APCO 2025

July 27-30 | Baltimore, MD

Using STIR/SHAKEN to Prevent SWATTING

Sridhar Kowdley – Department of Homeland Security, Science and Technology Directorate

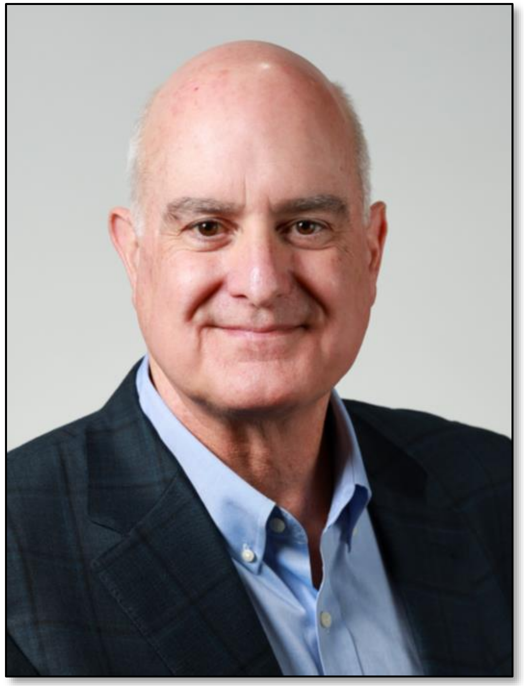
Scott Straub – TransUnion, Public Sector Market

Michael E Fox – Texas A&M Center for Applied Communications and Networks

Meet the Panelists

Sridhar Kowdley
Program Manager
Department of Homeland Security
Science and Technology Directorate

Scott Straub
Senior Director, Market Planning
TransUnion



Michael E Fox
Executive Director
Texas A&M Center for Applied
Communications and Networks

U.S. Department of Homeland Security | Science and Technology Directorate

Swatting Presentation

Science and Technology

July 29, 2025
Sridhar Kowdley
Office for Interoperability and Compatibility
DHS Science and Technology Directorate

DHS Science & Technology Authorities

- **Office for Interoperability and Capability Technology Center's (OIC-TC) Mission:** Provide subject matter expertise and core research capabilities needed to ensure that the Department of Homeland Security (DHS) Science & Technology (S&T) maintains the ability to identify and address current and future DHS component challenges in the areas of communication and network capabilities, as well as position, navigation, timing necessary for the functioning of many critical infrastructure sectors.
- S&T OIC-TC has a legislative mandate to enable interoperability for public safety (6 USC § 195 & 195a)
  - Support creation of national voluntary consensus standards for interoperable emergency communications
  - Understanding the strengths and weaknesses of the public safety communications systems in use
  - Evaluating and validating advanced technology concepts, and facilitating the development and deployment of interoperable emergency communication capabilities

Mapping of Interoperability Challenges/S&T Activities

Operate in many modes/standards/ frequencies
P25, DMR, Analog, encryption keys

DHS S&T

- P25 CAP (Subscribers, ISSI, CSSI); Interoperability and conformance to standards

Interconnection Systems- connect networks or systems

DHS S&T

- SBIR – Interconnection of multiple networks
- Interworking Interface (IWF)

Applications are non-standard and not interoperable
Inter-DHS issues; DHS/First responder Issues

DHS S&T

- Field Trials
- SBIR MCPTT Compliance Tools
- Broadband Interoperability Platforms

CAD-CAD Interfaces are non-standard and not interoperable; non-standard; proprietary systems; sharing of data not possible

DHS S&T

- Promoting CAD-to-CAD interoperability

NG-911 Systems must be standards compliant and interoperable;’ sharing data is critical;

- Researching on NG911 interoperability and standards-compliance
- Lab Development for testing
- AI for the telecommunicator

Science and Technology

Swatting Overview

- Malicious tactic of making hoax calls and reports to emergency services
- Conducted to harass, intimidate, or retaliate against intended targets
- Intended to cause confusion, chaos, or to divert public safety resources from valid emergencies, or to harass
- Could result in deadly consequences (targets could be public figures, schools, places of worship, and centers of mass transportation)
- Generally, use spoofing technology to conceal identity, phone numbers or other information (identify of the caller could also spoof
- Sources can be via e-mail, social media, or to a listed phone number and may come in the form of active shooter incidents, bomb threats, hostage situations, or other acts of violence

Swatting to PSAPs

Swatting sources:

- Calls sent Direct to the PSAP, public safety offices, schools (e.g., local police stations, administrative numbers)
- Relayed from third party
- Inbound calls are usually spoofed
- Use a relay service such as Telecommunications Relay Service, or even an innocent “Good Samaritan” using social media.

Swatting scenarios:

- Swatting scenarios include bomb threats, active shooter scenarios, threats of an imminent shooting rampage, hostage scenarios, and threats involving chemical, biological, radiological, nuclear, or explosives agents.

Potential Swatting Indicators

- Swatting call in singular report of emergency (usually multiple calls would be received)
- Incoming call number is spoofed or blocked- (Calls may use Voice over Internet Protocol (VoIP) services - all zeros or nines, blocked, unavailable)
- Caller's tone or background noises are inconsistent with claimed emergency
- Typing or clicking is heard (Swatters may be using video consoles or computers)
- Caller is unable to answer follow-up questions; caller details include specifics of terminology to refer to weapons used in video games (e.g., AR-15)
- Caller's story changes or escalates throughout the call
- Caller may mispronounce names such as the city, street or building names
- May be related to doxing (process of collecting and dissemination of personal information to intimidate, shame or embarrass) (In the news a great deal related)

S&T Recommendations / Related R&D

Training and Awareness:

- **Train Call Handlers:** Enhance training on swatting indicators using FBI resources and recent research.
- **SOPs:** Develop and integrate SOPs for handling swatting incidents in PSAPs, fusion centers, schools etc.

Information Sharing and Reporting:

- **Share Resources:** Distribute materials to schools, places of worship, and community centers. Develop community-specific emergency plans.
- **Report to Law Enforcement:** Ensure swatting incidents are reported and tracked in LEEP. Update with detailed post-incident information to ensure tactics and changes to approach by actors

Research and Development:

- **Call Spoofing Detection:** Fund R&D on spoofing detection technologies and transition successful solutions to the commercial sector.
- **STIR/SHAKEN Framework:** Collaborate with carriers to implement the framework to prevent caller ID spoofing.

S&T Recommendations / Related R&D

Artificial Intelligence and Machine Learning:

- **Sentiment and Stress Analysis:** Invest in AI to detect caller distress and deception cues.
- **Contextual Processing:** Advance techniques to interpret ambient sounds and detect mismatches.
- **Pattern Recognition:** Develop AI for recognizing spoofing tactics and behavioral anomalies.
- **Synthetic Datasets:** Create high-fidelity datasets for rare-event modeling.
- **Multimodal Fusion:** Integrate voice tone, metadata, social media signals, and prior records.
- **AI-Human Interfaces:** Design user-friendly dashboards for telecommunicator review.
- **Federated Learning:** Implement models that preserve privacy while improving performance.

Pilot Testing and Real-World Implementation:

- **Collaborations:** Work with NG911 systems, emergency responders, and financial community for pilot testing.
- **Technology Demonstrations:** Showcase research results and gather feedback through demos.

S&T Recommendations / Related R&D

Planning and Coordination:

- **Law Enforcement Coordination:** Identify potential swatting targets and verify service requests.
- **Contact Information:** Collect contact info and develop verification processes (e.g., code words).
- **Information Sharing:** Share data with neighboring jurisdictions and state agencies to identify common elements. Update LEEP with critical data (was the number spoofed, if so what number, originating location etc.,)

TransUnion

APCO 2025

TransUnion’s Comprehensive Strategy to Combat Swatting

2025

Agenda

1. Introduction
2. STIR/SHAKEN Overview & Global Trust Lab
3. Trusted Call Solutions
4. Branded Call Display

STIR/SHAKEN & Global Trust Lab

STIR/SHAKEN is comprised of a standard and framework

STIR
(Secure Telephone Identity Revisited)

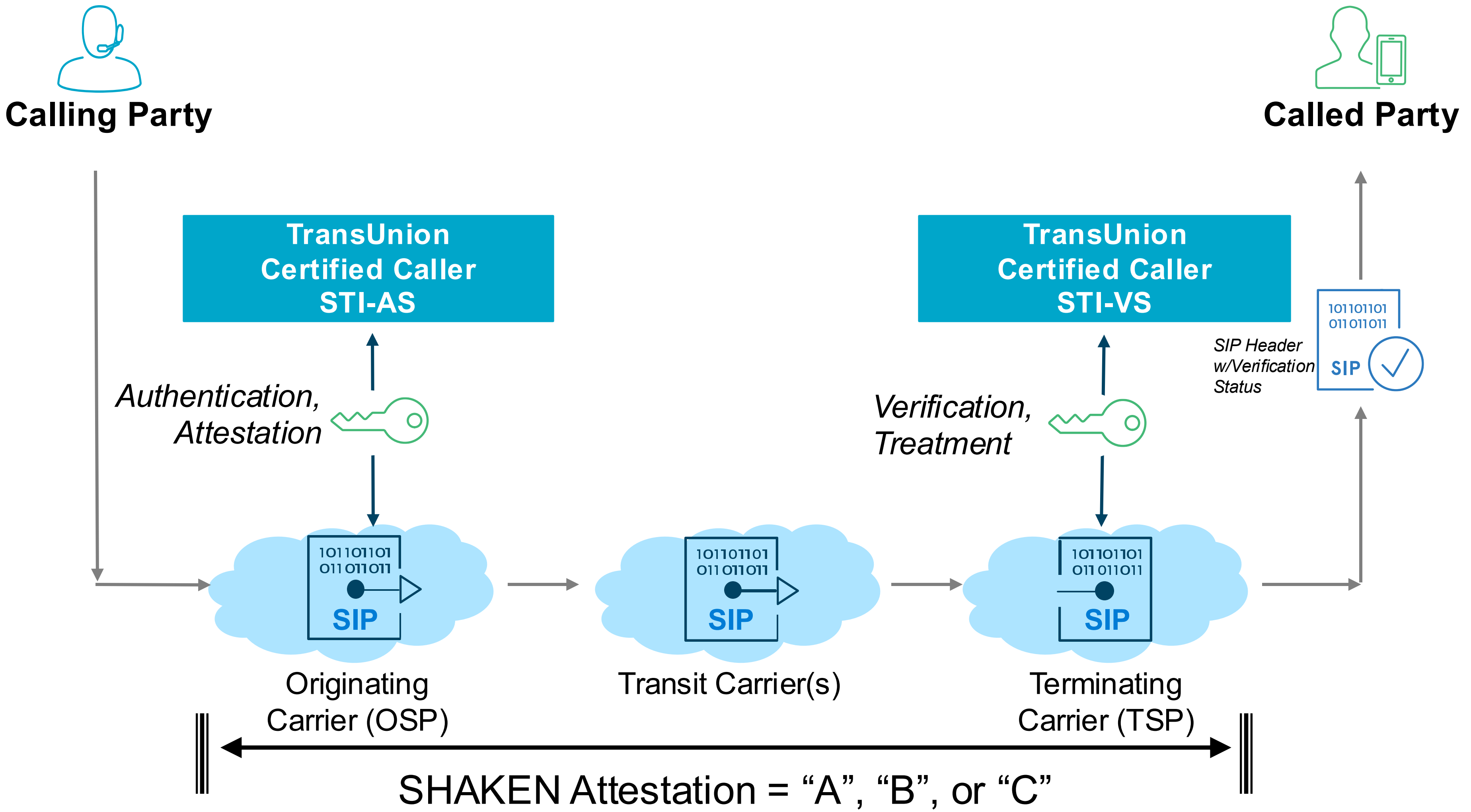
SHAKEN
(Signature-based Handling of Asserted information using toKENs)

Use certificates to identity legitimate calls, spoofed / fraud calls and enable traceback.

- Key RFCs (TransUnion co-author of each)
  - RFC 8225 – Defines the identity token, the Personal Assertion Token (or PASSporT)
  - RFC 8224 – Defines authenticated identity management in the Session Initiation Protocol (SIP)
  - RFC 8226 – Defines secure telephone identity credentials and credential management systems for support call authentication

- Key Specs (TransUnion contributor to each)
  - ATIS-1000074-E – Defines SHAKEN
  - ATIS-1000085 – Defines the support of "div" PASSporT
  - ATIS-1000080-E – Defines the governance model and certificate management
  - ATIS-1000084-E – Defines operational and management consideration for SHAKEN STI CA's

STIR/SHAKEN enables call authentication through an advanced cryptographic security methodology


Calling Party
Called Party
TransUnion Certified Caller STI-AS
TransUnion Certified Caller STI-VS
Authentication, Attestation
Verification, Treatment
SIP Header w/Verification Status
101101101 011011011
SIP
101101101 011011011
SIP
101101101 011011011
SIP
101101101 011011011
SIP
Originating Carrier (OSP)
Transit Carrier(s)
Terminating Carrier (TSP)
SHAKEN Attestation = “A”, “B”, or “C”

Attesting calls via STIR/SHAKEN enables traceback and reduction of nuisance calls

Traceback Process for Malicious Voice Traffic

- This is a network-based process that begins with the terminating service provider (TSP) receiving malicious voice traffic originating from a network that is not native to their own.
- Once calls are signed, traceback becomes feasible. The call is then methodically traced back through each non-native network in the call path, in reverse chronological order, until either:
- The originating party is identified, or
- The process encounters an uncooperative TSP along the path.

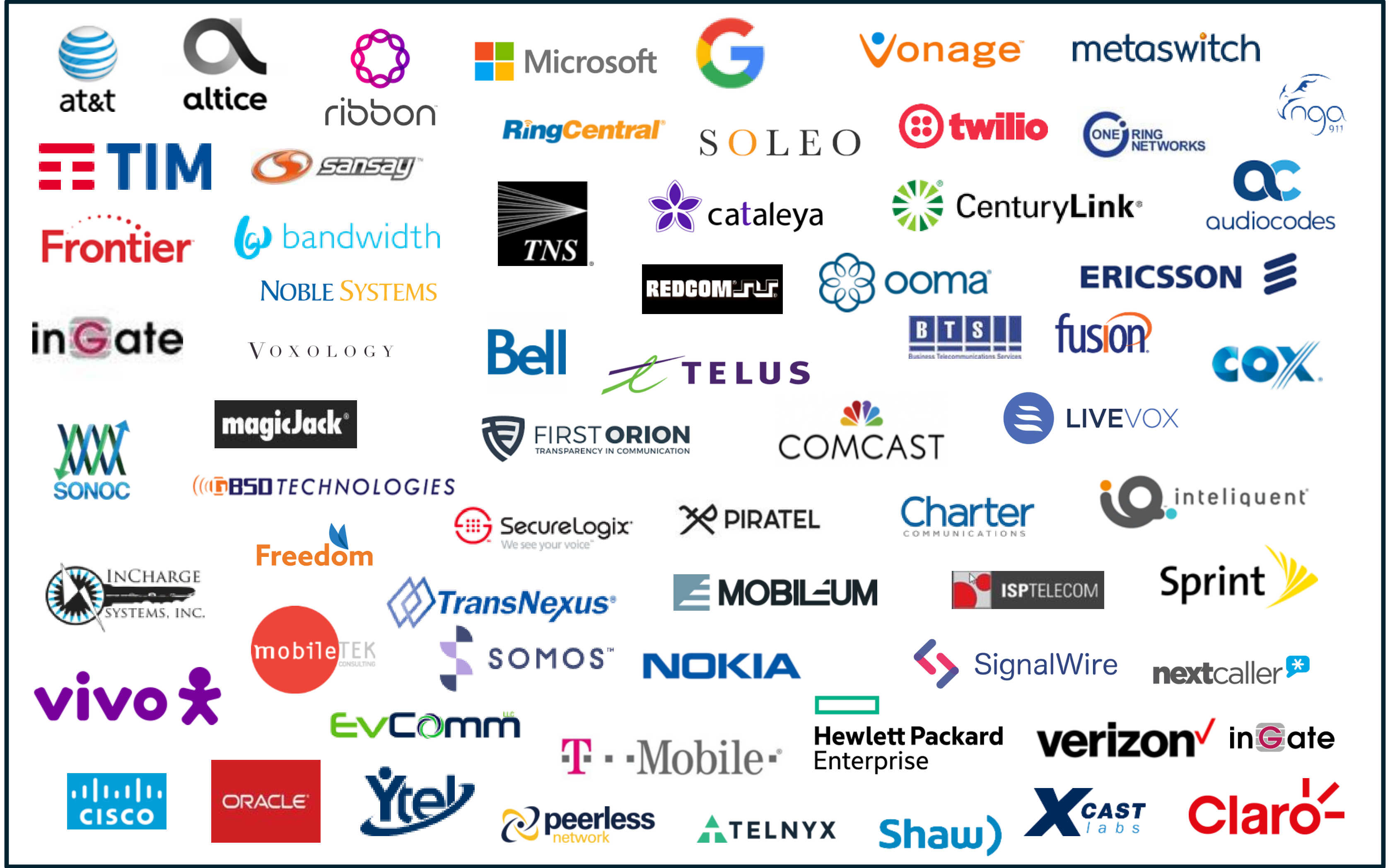
In layman's terms:

Going backward through the multiple carriers that a call traverses until we identify where it originated

TransUnion manages industry testbeds around the world to encourage and accelerate industry adoption

~100 Registered Global Trust Lab Test Participants

As of May 2025



- TransUnion is the exclusive provider of the ATIS Robocalling Testbed since Feb 2017, helping carriers and suppliers STIR/SHAKEN deadlines.
- Recently launched testbeds in Brazil and India
- Expanded to support emerging standards including Out-of-Band for TDM, Rich Call Data; and international interoperability.
- Tested with carriers from the following countries:

1. Brazil
2. Canada
3. China
4. India
5. Malaysia
6. Singapore
7. South Africa
8. U.K.

Trusted Call Solutions

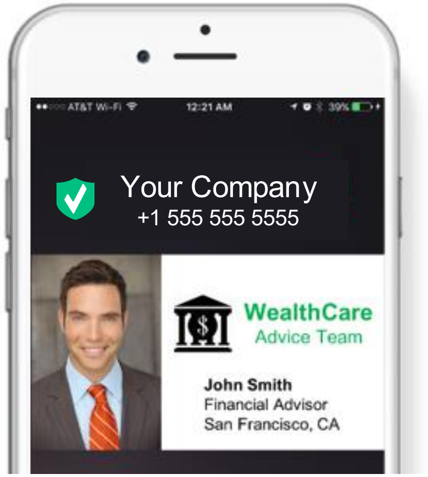
TransUnion's suite of Trusted Call Solutions consists of highly complementary products to help carriers and enterprises restore trust

AT&T Wi-Fi
12:21 AM
39%
Your Company
+1 555 555 5555

Caller Name & CN Optimization

Accurately display personal/business name on outbound calls.

Ensure identity & protect against blocking/mislabeling.



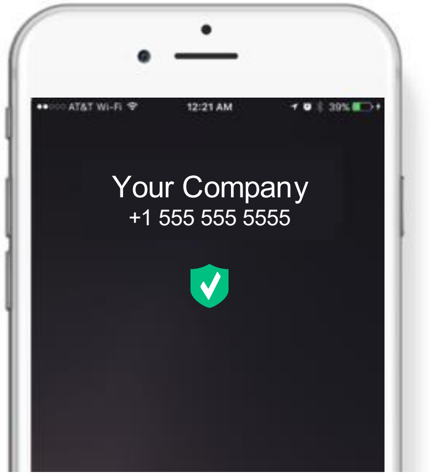
Branded Call Display (BCD)

Personalize mobile screens for contextual and branded customer call experience.

AT&T Wi-Fi
12:21 AM
39%
Spam Likely
+1 555 555 5555

Nuisance Call Mitigation

Apply rules & analytics to detect, block, or warn consumers, agents, and employees of illegal and unwanted calls.



Call Authentication (STIR)

Digitally sign outbound calls to battle spoofing and assure customers of the legitimacy of calls.

Applies to Carriers as well as to Enterprises.

Identity Vetting

Branded Call Display

Once trust in calling is restored, identity services, such as Branded Calling, can be enabled, transforming the call experience

1	Nationwide platform to manage call brand across major carriers
MM	Leverage STIR to enable extensive reach to consumer devices
90%	Reduction in improper call blocking & tagging
>50%	Increase in call answer rates
$$$	Enables carriers to recoup call authentication investment into new revenue

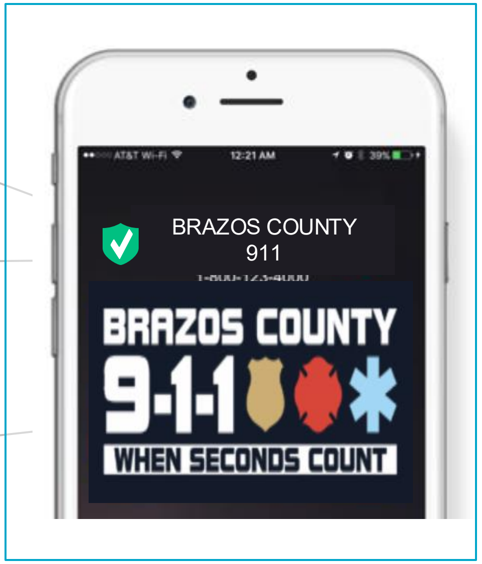
Branded Call Display (BCD) transforms the call experience by delivering verified caller information natively over the network–app required. This is valuable for emergency call-backs, as it clearly identifies the call as coming from 911. When citizens recognize the source, they are significantly more likely to answer, even during a crisis.

When consumer is called

The checkmark ✓ assures users that the call is certified end-to-end, and phone number has not been spoofed.

The caller name and phone number are vetted, registered and published by the service

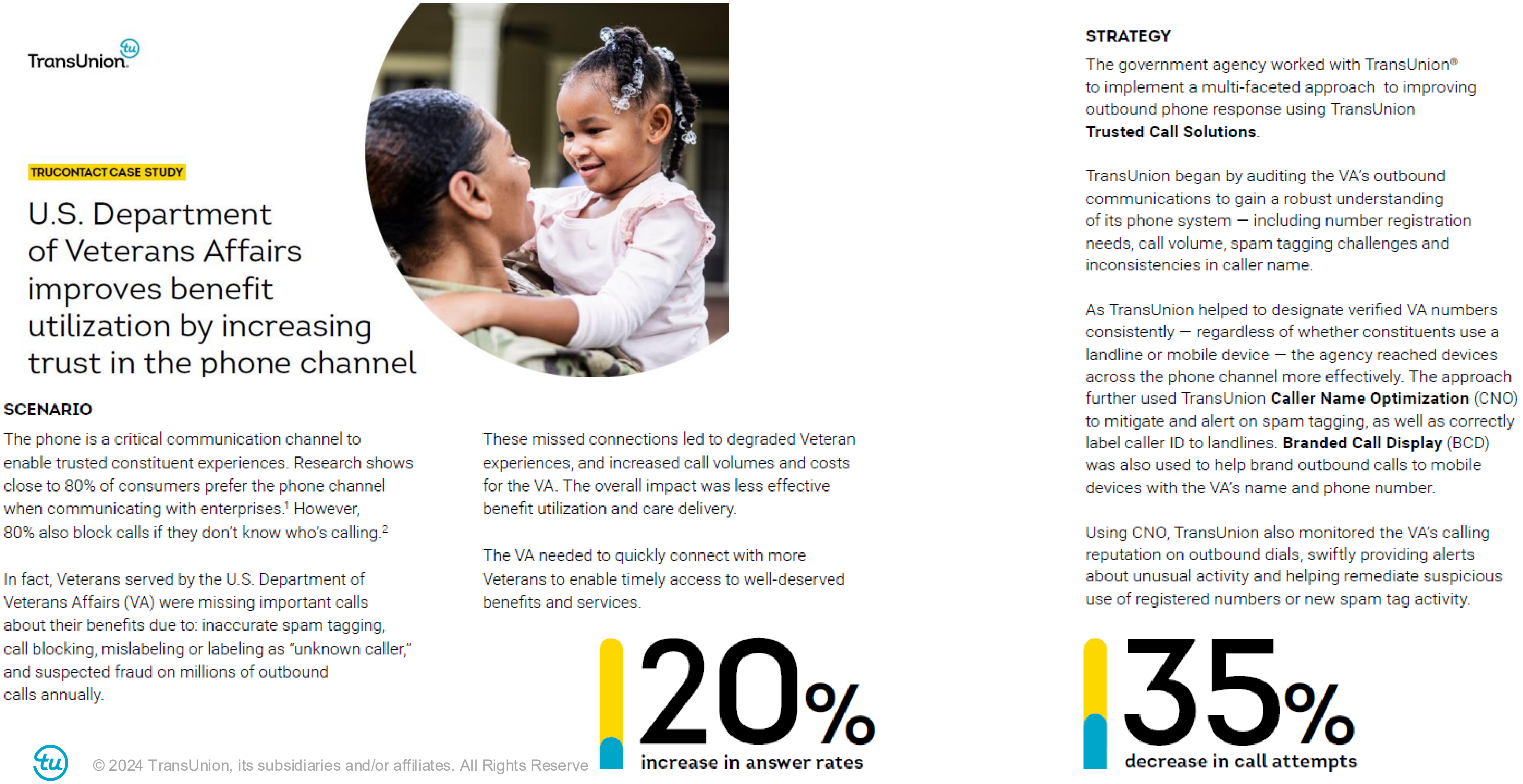
Logo are vetted, managed and centralized by the service



Personalize mobile screens for contextual and branded customer call experience.

Branded Call Display impact at the U.S. Department of Veterans Affairs

Click Here: U.S. Department of Veterans Affairs Improves Benefit Utilization by Increasing Trust in the Phone Channel | TransUnion



TransUnion

TRUCONTACT CASE STUDY

U.S. Department of Veterans Affairs improves benefit utilization by increasing trust in the phone channel

SCENARIO

The phone is a critical communication channel to enable trusted constituent experiences. Research shows close to 80% of consumers prefer the phone channel when communicating with enterprises.[1] However, 80% also block calls if they don't know who's calling.[2]

In fact, Veterans served by the U.S. Department of Veterans Affairs (VA) were missing important calls about their benefits due to: inaccurate spam tagging, call blocking, mislabeling or labeling as "unknown caller," and suspected fraud on millions of outbound calls annually.

These missed connections led to degraded Veteran experiences, and increased call volumes and costs for the VA. The overall impact was less effective benefit utilization and care delivery.

The VA needed to quickly connect with more Veterans to enable timely access to well-deserved benefits and services.

20% increase in answer rates

STRATEGY

The government agency worked with TransUnion® to implement a multi-faceted approach to improving outbound phone response using TransUnion **Trusted Call Solutions**.

TransUnion began by auditing the VA's outbound communications to gain a robust understanding of its phone system — including number registration needs, call volume, spam tagging challenges and inconsistencies in caller name.

As TransUnion helped to designate verified VA numbers consistently — regardless of whether constituents use a landline or mobile device — the agency reached devices across the phone channel more effectively. The approach further used TransUnion **Caller Name Optimization** (CNO) to mitigate and alert on spam tagging, as well as correctly label caller ID to landlines. **Branded Call Display** (BCD) was also used to help brand outbound calls to mobile devices with the VA's name and phone number.

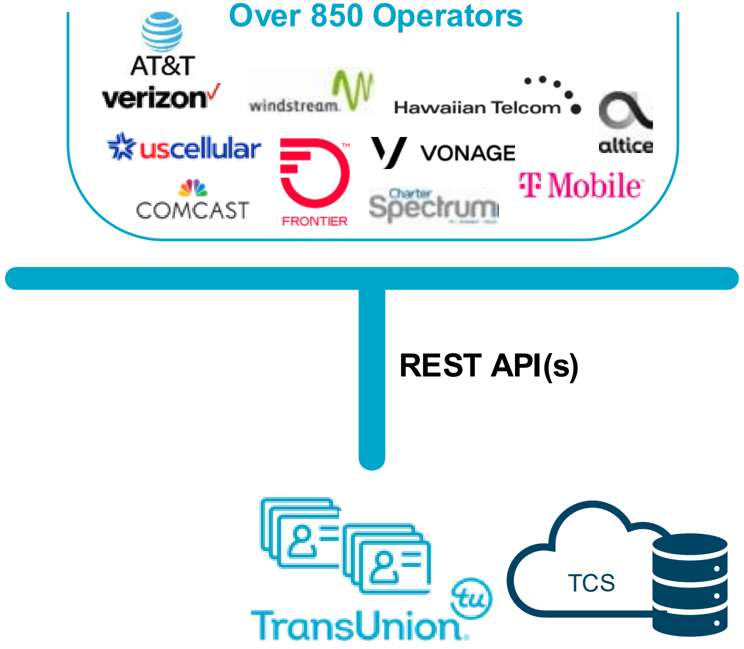
Using CNO, TransUnion also monitored the VA's calling reputation on outbound dials, swiftly providing alerts about unusual activity and helping remediate suspicious use of registered numbers or new spam tag activity.

35% decrease in call attempts

Trusted Call Solutions Caller Identification Services

STORAGE

Step 1
Carrier provisions CNAM/BCD data into Trusted Call Solutions Platform (TCS)

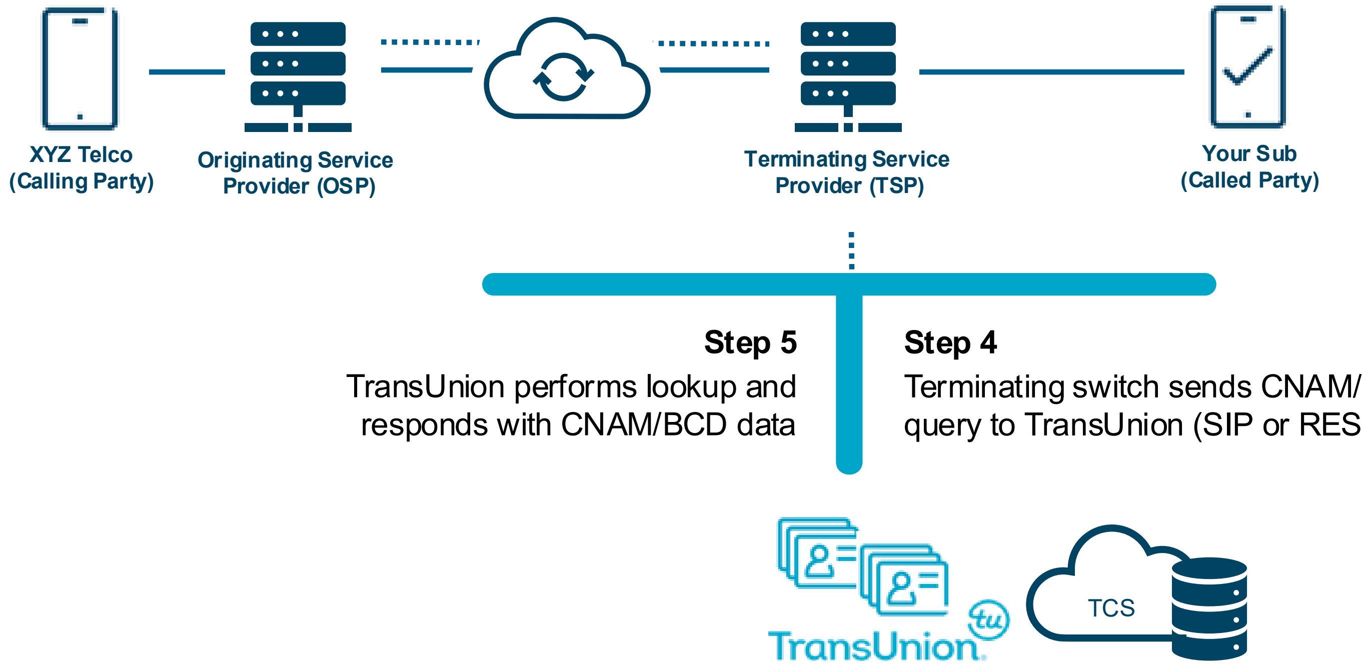


DELIVERY

Step 2
Call initiated

Step 3
Terminating switch receives call

Step 6
Terminating switch sends CNAM/BCD info for display



Step 5
TransUnion performs lookup and responds with CNAM/BCD data

Step 4
Terminating switch sends CNAM/BCD query to TransUnion (SIP or REST API)

“SINGLE SOURCE OF CALLING NAME TRUTH” FOR CARRIERS – OVER MANY YEARS

Collaborative Interoperability Testing with Texas A&M

- We are currently in discussions with Texas A&M to establish a connection between our lab and their system.
- This connection will enable other vendors to perform interoperability testing with our lab via the Texas A&M platform.
- The goal is to ensure seamless communication and compatibility across different systems.
- This initiative will help identify and resolve potential issues early in the development and deployment process.
- The collaboration will streamline the testing process for all participating stakeholders, improving efficiency and outcomes.

Questions?

Contact us to learn more: Scott.Straub@transunion.com
TransUnion.com/TruContact

2025

CENTER FOR APPLIED
COMMUNICATIONS AND NETWORKS

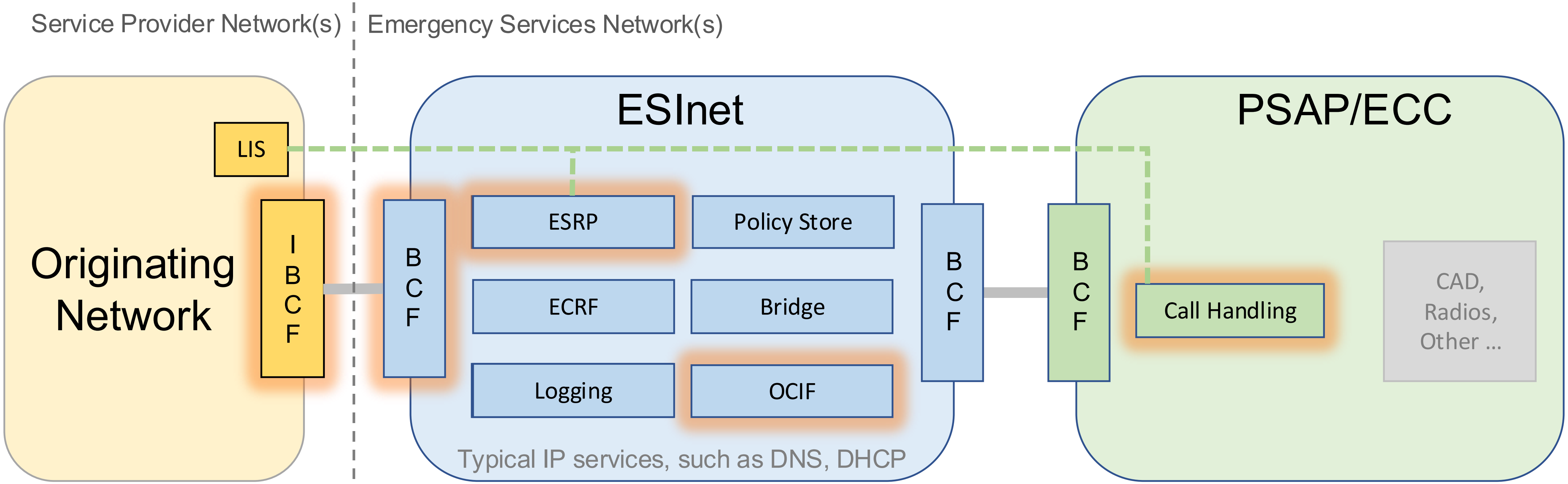
STIR/SHAKEN for NG9-1-1
A (very) Brief Introduction

APCO 2025

Michael E Fox, Executive Director, CACN

michael.fox@tamu.edu

NG9-1-1 Architecture: "Functional Elements"



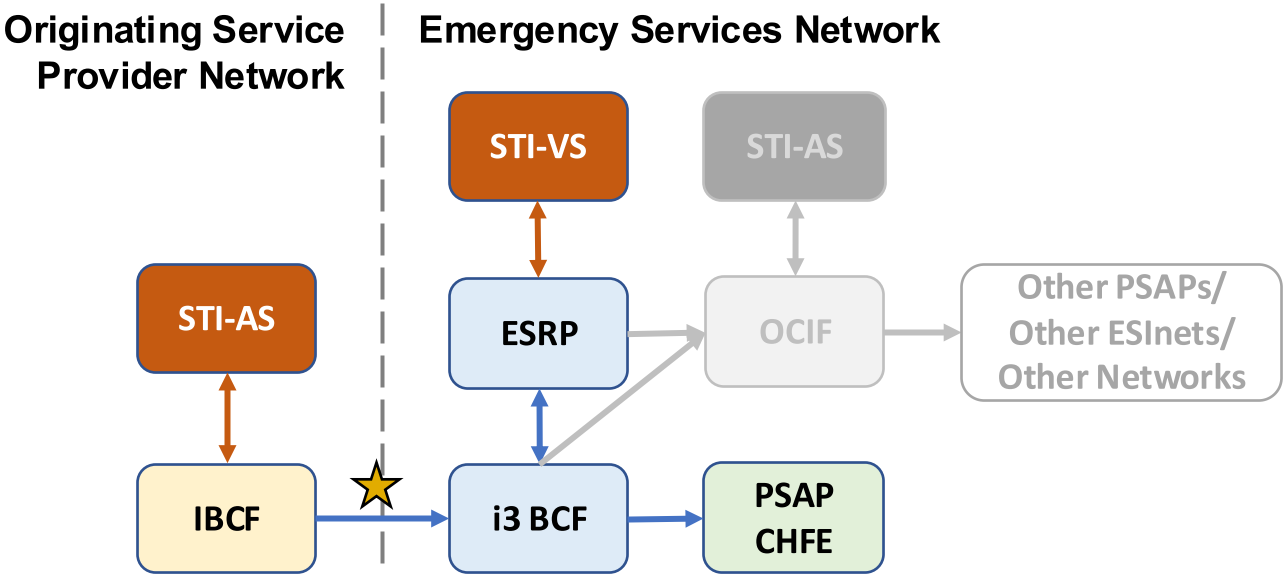
LIS = Location Information Server
IBCF = Interconnecting Border Control Function

ESInet = Emergency Services IP Network
BCF = Border Control Function
ESRP = Emergency Services Routing Proxy
ECRF = Emergency Call Routing Function
OCIF = Outbound Call Interface Function

PSAP = Public Safety Answering Point
ECC = Emergency Communications Center
CAD = Computer Aided Dispatch

STIR/SHAKEN for INbound NG9-1-1 Calls

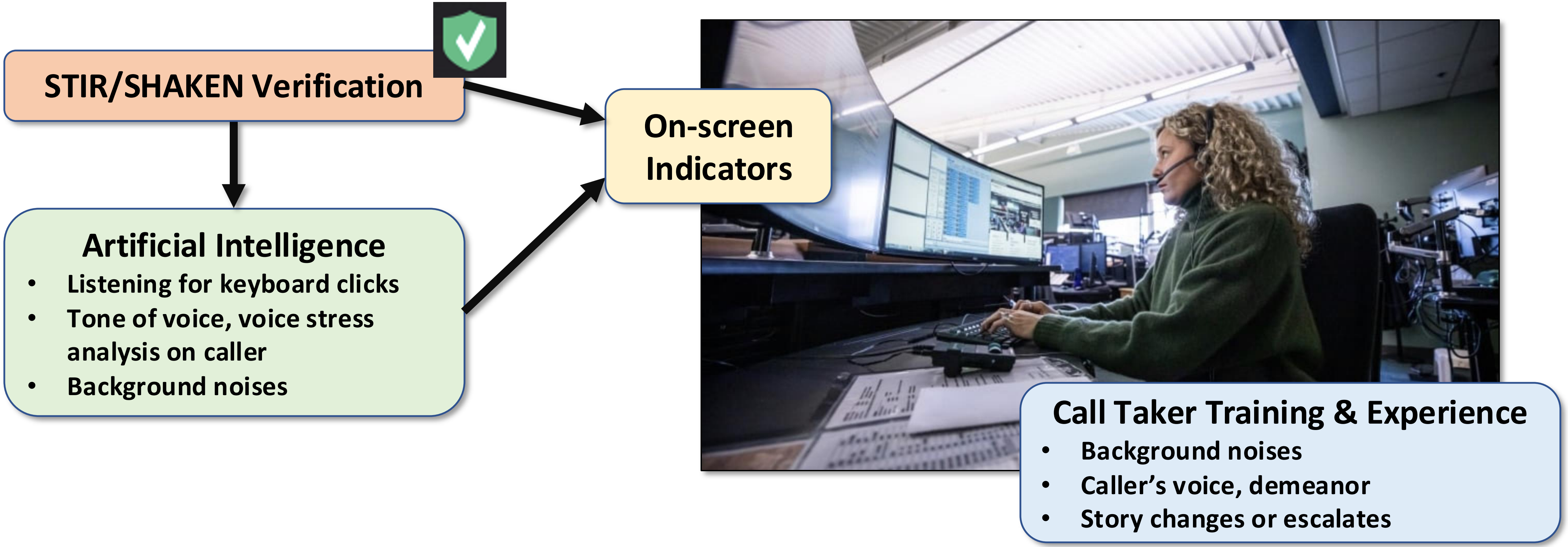
- Originating service provider performs Authentication function prior to sending call to ESInet
  - Full PASSporT info is passed with call to ESInet★
- ESRP performs Verification function
- ESRP performs call processing (location- & policy-based routing)
- ESRP sends call to the appropriate PSAP with “verstat” information


Originating Service Provider Network
Emergency Services Network
STI-AS
IBCF
STI-VS
ESRP
i3 BCF
STI-AS
OCIF
PSAP CHFE
Other PSAPs/ Other ESInets/ Other Networks

STI-AS	Secure Telephone Identity Authentication Service
STI-VS	Secure Telephone Identity Verification Service
[I]BCF	[Interconnection] Border Control Function
ESRP	Emergency Services Routing Proxy
OCIF	Outbound Call Interface Function
PSAP	Public Safety Answering Point
CHFE	Call Handling Functional Element

Is This Incoming Call Real?

STIR/SHAKEN and other tools can help with decision making



STIR/SHAKEN Verification

Artificial Intelligence
- Listening for keyboard clicks
- Tone of voice, voice stress analysis on caller
- Background noises

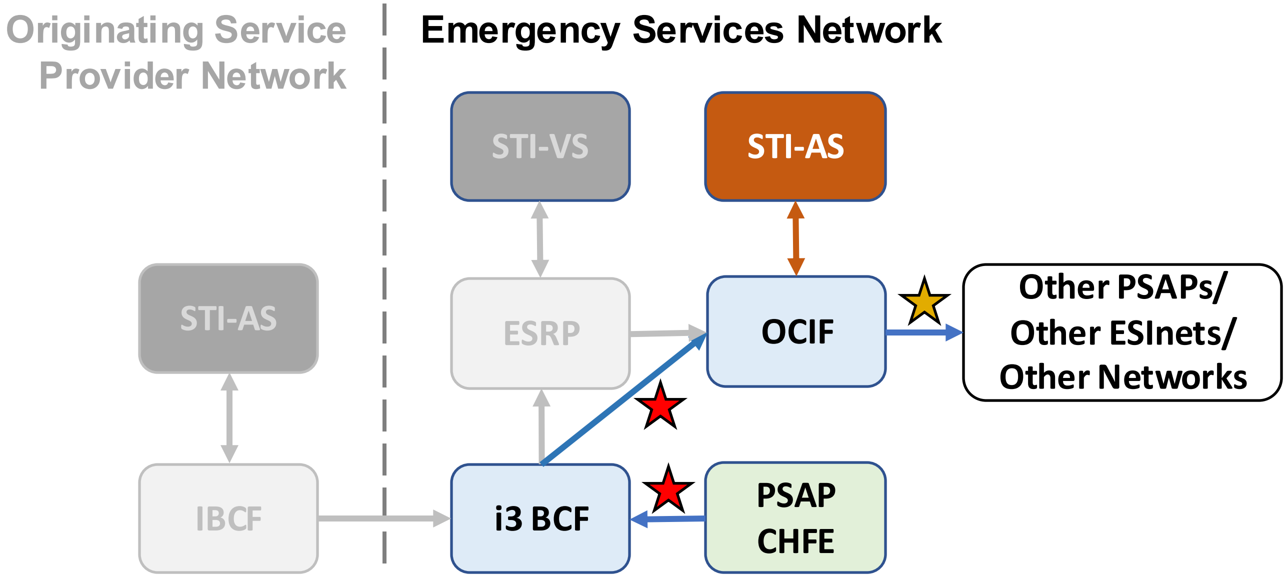
On-screen Indicators

Call Taker Training & Experience
- Background noises
- Caller’s voice, demeanor
- Story changes or escalates

STIR/SHAKEN for OUTbound NG9-1-1 Calls

(Example: Callbacks, Follow-ups, Transfers)

- PSAP initiates outbound call
  - Draft: PASSporT info is included ★
- OCIF invokes the STI-AS after call processing is completed (after interconnected network has been determined)
- OCIF sends the call toward the destination
  - Full S/S PASSporT info is included ★
- Can also include Rich Call Data

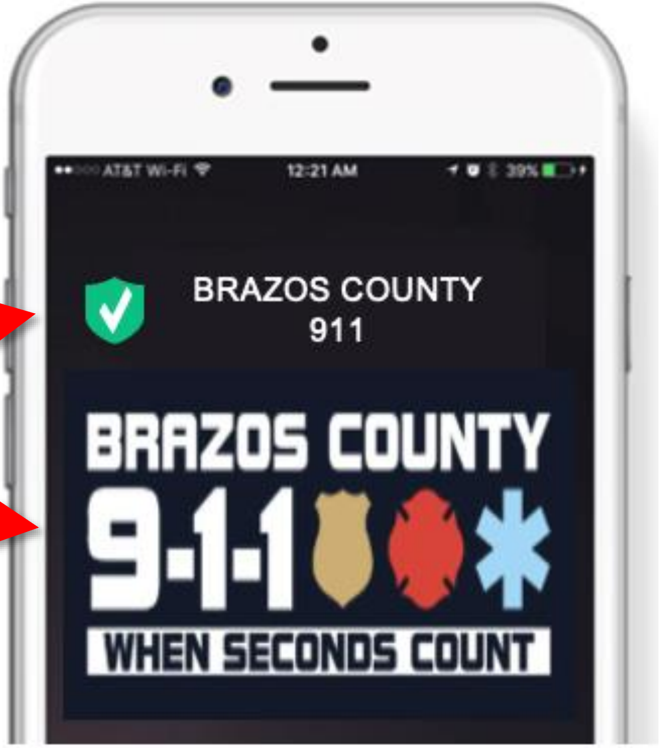


Originating Service Provider Network
Emergency Services Network
STI-AS
IBCF
STI-VS
ESRP
i3 BCF
STI-AS
OCIF
PSAP CHFE
Other PSAPs/ Other ESInets/ Other Networks

STI-AS	Secure Telephone Identity Authentication Service
STI-VS	Secure Telephone Identity Verification Service
[I]BCF	[Interconnection] Border Control Function
ESRP	Emergency Services Routing Proxy
OCIF	Outbound Call Interface Function
PSAP	Public Safety Answering Point
CHFE	Call Handling Functional Element

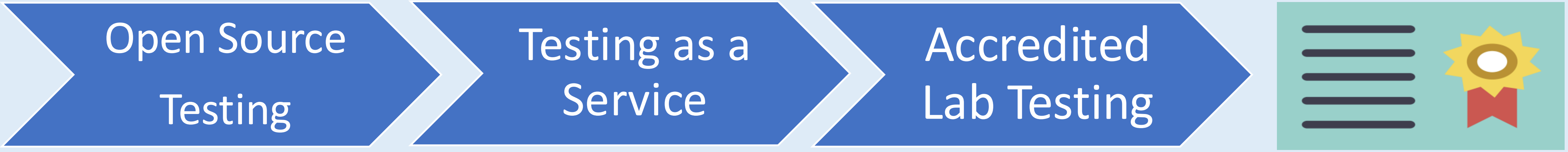
Will My Outbound Call Be Answered?

- Transfers to other PSAP/ECCs
- Callbacks and follow-ups to the RP
  - They may be in distress; disinclined to be interrupted
- Call Handling FE can show identity
  - STIR/SHAKEN verification of authenticity
  - Rich Call Data helps called party decide quickly
    - Neustar calls this "Branded Call Display"
- Or, privacy can be invoked, if desired



Will My NG9-1-1 System Do This?

- **DHS** is funding efforts in **NG9-1-1 Interoperability Testing** and **Cybersecurity Testing**
  - University of Illinois Critical Infrastructure Resilience Institute
  - Texas A&M Center for Applied Communications and Networks
- **Texas A&M** is building the test system to verify that NG9-1-1 components conform to the NG9-1-1 standards, are interoperable with each other, and are secure



Open Source Testing

- Free
- Use as often as needed
- Integrate into QA process
- Save time/resources
- Eliminate uncertainty & ambiguity
- Limited user interface
- Need SW dev skills

Testing as a Service

- Adds …
- Cloud-based, scalable, accessible
- Web-based UI
- Configuration management
- Extensive logging
- Reporting formatted for certification
- Affordable: subscription, pay per test models

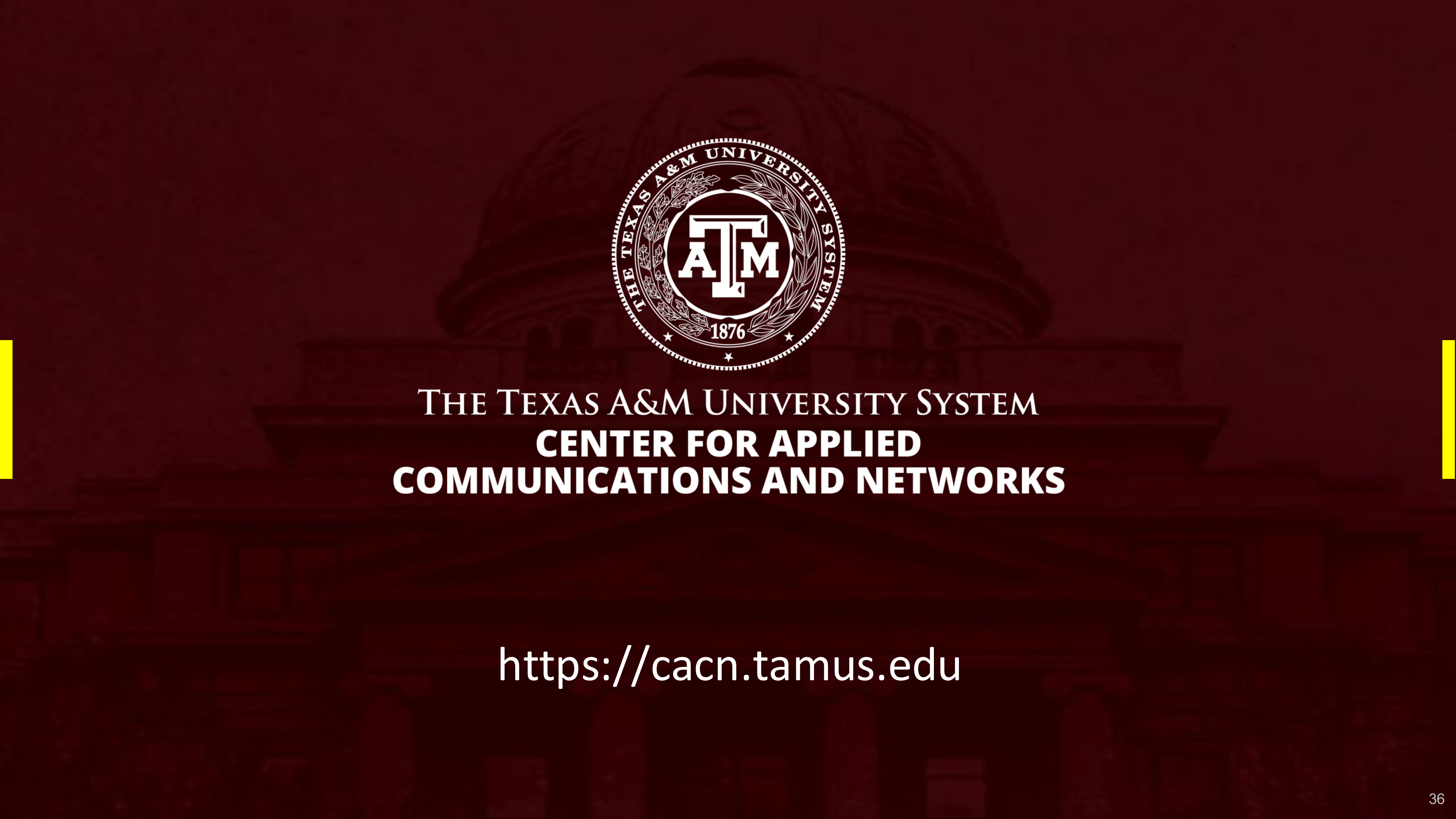
Accredited Lab Testing

- Adds …
- Tests run by ISO 17025 accredited lab
- No surprises
- Consistent and dependable process
- Confidential results
- Digitally co-signed test report
- NG9-1-1 system buyers can require in their RFPs!

- Vendor submits report to certifying agency
- Agency verifies info, posts to their website
- Vendor products are eligible for purchase using federal grant funds

STIR/SHAKEN and NG9-1-1

- STIR/SHAKEN is a key requirement in the NG9-1-1 standard
- Helps to identify legitimate vs. spoofed calls
- Inbound calls: helps call takers decide how to handle the call
- Outbound calls: increases likelihood of calls being answered



THE TEXAS A&M UNIVERSITY SYSTEM

CENTER FOR APPLIED COMMUNICATIONS AND NETWORKS

https://cacn.tamus.edu