Protecting Communications from Identity Spoofing

Presented by Numeracle & YouMail Protective Services

ABOUT THIS WHITEPAPER

This whitepaper interprets the potential consumer harm caused by illegal call and illegal brand spoofing that occurs when fraudulent actors use your business' information without your consent or awareness. We identify how this is done and how to protect your brand from the illegal use of your identity information through number reputation solutions, voice traffic monitoring, and KYC.

Plus, with the addition of branded calling as the newest layer of identity presentation, protecting your calling identity is crucial for both successfully reaching customers and ensuring the protection of your brand and phone numbers.

Identity Spoofing: Calls

ILLEGAL CALL SPOOFING

A highly unethical and deceptive practice, illegal call spoofing incidents happen when a bad actor electronically alters a calling party's originating phone number to display a number that is different from the originating party's caller ID, without any authorization to display and use that phone number.

When a bad actor displays an altered number to end-users that belongs to *your* brand, your customers may not be able to tell the difference between calls truly originating from you versus calls originating from a fraudulent source, harming your reputation and scamming your customers.

However, there are legitimate and completely legal reasons for spoofing a phone number, like a pharmacy calling to alert a patient that a prescription is ready for pick-up and displaying the regional number of the local pharmacy instead of the corporate number actually originating the call. But these calls aren't seeking to harm you or your customers.

WHAT WE'RE DOING ABOUT IT

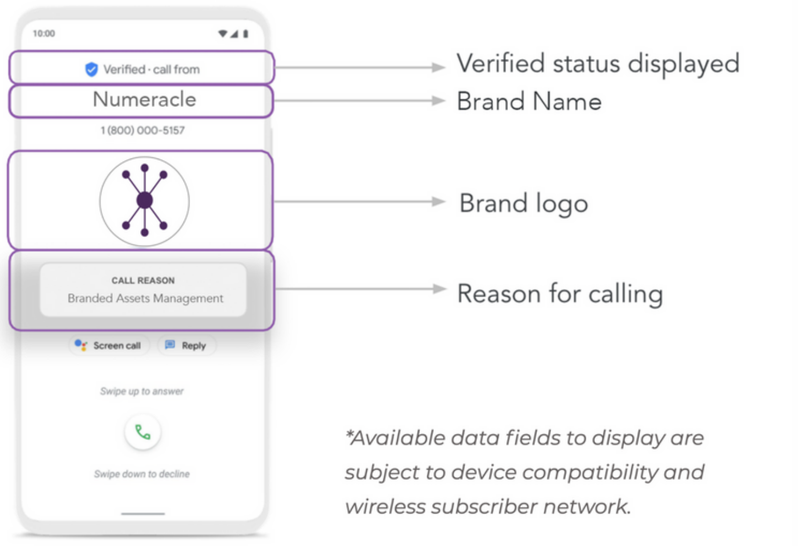
Numeracle prioritizes enterprise identity via a solution set that fully vets and verifies an entity's identity, either at the enterprise or voice service provider level, to authenticate the relationship between brand and phone number usage to protect number reputation.

YouMail Protective Services has designed a solution using AI-based algorithms and machine learning technology that creates a digital fingerprint to identify fraudulent brand representation taking place via illegal robocall campaigns as soon as it happens.

Identity Spoofing: Brands

ILLEGAL BRAND SPOOFING

The introduction of branded calling as the latest identity-enhancing technology has added a new presentation layer to the authentication of caller identity. It allows an enterprise to attach identity information like a brand name, logo, and customizable text describing the reason-for-call.



Available data fields to display are subject to device compatibility and wireless subscriber network.

This additional information is displayed on compatible end-user devices as a means of improving consumer trust with participating brands.

When used legally and properly, branded calling may also enhance consumer contact through improved call answer rates as well as post-call engagement.

While the end-user experience may vary depending on the network, solution, and device, a number of independent solutions have already entered the market, with call originators hungry to adopt the new technology as part of their dialing strategy.

The potential problem is that these solutions exist outside of the STIR/SHAKEN caller ID authentication standards, known as out-of-band solutions, meaning this data may be susceptible to brand spoofing by nefarious callers in potential call path gaps.

Without addressing vulnerabilities in how branded calling solutions deliver branded information, bad actors may be able to steal more than just phone numbers and enhance how they impersonate brands by using stolen logos to confuse and scam consumers.

Identity Spoofing: Impact

IMPACT ON BRAND IDENTITY

Branded calling and brand identity go hand in hand. If nefarious actors are using (spoofing) your phone numbers and branded content, they are harming your brand's reputation as well as your consumers and clients. As this continues you'll likely notice the answer rates of your legitimate calls start to decline as a result.

YouMail

FROM THE YOUMAIL BLOG

How to Stop Brand Impersonation Via Voice Calls, Also Known As Vishing

"The victims of brand impersonation aren't just those who were called, but also those who were being impersonated. That may include the IRS, the local police, financial institutions, and major brands."

Enterprise Solutions – How to Protect Your Brand From Fraudulent Imposters

"Fraudsters impersonate people and organizations you would ordinarily trust, or at least hear out. The most common pose involves government agencies such as Social Security, Medicare or the IRS. But crooks might adopt any number of guises, including companies you do business with, charities, a family member or friend, a lawyer or debt collector, or celebrities."

Partnering to Tackle Identity Spoofing

Numeracle has partnered with YouMail Protective Services to provide a comprehensive identity spoofing solution for enterprises and carriers looking to shut down voice and SMS communications that would otherwise cause harm to brands.

YouMail Protective Services leverages an innovative array of technologies including AI, machine learning, content-based analytics, and audio fingerprinting via a SaaS-based solution that provides protection for enterprises.

They protect against brand imposters that damage enterprise reputation, causing lost business and additional operational expenses such as recompense payments to maintain good will.

They also provide robocall mitigation services for voice service providers and detection of unwanted traffic and blocking unlawful robocalls that would otherwise originate, transit or terminate on their networks.

NUMERACLE + YOUMAIL ARTICLE

Spoof Protection with Help from YouMail

A Robocall Mitigation Solution to protect subscribers from unwanted robocalls or spoofed calls, improve service quality, and eliminate costs and complaints.

Spoof attacks are almost always identified only *after* a bad actor has already caused brand damage. However, YouMail Protective Services leverages its Sensor Network to provide 24/7/365 monitoring of robocall campaigns for its enterprise customers to prevent and quickly react to any illegal spoofing.

This is a core part of their managed detection and response solution for brand protection, which facilitates early detection of fraudulent brand representation and expeditious mitigation and enforcement.

State of the Industry

GAPS IN STIR/SHAKEN

Led by the FCC, the industry has taken steps to reduce illegal spoofing activity via authentication methods like STIR/SHAKEN but, unfortunately, it isn't a silver bullet solution and it won't be completely reliable until it's fully implemented on both an intra-carrier and inter-carrier basis.

Smaller networks may struggle with TDM network “holes” that prevent the seamless SIP signaling needed to transfer STIR/SHAKEN data, which is then lost. This means VSPs signing call traffic via STIR/SHAKEN cannot be assured that the authenticated information of A-level Attestation calls will reach the terminating network or destination.

Plus, there are no mutually agreed-upon standards for the display of attestation levels on end-user devices and no path to educate consumers on what these levels even mean to understand the level of trust they can have in the identity that's calling.

Numeracle's Implementation Reports

Monitoring the Robocall Mitigation Database

1 June 30th - Sept 28th   **2** Post-September 28th   **3** Database Milestone

Yet another challenge remains in instances where STIR/SHAKEN is applied with consideration to the credentials of the number owner/call originator while the *content* of the calling campaign is actually managed by the entity that could be *leasing* the telephone number.

This causes an incongruence between the authentication of telephone numbers/networks and KYC of the entity actually using the telephone number. In other words, STIR/SHAKEN is not enough to prevent unwanted, or even unlawful, call campaigns. There is a need for telephone usage behavior monitoring.

TRUST GAPS IN BRANDED CALLING

Discrepancies in terminating call display leave room for doubt that the incoming call has, without a doubt, been properly vetted and verified. Branded calling technologies are simply avenues through which brand trust can be delivered to a consumer, but the technology itself does not actually *guarantee* trust because it comes down to *how* and *why* it is being used.

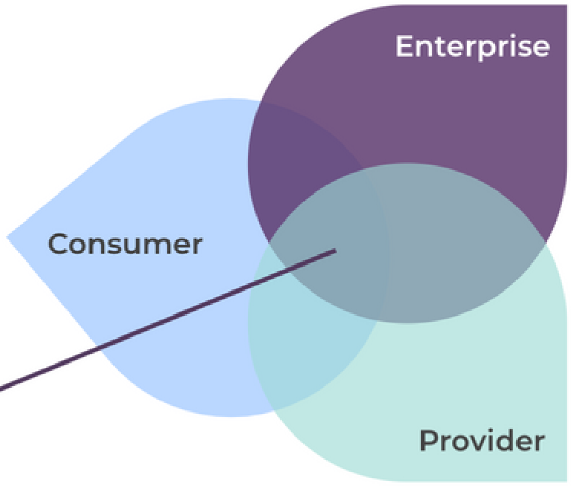
Since there is still no universal model, implementation framework, or set of approved standards for the implementation and delivery of branded calling assets, there are still many security concerns when it comes to storing and delivering precious brand data that may be vulnerable to identity spoofing.

Enterprise

The need to securely represent identity to the consumer

Consumer

The need to trust the identity of incoming calls



Trust is achieved when security is established from all three perspectives

Service Provider

The need to manage and secure identity across the network

In light of this industry progress, we must remain vigilant of how these technologies are being utilized and how consumers, enterprises, and providers are joining together to protect the recipients of these calls from scams while also protecting the legitimate brands that originate the calls from identity spoofing.

Measuring the Impact

CUSTOMER FRAUD

Bad actors spoofing your phone number or your complete brand identity may be scamming consumers while posing under your name.

*"If you're not doing everything in your power to stop them from getting scammed under your name — right or wrong — you will lose some business. When your customers suffer monetary fraud, it can expose your organization."**

EXPOSED BRAND REPUTATION

It can be difficult to recover from tarnished brand reputation, even if it wasn't your fault in the first place.

*"The price of this activity isn't just the amount picked from the pockets of customers, the damage to each brand's reputation is probably even more costly. The psychological damage of imposter scams creates an avalanche effect where customers can begin to associate your brand with the attacks."**

THE MARRIOTT CASE

Read the Marriott Case*, where the hotel company has filed a lawsuit "*seeking the disabling of robocall scams that violate consumers' rights and infringe upon Marriott's goodwill and valuable trademark rights*" after their name was improperly for telemarketing scams via illegal call and brand spoofing.

*"Without Marriott's authorization or consent, Marriott's valuable rights in its famous and distinctive MARRIOTT trademarks have been deliberately infringed upon through Defendants' unauthorized use of the MARRIOTT name and trademarks while telemarketing promotions via fraudulent robocalls."**

**Provided by YouMail Protective Services*

Measuring the Impact

DECLINE IN ANSWER RATES

Once your phone number or brand reputation has been harmed and you start to lose consumer trust, you may also notice a negative hit to your answer, contact, or callback rates.

*“That campaign you were hoping to launch to restore your name may not even get off the ground because formerly loyal customers are skeptical to pick up when you ring because they’re uncertain it’s really you and afraid to find out.”**

DRAIN ON RESOURCES

Trying to reinstate the reputation of your numbers and your brand identity can cause a significant drain on resources and expenses.

*“Now you’re trying to identify fraud sources, compile evidence, and file legal procedures — all amounting to a pretty penny. The cost of allowing your brand to be used in scams extends far beyond the initial fraud.”**

Four Reasons Why You Should Be Protecting Your Brand From Being Used in Scams

YouMail
PROTECTIVE SERVICES

*"The FTC received 2.8 million fraud reports from consumers in 2021. Imposter scams were the most common type of fraud reported to the agency, amounting to more than $2.3 billion in losses."**

**Provided by YouMail Protective Services*

Challenges & Considerations

VOICE SERVICE PROVIDER INTEROPERABILITY

Service providers originating, transmitting, or terminating voice traffic must be flexible and adaptable in their approach to rendering branded calls. For example, solutions that involve a combination of out-of-band authentication for branded calls and robocall content monitoring and analysis for all calls are advantageous and cover more ground where potential network vulnerabilities may be.

This approach is recommended to avoid vulnerabilities and identity spoofing associated with interoperability challenges, policy and standards gaps, or TDM holes, related to STIR/SHAKEN and RCD where data could be lost and calls dropped down to C-level attestation or potentially blocked or spoofed in smaller carrier network traffic.

GETTING A TRUSTED CALL TO THE DEVICE

Device capabilities and interoperability limitations aren't always taken into account when considering the inability to consistently display the identity of a caller in a way that will be definitively recognized by the consumer. There are many user interface options/scenarios including number only, number and name, or branded calling that may include full RCD capabilities.

In addition, STIR/SHAKEN introduces the prospect of a “Verified Caller” and/or a verification checkmark, which may provide a false sense of security to the consumer, when in reality it only means that a call is associated with a network (and potentially a network and telephone number) that has been authenticated upon origination and validated at the terminating network.

CENTRALIZATION

From a trust-building point of view, there is no centralized system for the orchestration or delivery of assets via branded calling which poses a challenge to integrating proper security or anti-spoofing, and trust, in the transmission of trusted information.

CONSUMER CHOICE

When considering the consumer experience, there should be opt-in or opt-out choices given to how they want to receive identity information and have consumer advocacy be implemented in how the design for branded calling works. If consumers are the ones being scammed, they should maintain a choice in how they want to be communicated with.

Steps to Protect Your Identity

1 KNOW YOUR CUSTOMER + NUMBER REPUTATION

The first thing to do as an enterprise is protect the reputation of your phone numbers via a Know Your Customer solution. When strategizing calling campaigns, you must determine who your customers are and consider the manner in which they want to communicate.

Control your number reputation via Numeracle's Number Reputation Management solution to mitigate and monitor improper labeling events and the reputation of your numbers. You can add vetted branding elements through Numeracle's Smart Branding™ Branded Calling Solution to control the consistency of how your name and brand are displayed to consumers.

2 KNOW YOUR TRAFFIC

You can't really know your customer if you don't know your customer's traffic, which is why you need a solution with traffic monitoring like the one offered by YouMail Protective Services.

The enterprise brand can be secured by detecting and eliminating imposter traffic and utilizing fishing protection against brand reputation damage. Through the use of robocall mitigation services that detect unwanted traffic originating, traversing, or terminating on the network, VSPs can do their part to further secure the network from illegal traffic.

3 BRAND DEFENSE & MONITORING

Protect your identity by implementing a solution that allows you to monitor how your brand is presented so that you'll be the first to know if someone if spoofing your identity information.

YouMail Brand Defense provides full protection against voice phishing attacks and threats to enterprise identity perpetrated by illegal impersonation and fraudulent robocallers. It is also a fraud management solution designed to mitigate enterprise damages and deter recurrence of brand abuse.

YouMail Brand Monitor provides surveillance of brand identity over the voice channel, including explicit unauthorized brand name mentions as part of voice phishing scams and implied references to brand relationships. Brands will be informed regarding the potential impact of the impersonation incidents including call volume of bad actor campaigns.

For More Information

FOR FURTHER READING

BLOGS & ARTICLES

YOUMAIL PROTECTIVE SERVICES

“Enterprise Solutions – How to Protect Your Brand From Fraudulent Imposters”
“Four Reasons Why You Should Be Protecting Your Brand From Being Used in Scams”
"How to Stop Brand Impersonation Via Voice Calls, Also Known As Vishing"

NUMERACLE

“Spoof Protection with the Help from YouMail”
“Trust in Branded Calling... Are We There Yet?”

FOR LISTENING

THE TUESDAY TALKS PODCAST

Season 2; Episode 4
“Safe Voice Communications: What to Watch for in 2022 and Beyond”

Season 1; Episode 12
“Spoofing: What it is, what threats does it pose, and what’s being done about it"

MORE ON BRANDED CALLING

Numeracle’s SIPNOC 2022 Webinar
“Consumer & Enterprise Trust in Branded Calling... Are We There Yet?”

Numeracle’s Branded Communications Resource Page

Numeracle’s Tuesday Talks Podcast Collection: Call Display & Branded Calling

CONTACT INFORMATION

If your brand or the brands you service on your network or platform would like additional information on how to secure the threat of brand spoofing, we’d be happy to connect with you to explore.

Numeracle
Molly Weis
VP Marketing & Comms
molly@numeracle.com

YouMail Protective Services
Gerry Christensen
VP of YouMail Protective Services Division
gchristensen@youmail.com