The Role of

STIR / SHAKEN and Traceback

In Tackling Illegal Robocalls

Thu, Dec 3, 2020 | 3:00 pm ET

Josh Bercu

USTELECOM
THE BROADBAND ASSOCIATION

VP of Policy and Advocacy

Jonjie Sena

neustar

Sr. Director, Product Marketing

TODAY'S CALL EXPERIENCE
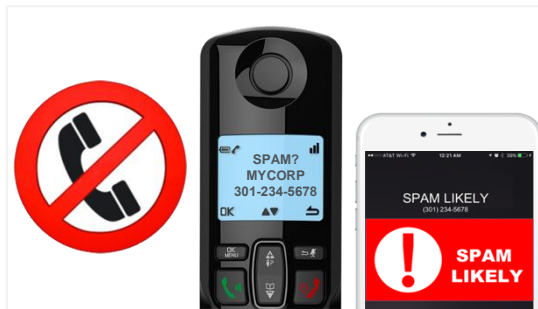
Calls we *don't want* are getting through

Spoofing of caller identity erodes brand and risks liability

Difficult to find the parties responsible for the fraud

Calls we *do want* are not getting through

Legitimate calls are mistakenly blocked or mislabeled as spam

Robocalls and call fraud mean consumers no longer answer

neustar

NO SILVER BULLET TO STOP ILLEGAL ROBOCALLS

OUR DISCUSSION

Regulations
- Federal TRACED Act (2019)
- FCC Safe Harbor for carriers to block illegal AND unwanted calls

Enterprise Vetting
- Know-Your-Customer (KYC)
- CATA best practices
- Outbound robocall mitigation carrier initiatives

STIR / SHAKEN
Call Authentication to battle call spoofing

Aggressive Enforcement
- FCC, FTC & DOJ actions & penalties

Robocall Analytics
- Call labeling and blocking
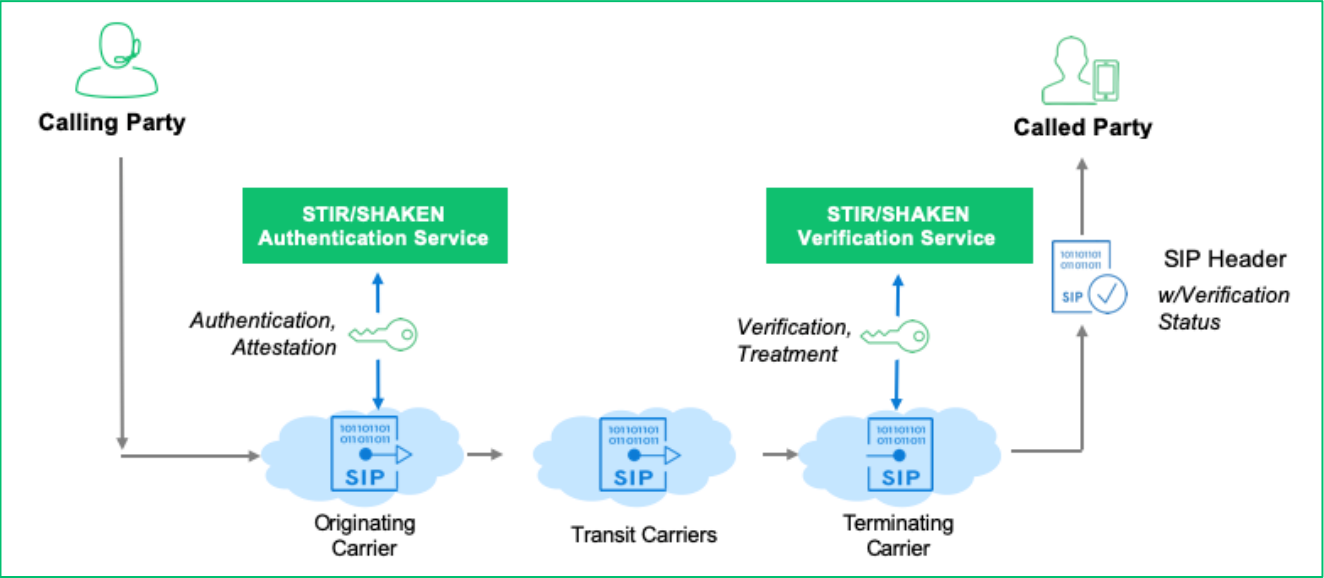- Registration of verified enterprises across carriers
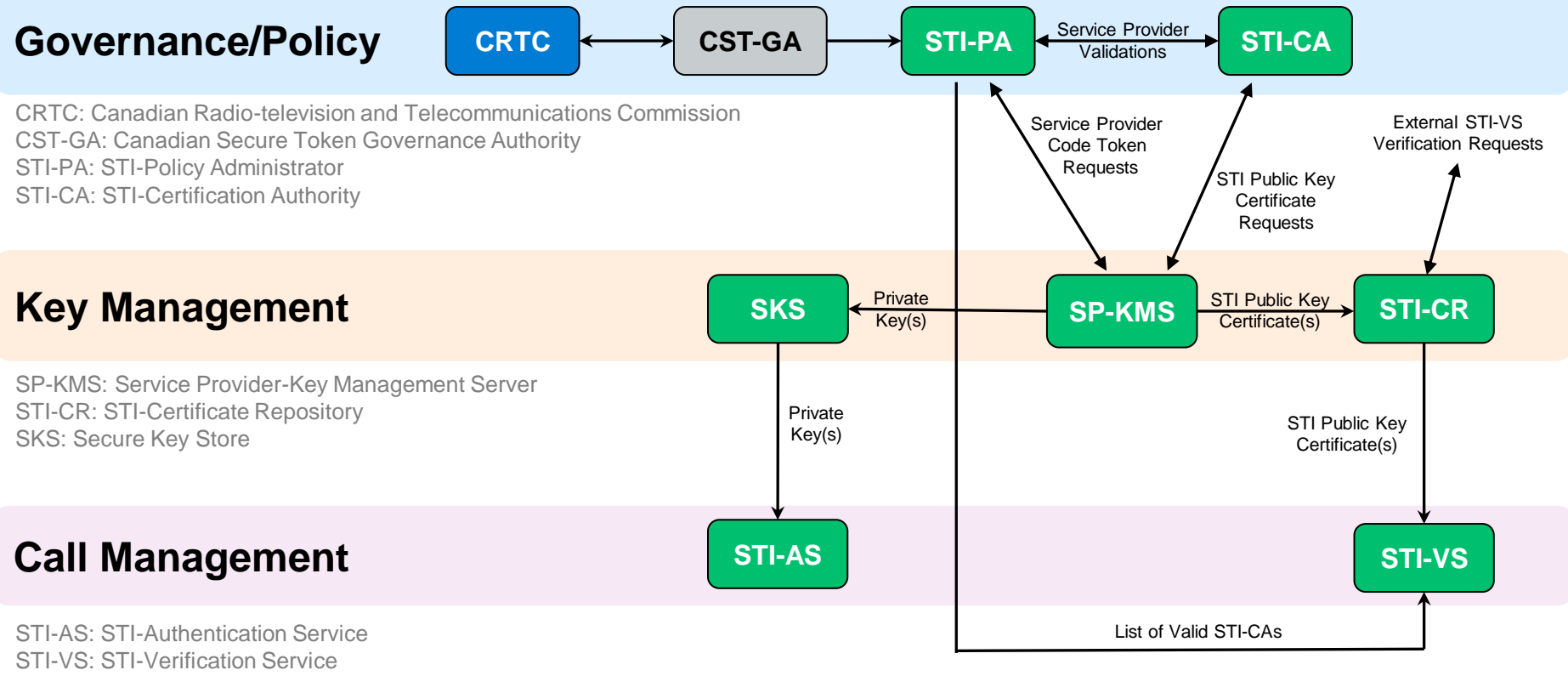- Do-Not-Originate

Traceback
Network forensics to identify source of illegal robocalls

neustar

STIR/SHAKEN

STIR/SHAKEN: USE DIGITAL CERTIFICATES TO AUTHENTICATE CALLS

STIR / SHAKEN FRAMEWORK

Governance/Policy

CRTC — CST-GA — STI-PA — Service Provider Validations — STI-CA

CRTC: Canadian Radio-television and Telecommunications Commission
CST-GA: Canadian Secure Token Governance Authority
STI-PA: STI-Policy Administrator
STI-CA: STI-Certification Authority

Service Provider Code Token Requests

STI Public Key Certificate Requests

External STI-VS Verification Requests

Key Management

SKS — Private Key(s) — SP-KMS — STI Public Key Certificate(s) — STI-CR

SP-KMS: Service Provider-Key Management Server
STI-CR: STI-Certificate Repository
SKS: Secure Key Store

Private Key(s)

STI Public Key Certificate(s)

Call Management

STI-AS

STI-VS

STI-AS: STI-Authentication Service
STI-VS: STI-Verification Service

List of Valid STI-CAs

Neustar Solution Components

neustar

STIR/SHAKEN ADOPTION IN ACCELERATING
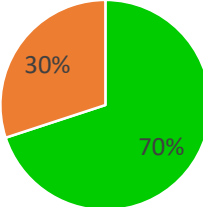
THE ATTESTATION GAP
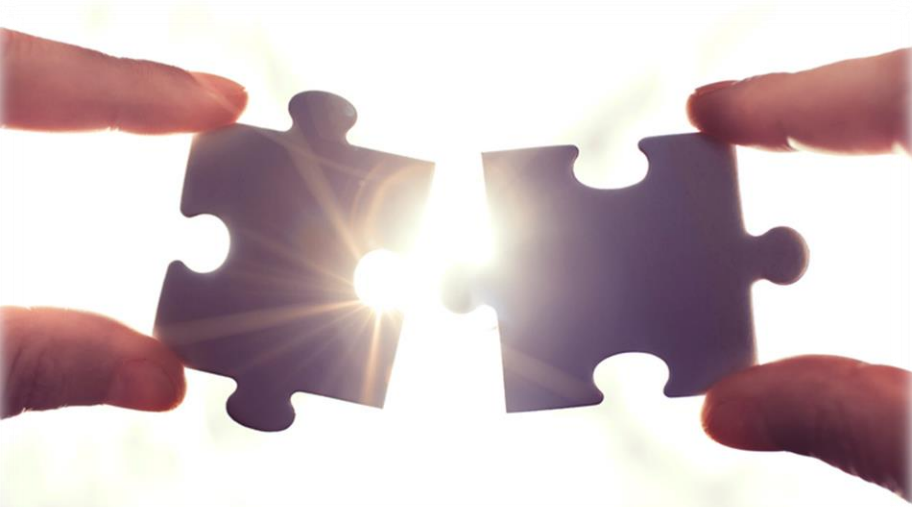
How can enterprises ensure their legitimate calls get the highest level of attestation?

A. FULL ATTESTATION

The OSP
- is responsible for the origination of the call onto the IP-based service provider voice network
- has a direct authenticated relationship with, and can identify the customer
- has established a verified association with the telephone number used for the call

Carrier A to Carrier B:
This is my customer. I gave them this telephone number. This call originated on my network.

B. PARTIAL ATTESTATION

The OSP
- is responsible for the origination of the call onto the IP-based service provider voice network
- has a direct authenticated relationship with, and can identify the customer
- has NOT established a verified association with the telephone number being used for the call

Carrier A to Carrier B:
This is my customer. This call originated on my network. However, I did not give them this telephone number.

C. GATEWAY ATTESTATION

The OSP
- has no relationship to the initiator of the call (e.g., international gateways).

Carrier A to Carrier B:
This call originated outside my network.

neustar

ATTESTATION GAP CREATES CONFUSION

CHALLENGE: An enterprise call to the same consumer, using the same originating number, can have different results!

WHY? Attestation level is determined by combination of
a) Which carrier (TNSP) is the source of the phone number
b) Which carrier (OSP) originates the call

TNSP X

TN - 703-123-5678

Enterprise

PBX / SBC,
BPO,
Call Center

Unsigned

OSP X

STI-AS

OSP Y

STI-AS

PSTN

attestation

A

attestation

B

Enterprises uses a TN from **TNSP X** to call a customer

TNSP X + OSP X = A attestation
TNSP X + OSP Y = B attestation

Same consumer, same originating number. Why different experience?
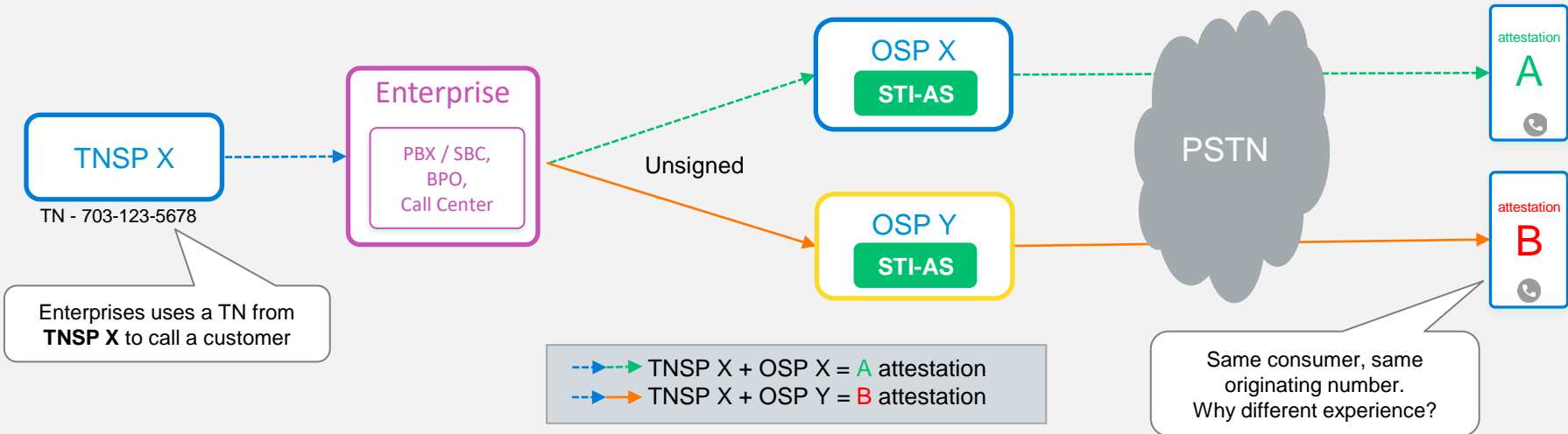
HOW ENTERPRISES CAN ATTEST TO THEIR OWN CALLS

SOLUTION: Enterprise signs call with a STIR certificate

WHY? Both calls receive Attestation A
   a)   OSP X signs call normally
   b)   OSP Y signs with A because STIR certificate alerts OSP that enterprise has been vetted, and is authorized to use this TN

Neustar CA

OSP X
STI-AS

attestation
A

Enterprise
PBX / SBC, BPO, Call Center

Sign w/ STIR Cert from Neustar

TNSP X

TN - 703-123-5678

Enterprises uses a TN from **TNSP X** to call a customer

OSP Y
STI-AS

PSTN

attestation
A

Same consumer call experience

TNSP X + OSP X = A attestation
TNSP X + **STIR Cert** + OSP Y = A attestation
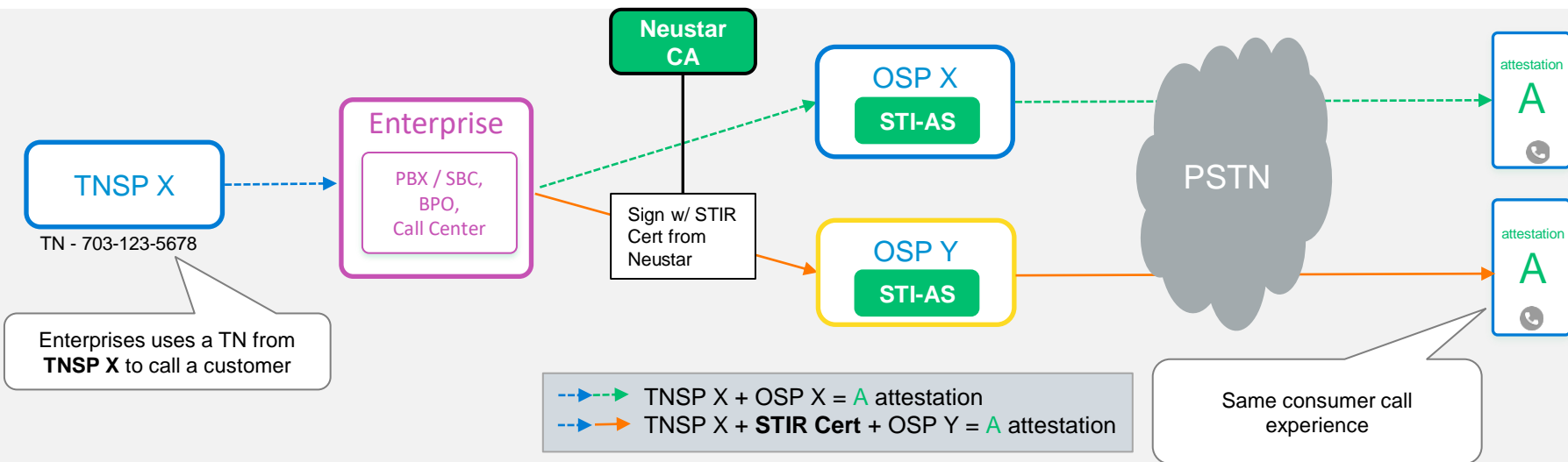
MULTIPLE WAYS TO ADDRESS ENTERPRISE ATTESTATION TODAY

Enterprise Attestation Elevation

Telephone Number (TN) Database

- Trusted database with TN vetting
  Options: Local, Centralized, Federated

- Industry proposal under consideration

SHAKEN Certificate Delegation

- TNSP delegates certificate to 3rd party
  Options: Carrier, Enterprise

- Industry proposal under consideration

STIR Certificate

- Validates business and TNs are authorized for use by enterprise

- Growing coalition of carriers will accept calls from enterprises verified by the Neustar Vetting Service, and sign with "A"

neustar

WHERE WE'RE HEADED
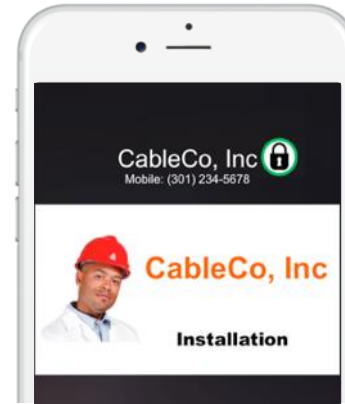
Traceback

USTELECOM
THE BROADBAND ASSOCIATION

WHAT IS A TRACEBACK?

Network-based process beginning with the terminating voice service provider (VSP) of the originating malicious traffic that is coming from a network, non-native to their own terminating network

The call is then systematically traced through the non-native networks that chronologically precede the terminating network(s) either until there is an uncooperative call path VSP or until the originating party is identified

In layman's terms:
Going backward through the multiple carriers that a call goes through until we find where it started

TRACEBACK CAST OF CHARACTERS

Calling Party | Terminating Voice Service Provider | Originating Voice Service Provider | United States Point of Entry (aka Gateway Provider) | Intermediate Carriers | Industry Traceback Group | State and Federal Enforcement Agencies
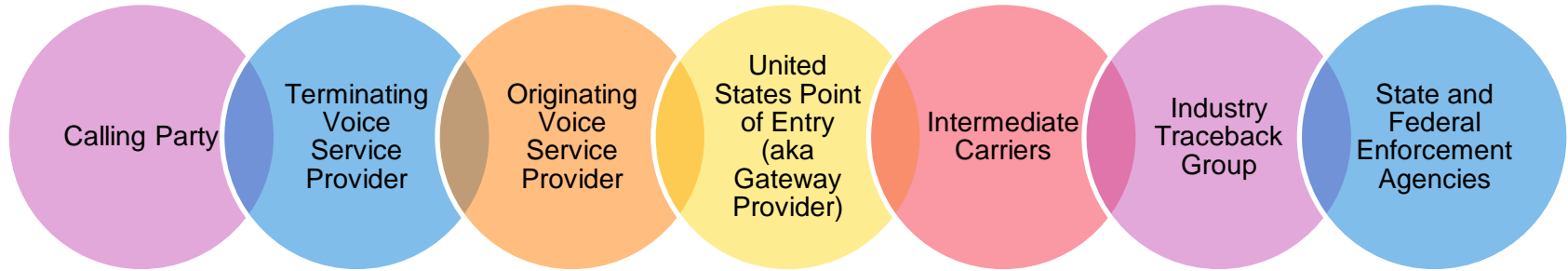
Calling party: entity responsible for placing illegal robocalls

Terminating VSP: first VSP in a traceback sequence

Originating VSP: last VSP in a traceback sequence.
The originating provider placed the call onto the network

U.S. Point of Entry (U.S. POE): first downstream VSP allowing traffic on to the US
Public Switched Telephone Network (PSTN) that was originated outside the US

RELEVANT TERMINOLOGY

An illegal robocalling **campaign** is a group of calls with identical or nearly identical messaging believed to be coming from the same source(s) as determined by the content and calling patterns of the caller; a single Campaign can represent hundreds of thousands or millions of calls.

Each campaign is broken up into **tracebacks** which are individual calls that are traced back associated with a given campaign; It typically only takes a handful of tracebacks to confidently identify the source of a campaign.
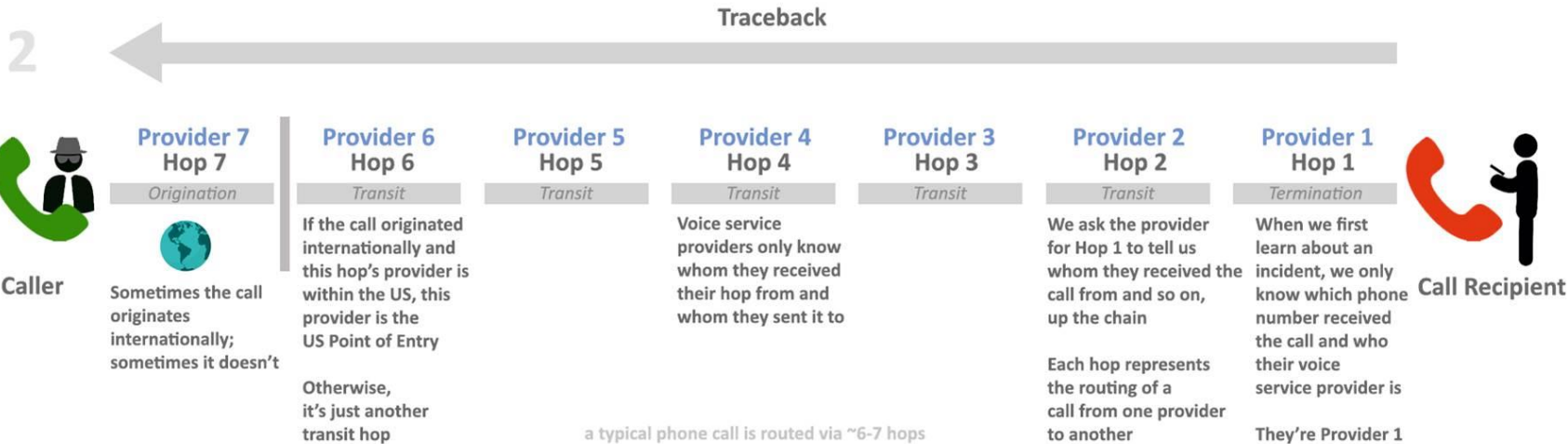
Each incident involves multiple **hops** which are the different VSPs that accept and pass traffic on to the next provider in the call path; most illegal robocalls contains multiple hops, often between 5-8 hops for a single call.

What is a Traceback?

1 USTelecom learns about potentially illegal calls from multiple sources

Traceback

2 ⟵

	Provider 7 Hop 7	Provider 6 Hop 6	Provider 5 Hop 5	Provider 4 Hop 4	Provider 3 Hop 3	Provider 2 Hop 2	Provider 1 Hop 1	
Caller	*Origination*	*Transit*	*Transit*	*Transit*	*Transit*	*Transit*	*Termination*	**Call Recipient**

Caller

Origination

Sometimes the call originates internationally; sometimes it doesn't

Transit

If the call originated internationally and this hop's provider is within the US, this provider is the US Point of Entry

Otherwise, it's just another transit hop

Transit

Transit

Voice service providers only know whom they received their hop from and whom they sent it to

Transit

a typical phone call is routed via ~6-7 hops

Transit

We ask the provider for Hop 1 to tell us whom they received the call from and so on, up the chain

Each hop represents the routing of a call from one provider to another

Termination

When we first learn about an incident, we only know which phone number received the call and who their voice service provider is

They're Provider 1

Call Recipient

3 In the case above, when the portal forwarded the call details to the provider for Hop 7, asking whom that provider received the call from, the Hop 7 provider told us that it was received from their subscriber and, ideally, provided us with some identifying information about that individual or business.

Other outcomes include:

- A stalled traceback where a provider doesn't respond or can't find the call record (CDR)

- A non-cooperative provider who refuses to share information

USTELECOM
THE BROADBAND ASSOCIATION

INDUSTRY TRACEBACK GROUP (ITG)
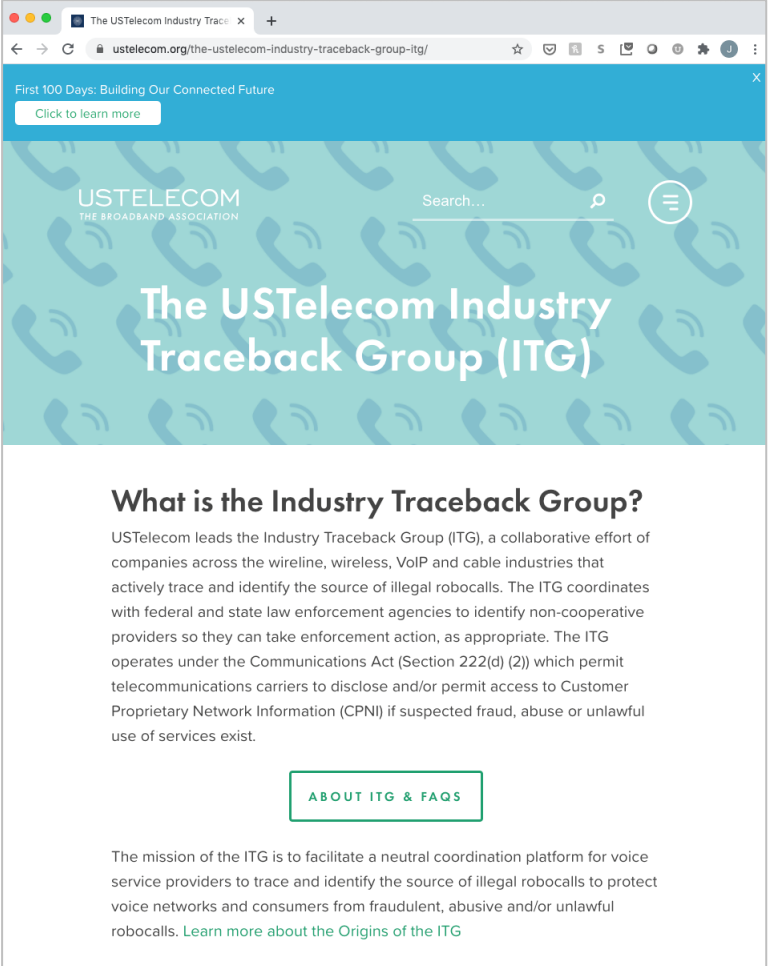
Collaborative effort of over 40 VSPs

- Includes wireless, wireline, VoIP, cable, ILEC, CLEC, wholesale

Mission: stop illegal robocalls at their source

- Identify the most prolific campaigns and trace them to their point of origin
- Identify severe and ongoing calls and trace them to their point of origin
- Work with VSPs to take appropriate mitigation steps to cut off access to the network for bad actors once identified
- Provide information to enforcement authorities as appropriate

Tracebacks conducted through a secure traceback portal

Governed by published Policies and Procedures

What is the Industry Traceback Group?

USTelecom leads the Industry Traceback Group (ITG), a collaborative effort of companies across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. The ITG operates under the Communications Act (Section 222(d) (2)) which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI) if suspected fraud, abuse or unlawful use of services exist.

ABOUT ITG & FAQS

The mission of the ITG is to facilitate a neutral coordination platform for voice service providers to trace and identify the source of illegal robocalls to protect voice networks and consumers from fraudulent, abusive and/or unlawful robocalls. Learn more about the Origins of the ITG

U.S. REGISTERED CONSORTIUM

June 2020

FCC Names USTelecom's Industry Traceback Group as Official Robocall Traceback Consortium

The TRACED Act (2019) required the FCC to issue rules and then designate *"a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls"*

Consortium must be neutral, maintain a set of written best practices, focus on *"fraudulent, abusive, or unlawful"* traffic

IDEAL TRACEBACK CANDIDATES

Incidents selected for traceback are generally:

- Representative of the highest-volume on-going illegal calling campaigns,
- Representative of on-going serious fraud or threat to life or property, or
- Needed as evidence in an active case

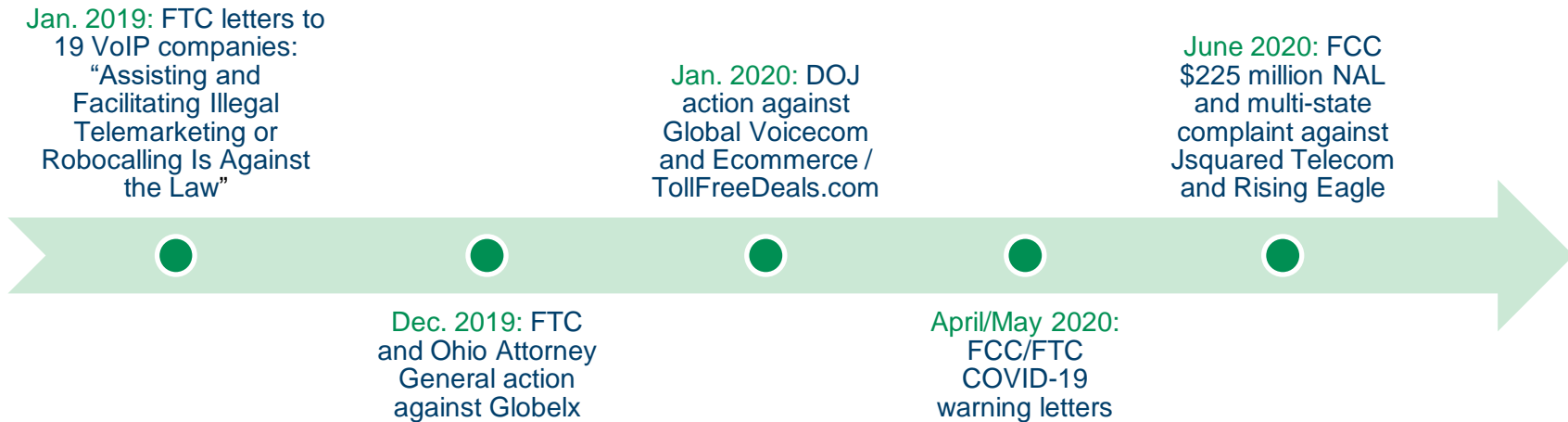**Ideal traceback candidates:**

- Include automatically captured (not manually written down) date, time and timezone of call
- Called and calling numbers
- Audio recording or transcript of robocaller's message
- List of violations making the call/campaign illegal
- Description of the campaign,
  including daily or monthly volume of calls

THE IMPACT OF TRACEBACKS

Goal is to stop illegal traffic and restore trust in the telephone network

Process itself can stop campaigns and encourage better practices in the industry

Coordination with federal and state enforcement agencies

Jan. 2019: FTC letters to 19 VoIP companies: "Assisting and Facilitating Illegal Telemarketing or Robocalling Is Against the Law"

Jan. 2020: DOJ action against Global Voicecom and Ecommerce / TollFreeDeals.com

June 2020: FCC $225 million NAL and multi-state complaint against Jsquared Telecom and Rising Eagle

Dec. 2019: FTC and Ohio Attorney General action against Globelx

April/May 2020: FCC/FTC COVID-19 warning letters

Discussion

neustar

USTELECOM
THE BROADBAND ASSOCIATION

COMPARISON OF THE TWO APPROACHES

When is it invoked?

- **S/S:** *start* of call
- **Traceback:** *post* call

For which call(s) is it invoked?

- **S/S:** For *every* call
- **Traceback:** For *call examples* in a reported suspected robocall campaign

What type of calls are the target?

- **S/S:** *All calls* to protect against calls illegal call spoofing
- **Traceback:** *Illegitimate calls* to find their source

Are there penalties for enterprises?

- **S/S:** No… but possible negative impact if unattested, opportunity to assure customers of legitimacy
- **Traceback:** No… but an opportunity to help protect brands and call centers

How is service made available to Enterprises?

- **S/S:** OSP normally signs; emerging use cases allows Enterprise to sign
- **Traceback:** Contact Josh and/or discuss with your vendor or telco provider (who should contact Josh)

Questions?

RESTORE TRUST IN PHONE CALLS

USTELECOM
THE BROADBAND ASSOCIATION

neustar

www.ustelecom.org

www.home.neustar