Is Your Branded Caller ID Solution Secure?

Wednesday, Oct. 19, 2022
11:30 a.m.–12:30 p.m. Eastern Time

Patrick Rea
Manager of Product Management for Hiya Connect
Most networks depend critically on authentication and protection layers to function.
Hiya Connect

**Branded Call**
Display your identity to engage with more people, faster

**Secure Call**
Pre-authentication of caller identity that stops spoofers

**Call Analytics & Insights**
Call delivery & performance reports with key KPIs

**SaaS-based User Console**
Self-serve management of number identity and rich analytics
How can a call recipient trust the display being shown represents a legitimate call?

- **Urgent**
  - Emergency?
- **Wanted**
  - Expected call?
- **Nuisance**
  - Spam call?
- **Fraud**
  - Extortion?

Blue Sky Insurance
+1 (646) 762-9160
New York, NY

Reminder to show up to your scheduled appointment.

- **79%** of unidentified calls go unanswered.
- **77%** of consumers will answer an identified call.
- **94%** of consumers believe unidentified calls may be fraud.
5 questions network providers should ask when evaluating Branded Caller ID solutions
Does the solution provider have a method to prevent scammers from branding calls?
Why is verifying company legitimacy and connection to the enterprise important?

- Bad actors take advantage of lenient processes
- Two recent examples:
  - The Federal Unemployment Benefits program
  - The Economic Injury Disaster Loan program
- $45B impact
- Both programs had some element of self-certification, essentially the “Honor System.”
- The individual could claim to be unemployed and receive a check with no verification.
- A business could claim to have been hurt or closed their business and receive relief without showing any proof.

To have a branded call product that is resistant to bad actors you cannot use the “Honor System”
Scam trends in the USA during 2022

Scammers…

- Are continuously looking for victims
- Know their victims
- Know what tricks are more likely to work

Recent scam trends, include:

- Healthcare
- Utilities
- Hurricane relief
- Student loan debt relief
- Credit card
- More!
Additionally, intermediaries matter!
2

Does the solution provider have a method of validation that ensures enterprises have the right to brand identity on given TNs?
As we see in CNAM, bad actors can pretend to be you

- Very easy to add a display name to your phone number that:
  - does not correspond to your brand
  - for which you do not own the trademark

- CNAM does not go through all the checks and reviews that a branded call experience does

- Carriers are viewed as “on the hook” to protect subscribers from misleading/wrong displays
3

Is there a way to protect valued brands from having their number (and name) hijacked?
STIR/SHAKEN is not enough, more is required

78% of calls go unsigned

Spoofers can easily spoof your number and show up with your branded identity

A secure, branded calling experience can prevent bad actors from using enterprise brands or spoof their numbers

Source: TransNexus
Secure Call

TRUST
- Authenticate calls with a fraud filter that verifies legitimate calls

IDENTITY
- Protect your identity by terminating unverified calls, applying a warning or stripping identity before call is completed

INTELLIGENCE
- Know how much potential spoofing is occurring on your numbers and if those calls are being answered or not
4

Are there protocols in place to prevent unauthorized users from being able to change identity?
Ensure the enterprise account can’t be hijacked

**Issues when unauthorized users gain access:**

- Displays can be changed by unauthorized users
- Employees who shouldn’t have access can edit/delete phone numbers and displays
- Lost the ability to audit changes to your account

User

Admin

Unauthorized user
Is a system in place to moderate content that is displayed?
Beyond the honor code, checking each phone display is important or else...

YTD 2022 Hiya has disapproved 14.55% of the displays submitted
5 questions network providers should ask when evaluating Branded Caller ID solutions

1. Is there a method to prevent scammers from branding calls?

2. Is there a method to ensure enterprises have the right to brand identity on given TNs?

3. Is there a way to protect valued brands from having their number (and name) hijacked?

4. Are there protocols in place to prevent unauthorized users from being able to change identity?

5. Is a system in place to moderate content that is displayed?
Thank you!

Check out hiya.com/solutions/carriers

Email us at carrier@hiya.com for more information!