Caller ID Spoofing and Call Authentication Technology

MODERATOR:

Kati Daffan, FTC

PANELISTS:

Henning Schulzrinne, FCC
Adam Panagia, AT&T
Patrick Cox, TrustID
Vijay A. Balasubramaniyan, Pindrop Security

ROBOCALLS
ALL THE RAGE

Henning Schulzrinne

Chief Technology Officer
Federal Communications Commission

ROBOCALLS
ALL THE RAGE

Caller ID spoofing

Caller ID Act of 2009: *Prohibits any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.*

Henning Schulzrinne, Federal Communications Commission

Number authentication

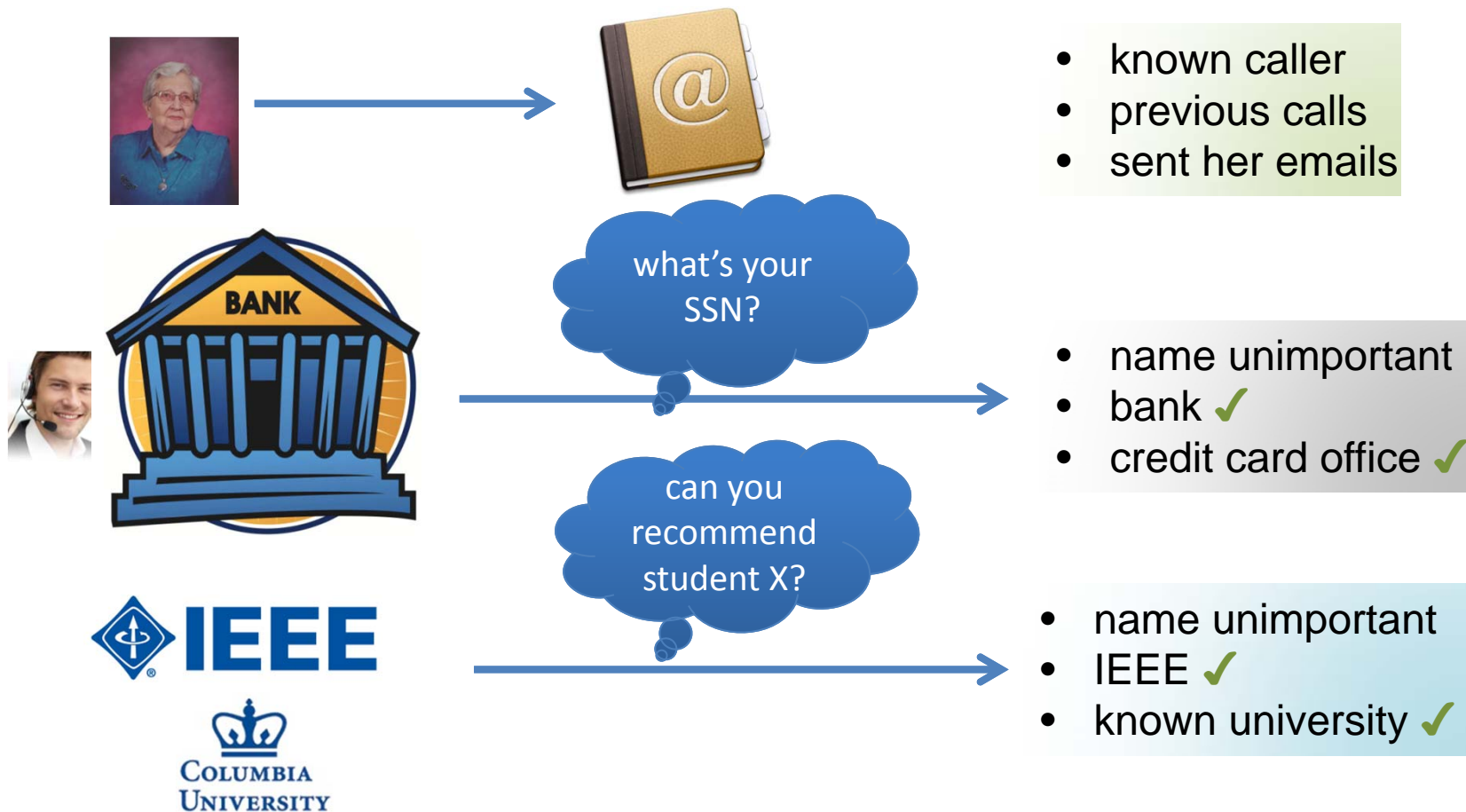```
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.net>
Contact: <sip:alice@pc33.example.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
```

RFC 3893 (2004)

public-private key pair
provided with phone number

# Caller identification



- known caller
- previous calls
- sent her emails

what's your SSN?

- name unimportant
- bank ✓
- credit card office ✓

can you recommend student X?

- name unimportant
- IEEE ✓
- known university ✓

ROBOCALLS
ALL THE RAGE

# Attribute validation

**Attribute Validation Server (AVS): Issuer**
e.g., fcc.gov

{Alice's username, credentials, user ID, role}

**Attribute Reference ID (ARID)**
https:/fcc.gov/4163

3. Validates ARID with access code and retrieves selected attributes (e.g., Alice's role)

1. Requests an ARID, selecting attributes to disclose

HTTP over TLS
SIP over TLS

2. Makes a call with the ARID and part of access code

**Caller: Principal =** *Alice*
Employee of fcc.gov
tel:+12345678

**Callee: Relying Party =** *Bob*
Accepts calls from members in *.gov; does not know Alice's phone number

draft-ono-dispatch-attribute-validation

# Adam Panagia

## Director
## AT&T Network Fraud Investigations

ROBOCALLS
ALL THE RAGE

# Caller ID Spoofing and Call Authentication Technology

**Current legislation prohibits Caller ID spoofing if the intent is to defraud, cause harm, or wrongfully obtain anything of value.**

**Historically spoofing required an advanced knowledge of telephony equipment and could be quite expensive**

**Spoofing is now available to the amateur due to the availability of open source software. The cost and the effort have been drastically reduced; thus decreasing the barrier to entry which has resulted in significant increases in the incidents of malicious large scale spoofing events**
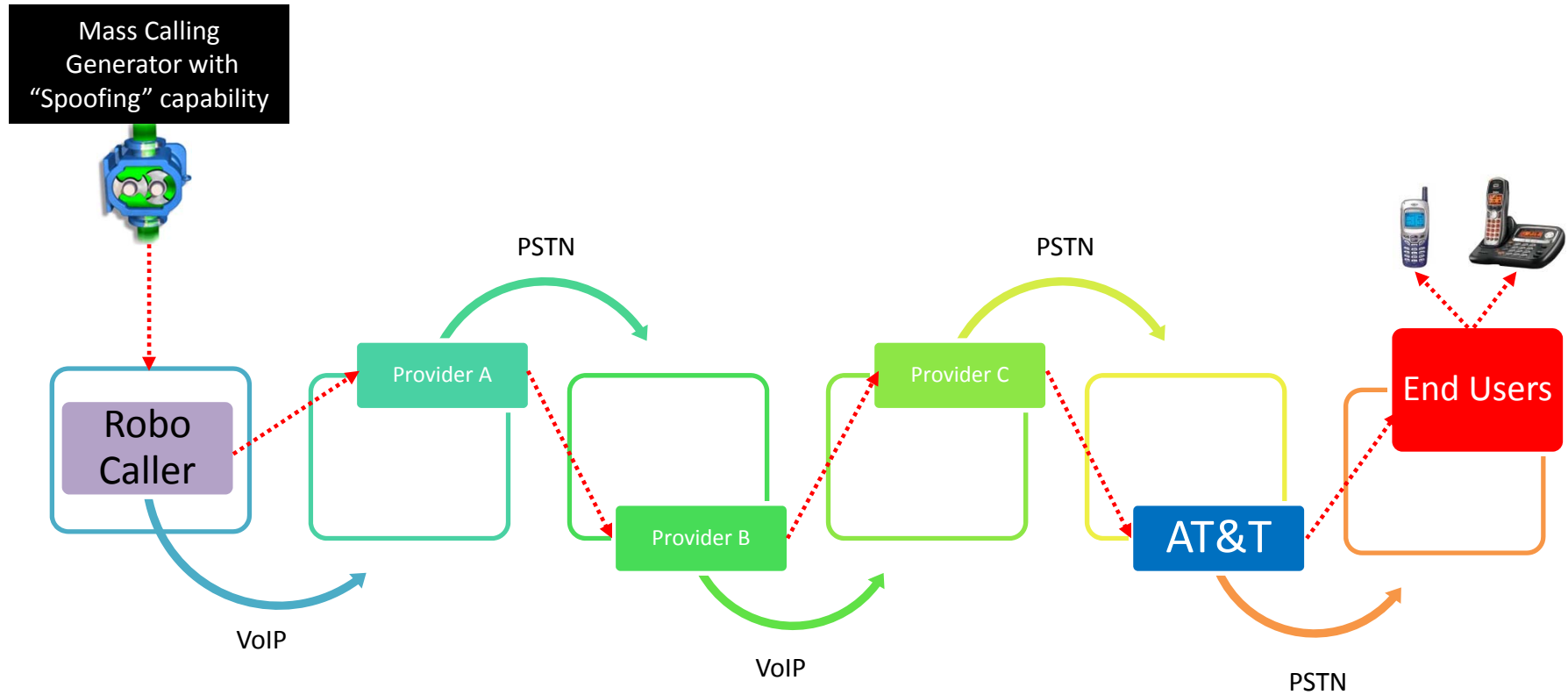
**There are currently no available solutions in the Public Switched Telephone Network that completely "eliminate" this risk**
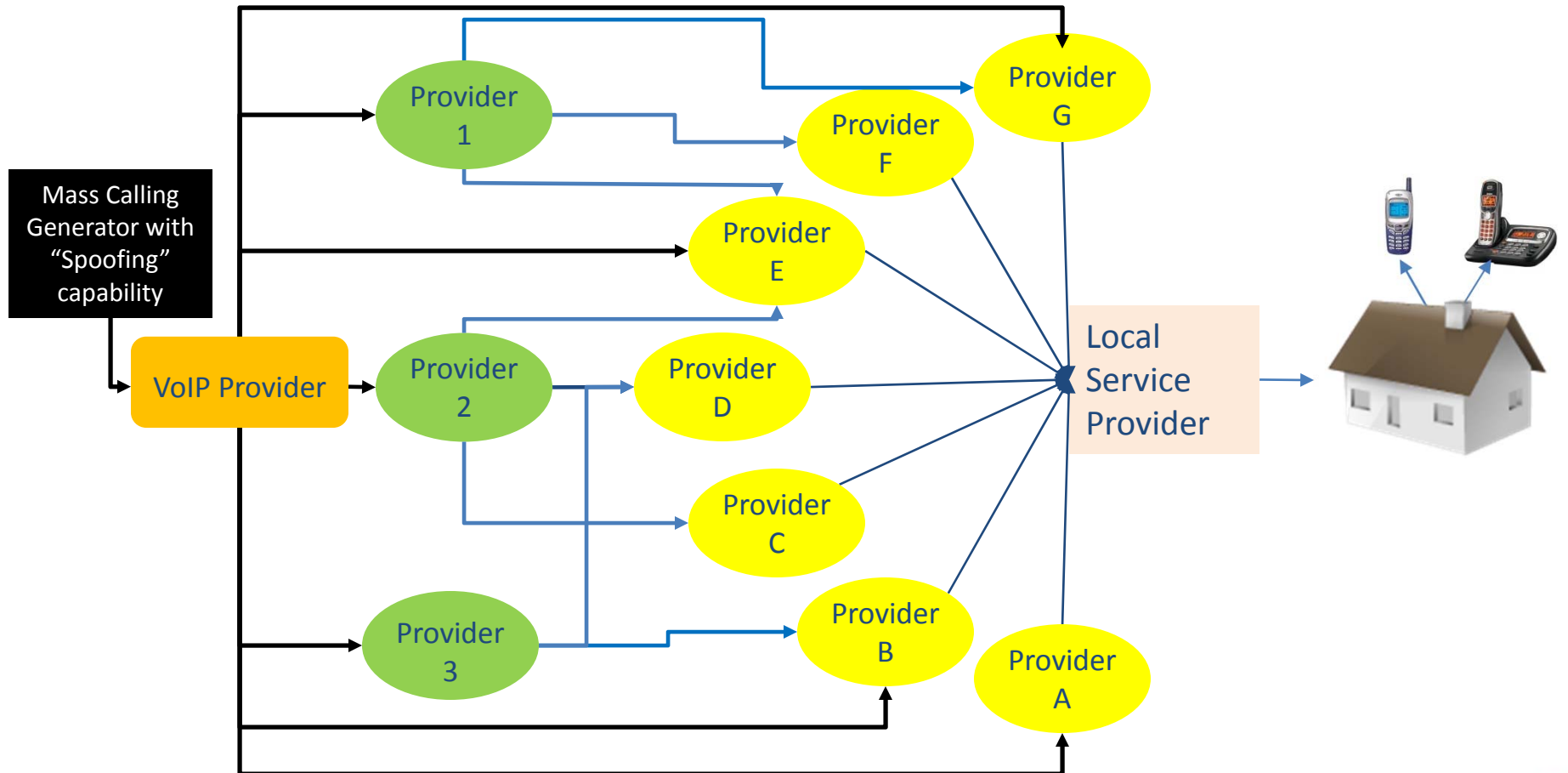
# "CALLER ID SPOOFING"

The practice of sending false or misleading information, so as to deceive the receiving party and/or hide the caller's true identity and/or call origination.

# Robo Call Flow

Mass Calling Generator with "Spoofing" capability

Robo Caller

Provider A

PSTN

Provider B

VoIP

Provider C

PSTN

AT&T

VoIP

PSTN

End Users

# Terminating Call Distribution Call Flow

# Patrick Cox

## CEO
## TrustID

*Who is **TRUSTID** and why are they represented at the FTC Robocall Summit?*

# TRUSTID technology enables businesses to <span style="color:orange">**Serve Customers**</span>, **Not Criminals**
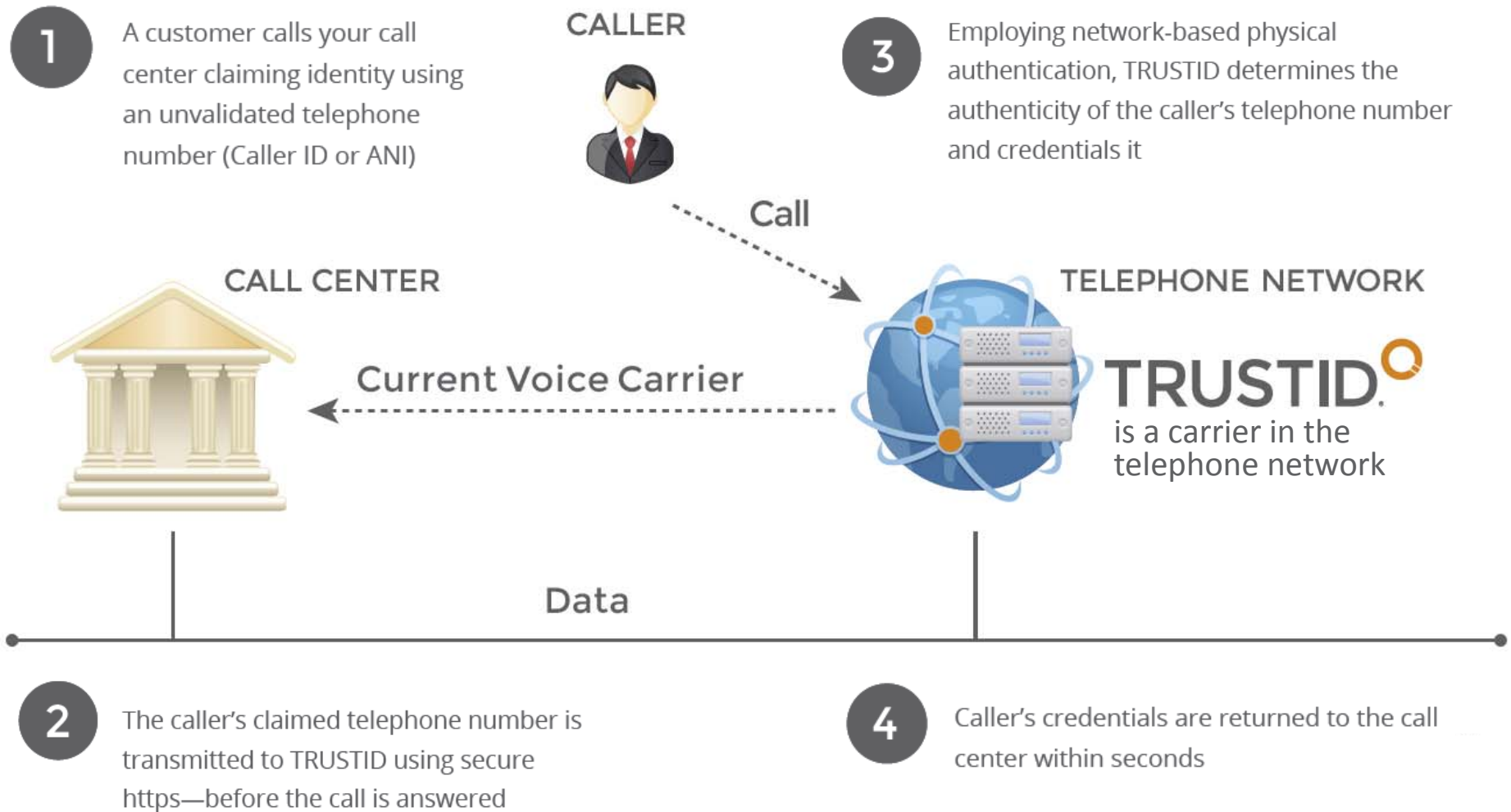
- TRUSTID credentials Caller ID and ANI, so that companies will know with certainty
  - who is *really* calling them before they answer
  - in an undetectable way
  - that stops spoofers from causing mayhem
  - and protects customer and company assets

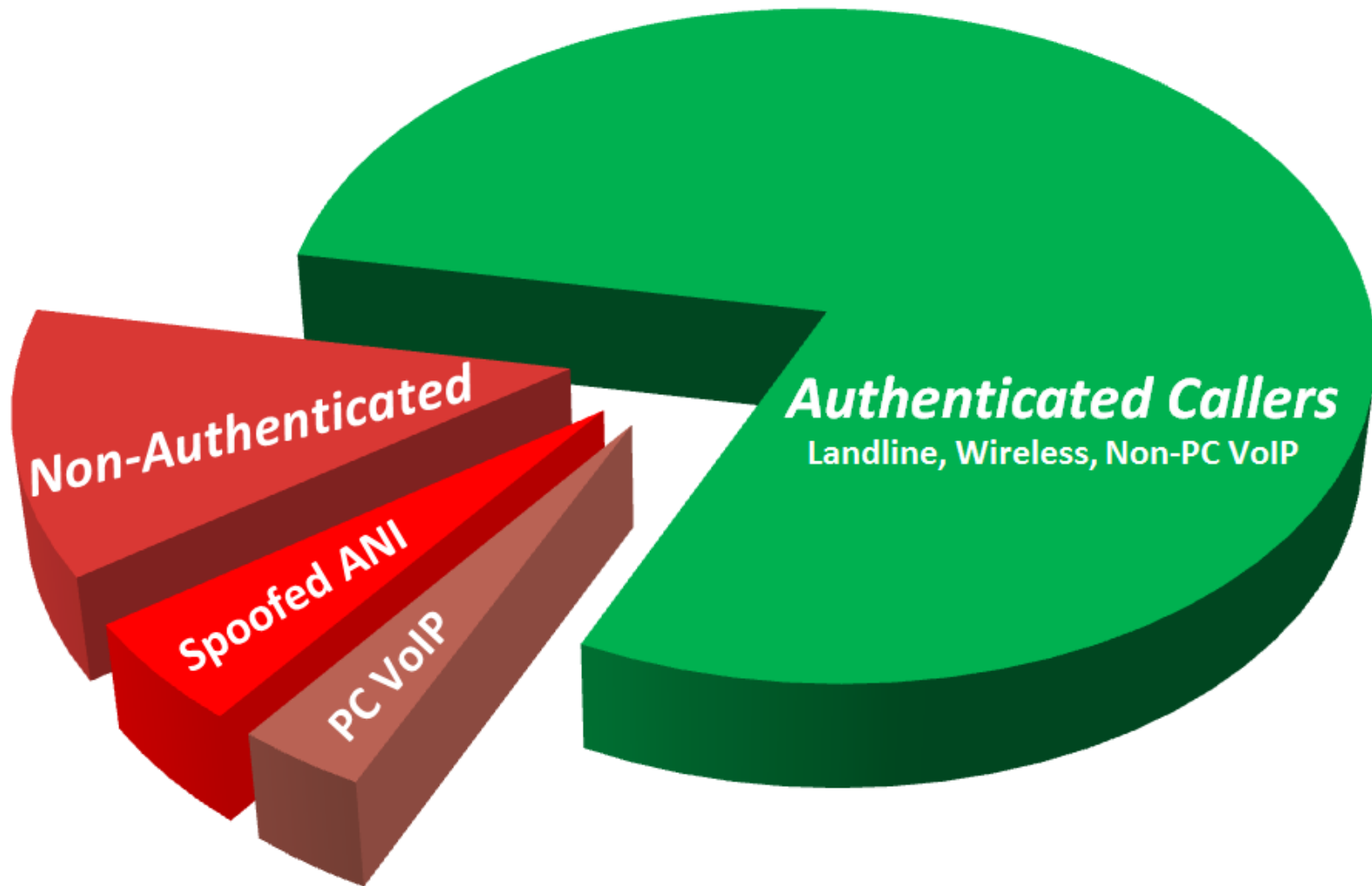*Why does my Caller ID sometimes show my Bank calling, when they aren't?*

Up to about 2004, Caller ID was mostly trustworthy

- That changed when the Internet and the telephone-network became deeply connected

- Now, anybody in the world with an Internet connection & basic computer skills controls Caller ID

- Threats to telephone-network security now resemble Internet security threats

## HOW TRUSTID AUTHENTICATION WORKS

**1** A customer calls your call center claiming identity using an unvalidated telephone number (Caller ID or ANI)

**CALLER**

**3** Employing network-based physical authentication, TRUSTID determines the authenticity of the caller's telephone number and credentials it

Call

**CALL CENTER**

**TELEPHONE NETWORK**

Current Voice Carrier

**TRUSTID.**
is a carrier in the telephone network

Data

**2** The caller's claimed telephone number is transmitted to TRUSTID using secure https—before the call is answered

**4** Caller's credentials are returned to the call center within seconds

*TRUSTID's technology value is in the **green** calls*



Non-Authenticated

Spoofed ANI

PC VoIP

**Authenticated Callers**
**Landline, Wireless, Non-PC VoIP**

*Can TRUSTID stop spoofing on my home phone too?*

- TRUSTID technology requires the line types (i.e. PRI) and PBX equipment that businesses use and will not work for consumers today
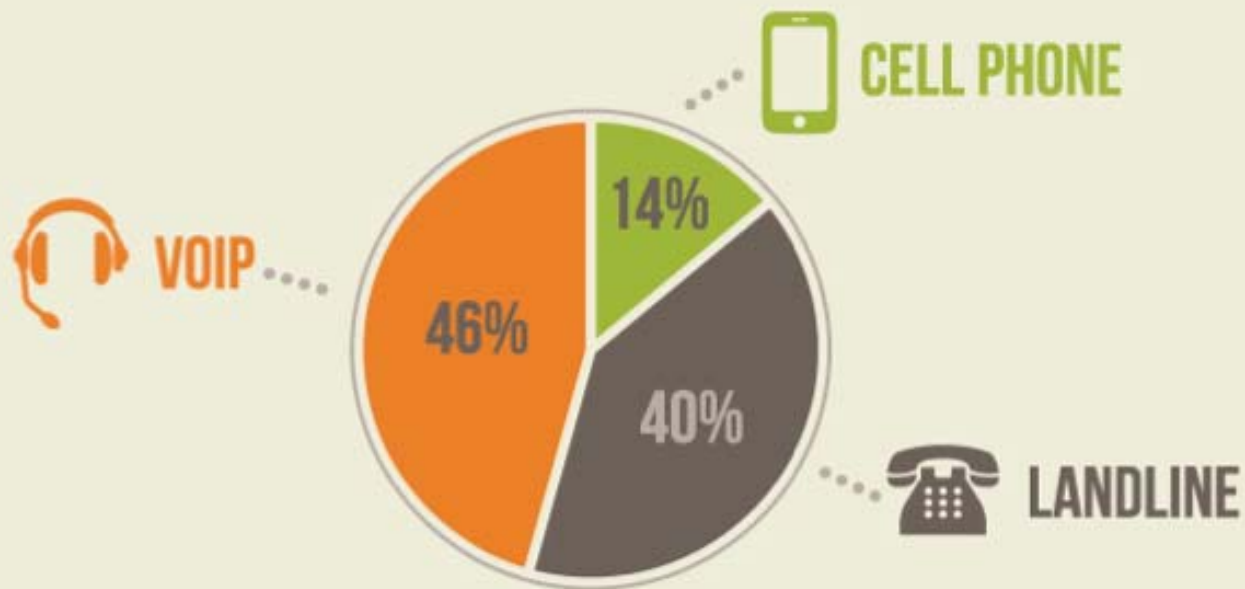
**Vijay Balasubramaniyan, PhD**
**CEO & Co-founder**
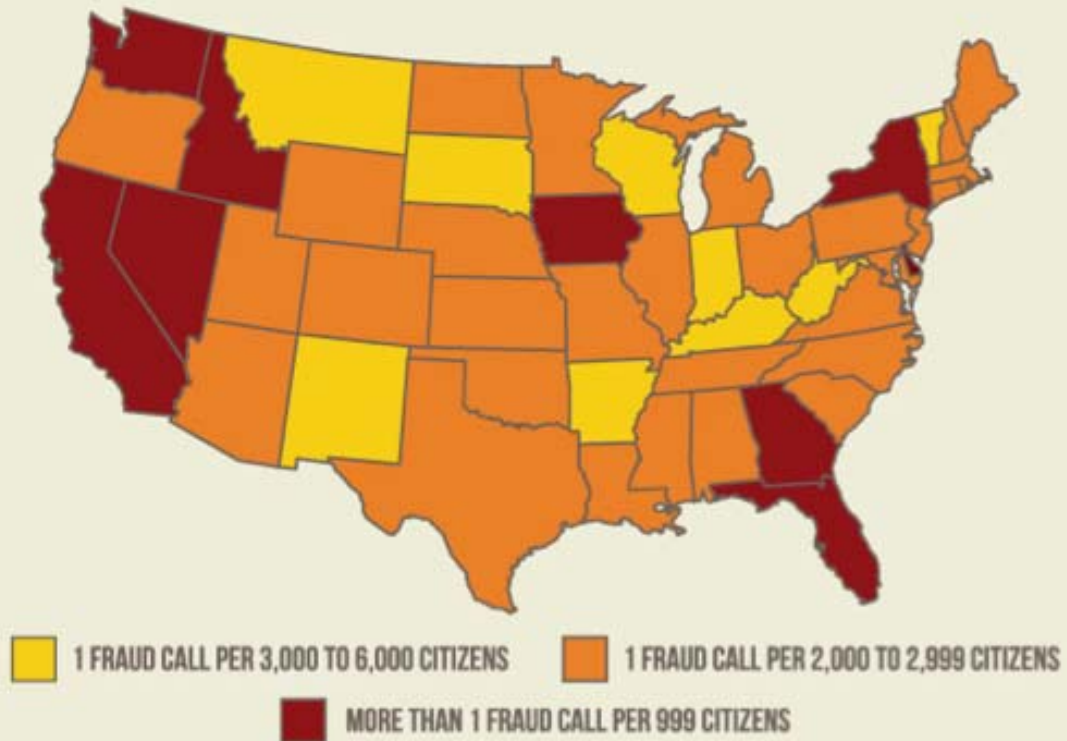**Pindrop Security**

# State of Fraud Report

# State of Fraud Report

# State of Fraud Report



FRAUD CALLS HAPPEN EVERYWHERE
FREQUENCY OF ATTACK BY STATE PER CAPITA

1 FRAUD CALL PER 3,000 TO 6,000 CITIZENS
1 FRAUD CALL PER 2,000 TO 2,999 CITIZENS
MORE THAN 1 FRAUD CALL PER 999 CITIZENS

# The Phone Channel Is Vulnerable

☐ **Caller ID** is easily spoofed

☐ **VoIP** makes it **cheap** and **easy** to call globally

☐ **No metadata** transmitted – only data is audio signal
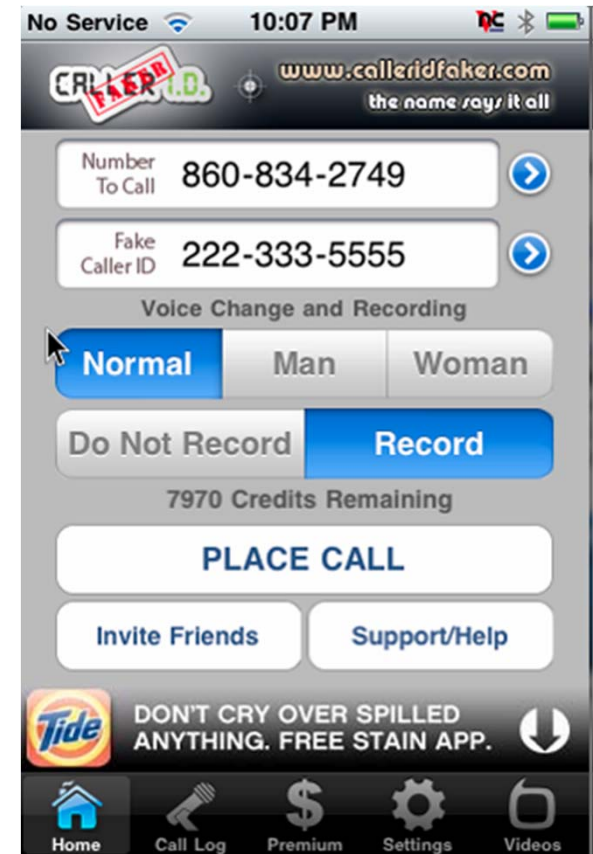


*There's an App for that!*

# Multi-layered Defense

| Known Attackers | New or Unknown Attackers | Authentication |
|---|---|---|
| Blacklist | Geography | Phone type | Caller ID |

# Acoustic Fingerprinting

ROBOCALLS
ALL THE RAGE

Call Audio

| LOSS | NOISE | SPECTRUM | VOICE |
|---|---|---|---|
| • Packet loss<br>• Robotization<br>• Dropped frames | • Clarity<br>• Correlation<br>• Signal-to-noise ratio | • Quantization<br>• Frequency taggers<br>• Codec artifacts | • Timbre<br>• Range<br>• Obfuscation |

*Acoustic Fingerprint*

RISK SCORE

Phone Type

Geo-location

Known Fraud Caller

| Ok | Caution | Risky | Alert |
|---|---|---|---|

25%  50%  75%

90

# Protecting the Phone Ecosystem