Don't Let Impostors Damage Your Brand

How to Identify and Prevent ROBOCALL SCAMS

YouMail
PROTECTIVE SERVICES

Contents

Introduction

Consumers make purchase decisions based on trust and value. Put more directly, a consumer's brand perception will directly affect whether or not your good or service is purchased, and if that consumer will remain loyal to your brand as a repeat customer.

But what happens when a bad actor impersonates your brand for illegitimate purposes? How can your valuable customers tell which is you and which is the imposter, and how does that affect their desire to return as future customers? What harm occurs as a result of brand impersonation and why should your enterprise be concerned?

Brand impersonation can potentially cost millions of dollars in lost profits through long-term damage to your company's reputation.

A company initially earns consumer trust only after developing a consistent, high-quality product or service, and then by investing significantly in marketing, branding, and goodwill efforts. As brand leaders can attest to, this is an ongoing process, as successful brands must constantly reevaluate their brand positioning and standing in an increasingly-competitive ecommerce marketplace in which consumer trust is paramount to survival. However, many leading consumer-facing brands are also constantly under various forms of attack over communications channels.

With the proliferation of mobile phones, one predominant attack vector that has seen a dramatic surge is through the voice channel.

Brand impersonation fraud has a massive scope of associated costs. New Federal Communications Commission (FCC) legislation such as STIR/SHAKEN can help businesses leverage content-based analytics to best protect enterprise identity from voice channel brand impersonation fraud.

Understanding Brand Impersonation Fraud

Scams involving brand impersonation fraud have become frequent front page news. For example, one long-running scam involving impersonation of the Social Security Administration (SSA), typically goes like this:

> **"..... your social security number with immediate affect. Due to this all your social benefits will be canceled until further clearance. In case you feel this ... in error you may connect with legal ... social security administration. In order to connect with a Social Security Administration officer press 1 now."**

While the fraudulent SSA calls represent a frequent occurring scam perpetrated against a U.S. government brand, impersonation occurs across a diverse range of brands within many consumer-oriented sectors including financial services, hospitality, public utilities, entertainment, computer and communication services. For example, DIRECTV has stated that many impersonators pose as representatives of DIRECTV in an effort to commit prepaid card fraud, which causes significant harm to both consumers and businesses.

One form of brand impersonation is quite easy. A bad actor simply:

- Creates an illicit offer using brand assets that may be found on legitimate internet and/or other sources such as a brand's own email campaigns
- Utilizes a style that appears very closely, if not exactly, like the product and positioning of the actual brand being impersonated.
- This offer will appear at face value to be something the brand offers such as an extended warranty, product or service upgrade, new product or service, etc.
- Millions of phone numbers can be procured at a very low cost from various communication service providers, to be used for robocalling outreach.
- Upon answering the phone or calling a number provided in a prerecorded message, consumers are sent to the bad actor's call center or website instead of to the legitimate enterprise.

Communications channel fraud can come in several formats:

- **Robocall Fraud:** A term referring to a service that uses a computer platform to dial a large quantity of phone numbers, often involving a prerecorded message. If a consumer answers the phone call, they may be connected to a bad actor posing as a legitimate brand.
- **Vishing:** Otherwise known as voice phishing, "vishing" refers to when a cybercriminal uses the voice channel to scam customers, employees, or the company itself. To perpetrate illegal activities. Vishing robocalls frequently involve the use of prerecorded audio imploring the called party to take form of action such as "press one to speak to a representative". If the consumer does not answer the robocall, the bad actor audio message may be left behind as voicemail.
- **Smishing:** A term describing when a cybercriminal uses text messaging for phishing purposes. Robotexting platforms cause text messages to be sent to phone numbers, after which bad actors frequently scam consumers into responding to such messages, which often involve impersonation of a specific brand with a fraudulent offer. These messages often include hypertext with a URL which, if clicked, may take the consumer to a fraudulent website (e.g. brand domain and/or trademark spoofing) and/or cause the bad actor to realize they have reached a consumer that is willing to engage.

The combined effect of impostor messages sent via just two of these voice-channel methods can significantly impact the relationship between your brand and your customer. The addition of brand impersonation messages sent via email can easily end the relationship your customer has with your brand.

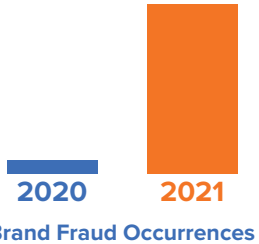
There is the potential for a great deal of damage to brands even if fraud attempts are not successful. It's been proven that people form a lasting impression of a brand, even if they don't engage in two-way communications. In terms of the combined effect of domain and/or trademark spoofing, people that see (logos), read (narrative), and hear (robocall audio) with consistency and frequency are arguably much more inclined to find the messaging credible.

Coupled with the impact of frequency and reach over multi-media channels (e.g. emails and phone calls), the longer-lasting impact of auditory messages on the brain represents a particularly troublesome threat to consumer-brand relationships.

The bottom line is that brand impersonation has a substantially negative impact on the brand-consumer relationship. Both the consumer and brand suffer, even when cybercriminals are unsuccessful in extracting monetary value from the recipients of fraudulent emails, texts and phone calls.

The Rising Cost of Enterprise Identity Impersonation

No business is immune to theft of their own identity. Consider that 25 percent of branded emails are illegitimate.[1] In fact, 90 percent of data breaches are caused by phishing. Companies experienced a 381 percent increase in brand impersonation attacks in the months prior to the pandemic.[2] This trend is accelerating as occurrences of brand fraud in 2021 were 15 times higher than they were in 2020.[3]



Since 2021, consumers have reported losing more than $1 billion to scams originating on social media.[4] Of that total, $417 million were cryptocurrency losses and $35 million of those losses were categorized as business imposters.[5] Imposter scams are the No. 2 most common type of fraud reported to the FTC.[6] About one in five people lost money to imposter scams at a median of $1,000.

Highly Targeted Business Sectors and Government Agencies:

- In Q1 2022, the most targeted industries of brand impersonation attacks were financial services (23.6 percent),[7] SAAS/Webmail (20.5 percent), ecommerce (14.6 percent), social media (12.5 percent), and crypto (6.6 percent).

- From July 2020 to June 2021, about one in three reports of business impersonation were of Amazon — 96,000 people were targeted and nearly 6,000 people lost a total of $27 million.[8]

amazon

96k people targeted
6k people lost a total of
$27M

$46M

- Brand imposters even spread their tentacles beyond the private sector. 147,051 reports of fraud involving government imposters have been reported so far in 2022.[9] The most common government imposter scams pose as the Social Security Administration (SSA), U.S. Department of Health & Human Services (HHS)/Medicare, U.S. Customs & Border Protection (CBP), the U.S. Postal Service (USPS), and the Internal Revenue Service (IRS). SSA imposter scams have resulted in $46.37 million in losses. The FTC even warns consumers "do not trust caller ID."

The U.S. Federal Bureau of Investigation (FBI) estimates that losses of over $5.3 billion have been caused by impersonation attacks.

Legislative Efforts and Regulations

These numbers and their implications are staggering, and even more staggering is that they are this high despite legislation aimed specifically at combating such fraudulent activity. The Truth in Caller Act of 2009 had amended the Communications Act of 1934 to make it unlawful for any person within the United States, in connection with any telecommunications service or Internet protocol (IP)-enabled voice service, to cause any caller identification (ID) service to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted in connection with: (1) authorized activities of law enforcement agencies; or (2) a court order specifically authorizing the use of caller ID manipulation. Furthermore, the RAY BAUM's Act, which went into effect January 6, 2021, had expanded the reach of covered entities from "any person within the United States" to include "any person outside the United States if the recipient is within the United States."

Through the sweeping TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, the FCC has been able to begin implementing a series of protocols, referred to as STIR/SHAKEN.[10]

The Impact of STIR/SHAKEN For Enterprises

STIR (**S**ecure **T**elephony **I**dentity **R**evisited) and SHAKEN (**S**ignature-based **H**andling of **A**sserted information using to**KEN**s) standard, or STIR/SHAKEN, was created to combat the phone number/network spoofing problem.

STIR/SHAKEN represents a means of authenticating and verifying phone calls. Along with providing a vetting framework for establishing originating network operator accountability, one of the primary purposes of STIR/SHAKEN is to prevent unethical and illegal phone number spoofing.

In some respects, STIR/SHAKEN authentication is akin to a digital certificate for websites, which indicates that a certain level of vetting has occurred with respect to the URL owner/website manager. Just like the green symbol on the browser that indicates a website is genuine, STIR/SHAKEN confirms whether or not a phone call has originated from a known entity, as well as the degree of knowledge about that entity. However, just as the behaviors of a website owner cannot be predicted in advance, neither can trust be assumed as implicit for calls that have been authenticated and verified via STIR/SHAKEN.

Two important concepts to understand about STIR/SHAKEN are (1) Verification Status and (2) Attestation. Verification status indicates whether a call has been authenticated and verified or not and attestation refers to the degree of knowledge a call originator has about the calling party.

Verification Status

Verification status (verstat) indicates whether authentication is verified. When verification has successfully occurred, verstat=1 conveys to the terminating network that they may be assured that the call has been authenticated. This status may be leveraged by the carrier receiving calls to present to subscribers a message on the handset indicating "Verified Call", which may be accompanied by a green checkmark.

Attestation

Attestation level refers to the level of trust associated with authenticated calls and is indexed as follows:

Level A:	**Level B:**	**Level C:**
Can attest to the network and that the phone number is associated with the network	Can attest to the network but not the phone number	Cannot attest to either one (typical for international gateways)

Shortcomings of STIR/SHAKEN

While STIR/SHAKEN is effective in achieving its intended purpose of preventing spoofing in some cases, it falls short in terms of fully preventing unlawful robocalls. Phone numbers that successfully receive identity verification, attestation and validation may still be used in conjunction with illegal calls. This concern pertains to phone numbers that receive B-level (or even A-level) attestation.

Despite the implementation of STIR/SHAKEN and other industry efforts to stop unlawful communications, fraud continues unabated, and by many accounts is accelerating.

How to Protect Brand Identity over Communications Channels

With knowledge comes power. Knowing what scams are being perpetrated by bad actors impersonating a brand is the first step to understanding the following:

- **What:** The nature of the scam (e.g. robocalling, vishing, smishing) and its impact. Understanding the context of scams and their attack vectors allows enterprise to make more informed decisions about customer awareness, education, and mitigation efforts.
- **Where:** The focus areas scams (e.g. geography, customer demographic). Knowing where unlawful campaigns are occurring allows enterprise to better assess business impacts and mitigation strategies.
- **How:** What entities are involved (e.g. communication service providers). Knowing how impersonation occurs allows enterprise to remove fraudulent traffic as prevent the source from re-originating unlawful campaigns.
- **When:** The Identifying the instances and measuring the frequency of brand impersonation allows enterprise to prioritize mitigation and deterrence efforts.

With this knowledge, an enterprise may utilize a managed detection and response (MDR) service to shut down bad actor campaigns, minimizing their impact on business operations and corporate reputation. The faster the brand impersonation is identified, the less damage fraudsters can inflict upon that brand and its customers.

Understanding and adopting a brand impersonation identification, mitigation and deterrence service is an essential component to all enterprise risk mitigation and fraud prevention programs.

In order to defend against misinformation and imitation, service enterprise organizations should adopt ongoing brand monitoring via a turn-key MDR solution, to supplement other security and compliance initiatives.

Brand impersonation identification, mitigation and deterrence should include web scanning tools that detect misuse of logos, domain names, and other assets. It should also monitor postings on social media, and phishing and vishing attempts that use brand names in attacks over email and phone lines. By taking action against brand impersonation attacks, an enterprise will ensure that its good reputation is not tarnished by the bad behavior of others that is perpetrated in the name of the enterprise's brand.

Understanding Brand Reputation Management Services

A turn-key brand reputation service should provide a full spectrum of protection against vishing attacks. It should be designed to mitigate enterprise damages and deter recurrence of brand abuse. Solutions should offer alerts, reporting, mitigation, and support for litigation against bad actors.

Surveillance is another key trait in an effective brand reputation protection strategy. All explicit unauthorized brand name mentions and implied references to brand relationships should be monitored. Upon detection of potential trademark infringement or inappropriate brand mentions, the enterprise should be notified immediately.

Don't forget that a brand reputation management solution should be highly automated and include human and AI-based intelligence to identify consumer perceptions. It should be able to spot trends and respond to any misperceptions on social media, chat sites, voice services, and other online media.

YouMail Protective Services provides zero-hour identification of unwanted robocalls that protects against the fall-out of brand imposter attacks perpetrated by bad actor campaigns.

The result:

- **Reduced risk from brand impersonation vishing attacks**
- **Avoid bad press and lost customers**
- **Save IT resources by outsourcing the matter to outside experts**
- **Greater efficacy due to YouMail PS's superior accuracy and millions of data points**

YouMail PROTECTIVE SERVICES

YouMailPS.com

About Brand Defense

YouMail Brand Defense is a managed solution that provides full spectrum protection against vishing attacks perpetrated against enterprise by bad actors. This turn-key risk management solution addresses threats to enterprise identity due to fraudulent robocalls including brand impersonation over the voice channel. It is also a fraud management solution designed to mitigate enterprise damages and deter recurrence of brand abuse. Brand Defense customers benefit from a comprehensive solution that incorporates alerts and reporting, mitigation, and enforcement including support for litigation against bad actors.

About YouMail Protective Services

A division of YouMail, Inc., YouMail Protective Services (YouMail PS) works with enterprises and carriers to shut down unlawful voice and SMS communications. YouMail PS leverages content-based analytics, based on our patented audio fingerprinting, real-time real-user audio collection and more to provides SaaS offerings that achieve the following:

- **Protect enterprises:** by detecting and eliminating imposter traffic, providing vishing protection against brand reputation damage
- **Protect communication service providers:** with robocall mitigation services that detect unwanted traffic that is originating, traversing, or terminating on their networks

Contact

Contact **Gerry Christensen** to evaluate your unwanted robocall detection, mitigation, and deterrence needs. Email **gchristensen@youmail.com** or call 206-472-7060.

Endnotes

1 Admin, "Worrying Phishing Attacks Statistics (Editor's Choice)," Digital in the Round, 18 July 2021.
https://digitalintheround.com/phishing-statistics/

2 ITP Staff, "Summer Surprises could be a bonanza for brand impersonators," ITP.net, 19 August 2021.
https://www.itp.net/security/99579-summer-surprises-could-be-a-bonanza-for-brand-impersonators

3 Bassett, Gabriel, et al. 2021 Data Breach Investigations Report (DBIR). Verizon, 20 July 2021.
https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf?_ga=2.117728905.1684326587.1626974965-1383700957.1626208142&_gac=1.221899242.1626990866.CjwKCAjwruSHBhAtEiwA_qCp-pgO54kq6nYRAv3_5nZPpILqAzBdw5CUfwc-Pk3ax5viCtbFDxwMT1hoC4-0QAvD_BwE

4 Federal Trade Commission. "New Analysis Finds Consumers Reported Losing More than $1 Billion in Cryptocurrency to Scams since 2021," Federal Trade Commission Press Release, 3 June 2022.
https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021

5 Fletcher, Emma. "Reports show scammers cashing in on crypto craze," Federal Trade Commission, 3 June 2022.
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

6 Federal Trade Commission. "Top Three Categories," Consumer Sentinel Network, 3 November 2022.
https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic

7 APWG Phishing Activity Trends Report (1st Quarter 2022). Anti-Phishing Working Group (APWG), 7 June 2022.
https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

8 Fletcher, Emma. "Amazon tops list of impersonated businesses," Federal Trade Commission, 20 October 2021.
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/10/amazon-tops-list-impersonated-businesses

9 Federal Trade Commission. "Explore Government Imposter Scams," Consumer Sentinel Network, 3 November 2022.
https://public.tableau.com/app/profile/federal.trade.commission/viz/GovernmentImposter/Infographic

10 "TRACED Act Implementation," Federal Communications Commission, 5 November 2021.
https://www.fcc.gov/TRACEDAct