service providers** and their Delivery Telemarketers to take immediate action including implementing technical solutions for traceability and **to prevent bulk calling by their enterprise customers using 10-digit numbers through PRI/SIP**.
    - **Conveyed a strong message to the service providers and their Telemarketers to come forward and take effective measures to curb illegal robocalling.**

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **India (cont'd)**
  - Aug. 13, 2024 - TRAI, in a major step to curb the increasing number of spam calls:
    - Mandated all **Access Service Providers to stop voice promotional calls whether** pre-recorded or computer generated or otherwise from all **Unregistered Senders or Telemarketers (UTMs) using SIP/ PRI or other telecom resources**, as per following Directions:
      - **All promotional voice calls from the unregistered Senders/ Unregistered Telemarketer (UTMs) using Telecom Resources (SIP/ PRI/ other telecom resources) shall be stopped immediately.**

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **India (cont'd)**
  - If any unregistered Sender/ Unregistered Telemarketer (UTM) is found to be **misusing its Telecom Resources (SIP/ PRI/ other telecom resources) for making commercial voice calls** in violation of the regulations resulting into consumer complaints against any one or more number of resource indicators allocated to the Sender:
    - All the telecom resources of such Sender **shall be disconnected by the Originating Access Provider (OAP) for a period up to two years** as per regulation 25 provisions;
    - Such Sender shall be **blacklisted** by the OAP for a period up to **two years** as per the regulations' provisions;
    - Information regarding blacklisting of the Sender shall be shared by the OAP with all other Access Providers on DLT platform, **within 24 hours, who will, in turn, disconnect all the telecom resources given by them to that Sender within the next 24 hours**;
    - No new telecom resources shall be allocated to such Sender by any Access Provider during the period of **blacklisting** as provided for in the regulations;

# SNAPSHOT OF INTERNATIONAL ADOPTION OF STIR/SHAKEN

- **India (cont'd)**
  - All the **unregistered Senders/ Unregistered Telemarketers (UTMs) using SIP/ PRI/ other telecom resources to make commercial voice calls to the citizen shall be migrated to the DLT platform within one month of the issue of this Direction** and submit compliance report within **seven days** thereafter;
  - All Access Providers have been directed to comply with these directives and submit regular updates on the actions taken on **the 1st and 16th of every month**.
  - This decisive action by TRAI is expected to significantly reduce spam calls and provide relief to consumers.
- Sep. 3, 2024: TRAI announced that during the last two weeks, Access Providers have **blacklisted over 50 entities and disconnected more than 2.75 lakh (275K) SIP DID/Mobile Numbers/Telecom** resources

# CROSS BORDER AUTHENTICATION TRIAL

- **August 15, 2024**: ATIS, iconectiv Trial Industry Robocall Initiative With Bandwidth, Microsoft to Mitigate Unwanted Robocalls Globally.
  - ATIS and iconectiv prompting this new robocall mitigation initiative to combat unwanted robocalls and fraudulent scam calls on a global basis.
  - Bandwidth and Microsoft will be the first companies to trial the initiative that will deploy SHAKEN protocol for cross-border authentication.
    - Particularly important for calls that originate or terminate in countries that have not deployed SHAKEN nationally.

# QUESTIONS??

**Philip J. Macres**
**Principal**
**KLEIN LAW GROUP PLLC**
**1250 Connecticut Avenue N.W.**
**Suite 700**
**Washington, D.C. 20036**
**(202) 289-6956**
pmacres@kleinlawpllc.com