HOW THE HOSPITALITY INDUSTRY MUST TACKLE CALL SPOOFING & ROBOCALLING

A Whitepaper Prepared for TNS

TNS

JUNIPER RESEARCH

Contents

WHITEPAPER PREPARED FOR TNS

1. The Current State of Robocalling

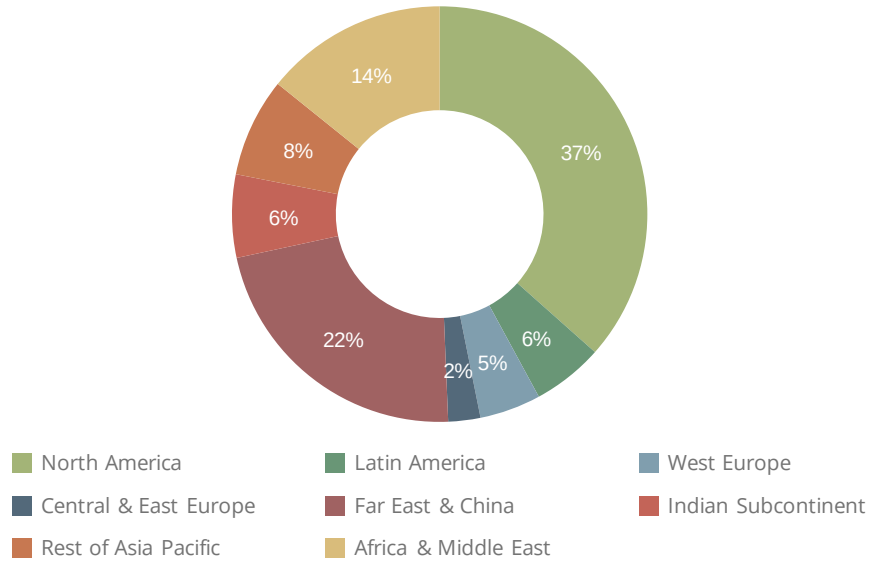
JUNIPER RESEARCH

1.1 The Current State of Robocalling

As the number of mobile subscribers grows, so do the opportunities for fraudulent players. The voice channel remains undervalued, in part owing to the prevalence of unwanted or illegal robocalling. Robocalling is defined by Juniper Research as:

'An automated telephone call which delivers pre-recorded messages to a large number of recipients.'

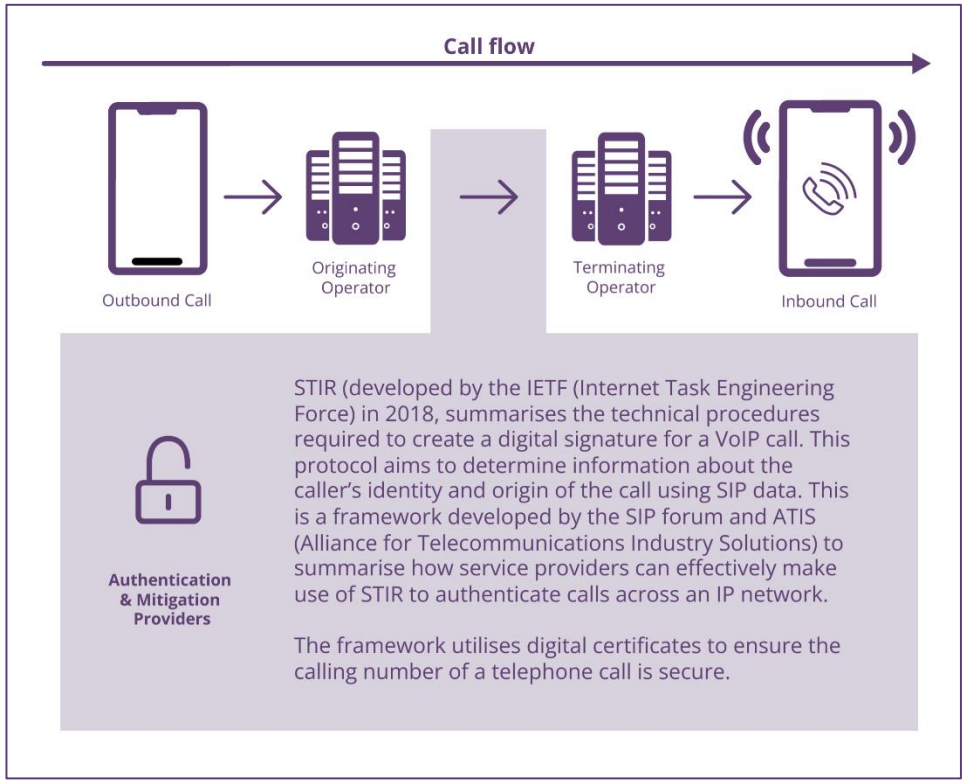
Figure 1.1: Total Number of Fraudulent Robocalls in 2023, Split by 8 Key Regions: 16.2 Billion



Source: Juniper Research

Juniper Research anticipates the total number of fraudulent robocalls will reach 17 billion in 2027, an absolute growth of 7% from 16 billion in 2023.

Figure 1.2: The Role of Third-party Authentication in Voice Calls



Source: Juniper Research

1.1.1 Losses to Fraudulent Robocalls

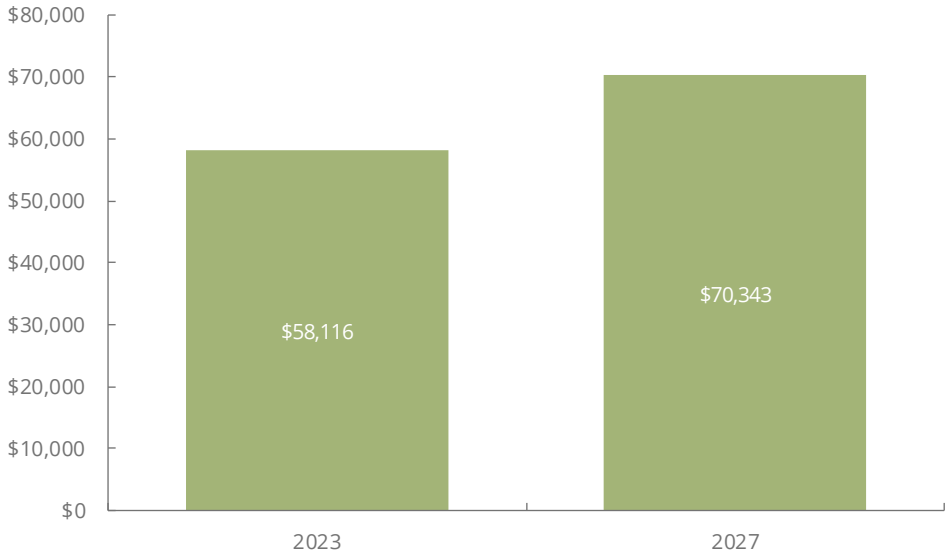
North America remains the most impacted by fraudulent robocalls, and in turn, is the region most in need of branded caller display solutions. However, this has led to the

STIR/SHAKEN framework being developed, and according to Juniper Research, the losses attributable to fraudulent robocalls in North America are predicted to decrease by 28% from $33 billion in 2023 to $24 billion in 2027, owing to this framework and the increasing adoption of branded caller display.

North America is expected to be the only region to experience a decline in the number of fraudulent losses made to robocalls, compared with all other regions which are predicted to increase. This owes to North America's early-mover advantage in an industry-wide collaboration on a framework to tackle fraudulent robocalling; of which branded call display has become an integral element.

Whilst the STIR/SHAKEN framework is yet to generate a decline in fraudulent losses to robocalling, enterprises must begin setting up services such as branded calling to further fight against such calls.

Figure 1.3: Global Consumer Losses to Fraudulent Robocalling ($m), 2023 & 2027



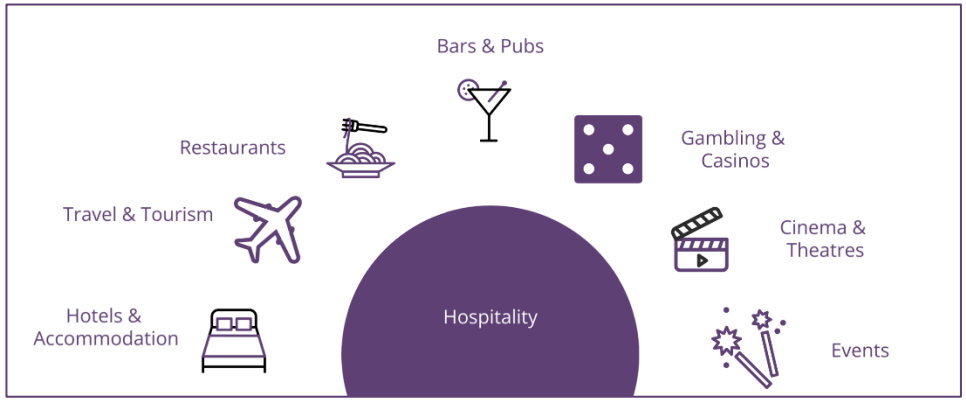
Source: Juniper Research

As shown in figure 1.3, Juniper Research forecasts that the total fraudulent losses made to illegitimate robocalls is expected to increase by 21% globally; rising from $58.1 billion in 2023 to $70.3 billion in 2027.

1.1.2 The Impact on the Hospitality Industry

The hospitality industry is uniquely positioned; in no other industry is customer relationship as important as those verticals found within the hospitality sector. The companies found within the various verticals highlighted in figure 1.4 strive to implement strategies that provide the best customer experience. This has often been achieved through omnichannel communications strategies, including contacting customers through various different channels, such as voice. However, without the correct tools, voice channels are often overlooked, as they are perceived as untrustworthy, owing to fraudulent scam calls and no means for the user to verify the call before it is answered.

Figure 1.4: The Various Verticals within Hospitality



Source: Juniper Research

The voice channel will be preferred by a significant number of customers in each of these verticals. Hospitality service providers who are not communicating via voice to these subscribers are diminishing their reputation.

Users of hospitality services are increasingly likely to pick a call service that uses enterprise-branded calling, as it will remove uncertainty for mobile subscribers once the call has been placed. Without the display of the hospitality provider's name or branding, there is an increased chance of purposefully unanswered or blocked calls. This can have a multitude of ramifications for those in the hospitality industry:

- Reduced Revenue from Hospitality Services: By far, the most important indirect consequence of a failure to implement branded calling solutions is the loss of revenue. This will owe to hospitality providers not maximising the potential of their client relationship tools over voice channels. Adopting enterprise branded calling is the most immediate opportunity to improve communication strategies.
- Diminished Brand Reputation: The damage caused by call spoofing is often irreparable and seldom in control of the enterprise. Adopting branded calling display can enable enterprises in the hospitality industry to encourage trust amongst their customers when making outbound calls. However, call spoofing can be accomplished by fraudsters impersonating an enterprise – and the opinion on this enterprise will be impacted negatively, despite no involvement from the enterprise itself.
- Diminished Ability to Attract Repeat Customers: The absence of communication between company and customer will alter the relationship and ability for the company to offer and promote its products. In turn, the company's revenue will likely suffer in the long term.
- Missed Chances for Upselling: The ability to upsell services is key. Building a relationship with clients must be at the heart of all omnichannel communication strategies for hospitality service providers. Voice is currently an underused element in omnichannel communication strategies. However, with the continuing adoption of STIR/SHAKEN and other authentication methods, such as out-of-band STIR, it will play a more prominent role for enterprises.

WHITEPAPER PREPARED FOR TNS

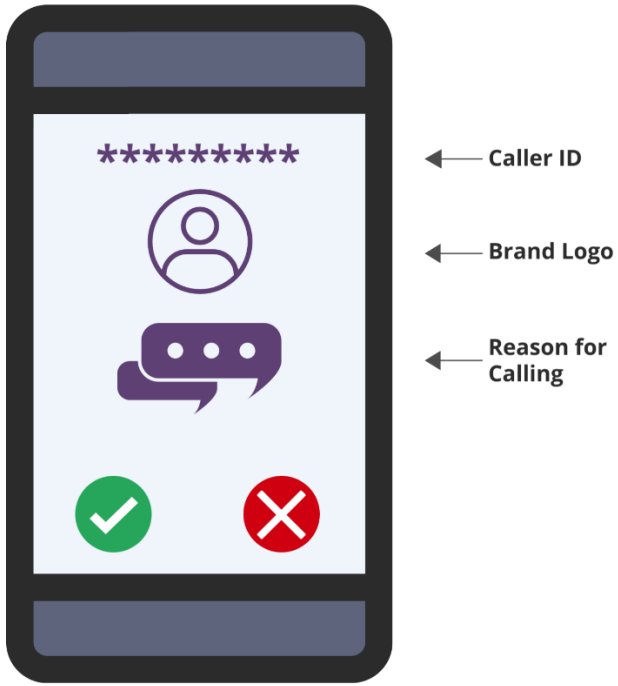
2. Emerging Anti-fraud Services & Brand Authentication

JUNIPER RESEARCH

2.1 Advancements in Robocall Mitigation Technologies & Benefits for Hospitality

Branded calling for enterprises is bringing innovation that enables companies to display information on a call screen before the call is answered, enabling companies in the hospitality industry to build further trust amongst consumers over voice channels. The STIR/SHAKEN framework will help to further authenticate calls and improve customer experience.

Figure 2.1: Brand Authentication Screen Example



Source: Juniper Research

This is noticeably important in the hospitality industry, which is still reliant on voice communications for the delivery of successful customer service.

Without branded calling for enterprises, unwanted robocalls will diminish the reputation of the brand and result in enterprises having to repair relationships with customers after an unwarranted attack. Interestingly, this does not only apply to the hospitality industry, but to all industries – the increasing number of fraudulent robocalls will lead to further decreases in call pick-up rates.

However, branded calling for enterprises aims to fix this:

Branded calling is vital for organisations to adopt when contacting customers, to avoid becoming blocked or ignored in light of the growing number of fraudulent robocalls.

As more enterprises implement branded calling, an increasing amount of users will be able to trust mobile voice channels. As this occurs, enterprises in the hospitality industry will experience higher pick-up rates for outbound calls. They will be able to identify whether this is a brand they want to interact with.

Additionally, advanced branded calling for enterprises is able to not only verify the brand that is calling, but also display the reason for the incoming call. This will place further trust amongst mobile subscribers when answering potential unwanted calls.

The methods in which fraudulent players operate is continually evolving amidst the developments of new fraud mitigation technologies. One of the most effective strategies is to exploit mobile subscribers by imitating a known or trusted organisation, in the hope of gaining personal information and data.

For the clients of hospitality service providers, this can impact the relationship between themselves and their customers: despite the blamelessness of the enterprise itself. The end user will then associate this scam calling with the brand regardless of the lack of involvement in any fraudulent process. The consequence of this is that customers may churn to competing services without the adoption of branded calling technologies.

2.1.1 The Level of Verification for Brands over Voice Channels

There needs to be industry-wide collaboration to tackle robocalling and increase consumer confidence in mobile voice channels. Indeed, customers expect protection from fraudulent attacks from their chosen network operators. However, they seldom have the tools to create the necessary frameworks to efficiently mitigate the threat from robocalling. Listed below are some of the key activities in tackling illegal and unwanted robocalling:

- Call Blocking: In line with the rules set by the FCC (Federal Communications Commission), US operators can implement call blocking technologies to minimise the number of illegal and unwarranted calls reaching the consumer. Both mobile subscribers and companies are able to tackle unfamiliar calls by blocking incoming calls from specific numbers through this strategy, to reduce the number of illegal calls and spam through one's phone.
- Call Labelling: Operators can also implement call labelling and reasonable analytics solutions, to ensure customers can more safely determine which calls they can answer. Such labels are shown through the caller ID, with unfamiliar or illegal numbers being represented as potential fraud on the caller ID display. In turn, this can provide mobile subscribers on the advice on whether to accept the call or not based on the caller ID. Additionally, some companies offer inexpensive call blocking apps as part of their mobile plans, which mobile users can utilise to further label and block unwanted calls.
- Reasonable Call Analytics: A call analytics system will count calls from its source over a particular period of time, using multiple inputs and features, including STIR/SHAKEN. This helps improve the efficiency of mitigation solutions that identify fraudulent and unwanted calls. This is particularly effective when using dynamic traffic analysis to spot and fight the robocall at its origin, and identify the sources of fraudulent or unwanted robocalls more efficiently.
    a) Fraudulent robocallers frequently use a spoofed calling number and attempt to 'outsmart' network operators by switching between different spoofed calling numbers.
- Call Authentication: Call authentication is a widespread and integrative service to identifying and stopping robocalls. This mechanism works by verifying the origin of the call through subscriber vetting, phone number validation and attestation.
    a) Subscriber Vetting: This includes verifying the authenticity of the call through authentication services. However, given the call journey, it is imperative that all members of ecosystem are able to collaborate to maximise the mitigation of robocalling.
    b) Phone Number Validation: Validating phone numbers is a vital aspect to prevent unauthorised users from hacking and spoofing a number associated with a business. The validation of said phone number is important to legitimise the origin of the caller and the number of which they are calling from. Businesses must work with independent third-party authorisation service providers, such as TNS, to ensure that their customers are able to quickly identify the call as originating from the business before answering the call.
    c) Attestation Levels: Such levels are utilised to determine the legitimacy of the entity's calling phone number identity, which is broken down into three particular ratings: full attestation, partial attestation, gateway attestation. The STIR/SHAKEN framework implemented the attestation ratings to further fight against robocalls.

WHITEPAPER PREPARED FOR TNS

3. TNS & The Fight Against Illegal and Unwanted Robocalls

JUNIPER RESEARCH

3.1 TNS & Enterprise Branded Calling

3.1.1 Corporate Information

Founded in 1990, TNS is a global provider of mission-critical communications platforms, designed to improve communications and transactions for the Payments, Financial, and Communications industries.

The leadership team consists of Mike Keegan (CEO); Dennis Randolph (CFO and Treasurer); Mark Cole (CNO); and Jim McLaughlin (General Counsel & Secretary).

TNS' revenue for 2021 was ~$400 million.

3.1.2 Geographical Spread

Headquartered in Reston, VA, TNS has offices throughout North America as well as in Brazil, Italy, France, Germany, Spain, Ireland and the UK, with Asia Pacific operations in Australia, New Zealand, Hong Kong, India, Japan, Malaysia, Philippines, South Korea, Singapore, Sri Lanka, Taiwan, and Thailand.

3.1.3 Key Clients & Strategic Partnerships

With numerous key clients and partners, TNS serves the financial, banking, and telecommunications industries worldwide. These include Verizon, Commonwealth Bank, Mastercard, the NYSE (New York Stock Exchange), Visa, Vodafone, and T-Mobile.

In 2021, TNS was acquired by Koch Equity Development, the investment and acquisition subsidiary of Wichita, Kansas-based Koch. Koch companies have made more than $30 billion in technology-related investments in recent years, and its acquisition of TNS will expand its approach to technological transformation.

In December 2022, TNS formed a partnership with Neustar, First Orion and Hiya to advance call vetting and authentication standards with a single framework across the largest carriers in North America. This will enable secure and trusted calls to many households that rely on landline phones.

3.1.4 TNS Enterprise Branded Calling

The TNS Communications Market portfolio includes a comprehensive Identity and Protection remit where rich call data branding identification can be integrated into major wireless networks; increasing answer rates, and building trust with customers.

TNS acts as the third party between operators and enterprises for brand authentication. This enables TNS to verify whether the call originator has the right to use the telephone number, using a pre-call API. Call originators must let TNS know that they will be using this phone number before any calls are originating from it to ensure that the numbers are not being spoofed.

To provide brand authentication services, enterprises must work with TNS to provide a logo to ensure it can be displayed before the call is answered. At present, apps that support TNS' services are preloaded on over 30 million devices in the US.

- TNS Enterprise Branded Calling: TNS' technology allows businesses to make calls with more caller information on the display screen, helping to enhance brand reputation and improve call answer rates among call recipients.

Additional solutions within the identity and protection suite:

- TNS Call Guardian: A managed end-to-end caller authentication solution that analyses real-time call events combined and compliant with STIR/SHAKEN authentication to validate the callers ID; allowing operators to discern between legitimate users and those with criminal intentions. Call Guardian aims to deliver a better customer experience for call recipients.
- Call Guardian Authentication Hub: A solution for smaller carriers. It combines the capabilities of Call Guardian analytics and Metaswitch's MetaSphere Qcall SIP

application server to analyze real-time call events and differentiate legitimate users from those with abusive or fraudulent profiles.

- Enhanced Caller ID: Leverages networks to empower identity and facilitate trust in personal and business mobile communications. The service informs recipients on who is calling them; giving them the choice as to whether to answer the call. Text ID gives greater clarity to the caller's identity, especially if it is not one of the recipient's contacts.
- Spam ID: Leverages Call Guardian with real-time reputational scores; giving the end user complete control. This includes a large reputational insight database resulting in a high level of accuracy, and an ability to detect neighbour spoofing where a similar number to the recipient might prompt the call to be answered.
- TNS Telephone Number Reputation Monitoring: Allows businesses to be cognisant of their own reputational score, which may be low due to robocalling and associated call fraudsters impersonating their legitimate work. This service has the potential to also alert businesses of the scale of legitimate calls that are being incorrectly labelled as spam, and where applicable, the steps needed to be taken for an improved reputational score, and an uptick in answered calls.
- Crowd-sourced Feedback: A feature of TNS' unilateral approach to robocalling and caller fraud. This has the potential to leverage large amounts of real-time data. As fraud is reported on third-party websites, there is insufficient clarity from reported instances, as a standardised rating system is used that is highly subjective, and may generate different ratings from the same call received by many individuals. There is also the possibility that fraudulent calls could be ranked, with these regarded as neutral or safe by the bad actors perpetrating them.
- STIR/SHAKEN: The default benchmark by which all relevant stakeholders and participants in the ecosystem must comply. STIR/SHAKEN uses digital certificates, based on common public key cryptography, to ensure the calling number of a telephone call is secure. The originating service provider checks the call source and calling number to validate the calling number. TNS' unilateral approach to complementing mandatory legislation with its own Call Guardian solution includes crowd-sourced data. In the absence of authenticating and ranking the source, as well as the level of concern/harassment caused by a seemingly fraudulent call, operators should adopt a cautious approach to subjective data that lacks industry standards by which it can be ranked.

Figure 3.1: TNS' Enterprise Branded Calling

Source: TNS

About TNS

TNS has a global reach with a regional touch, customizing secure network solutions and support to the individual needs of organizations while expanding their scope to new horizons.

TNS has been growing for more than 30 years, building its innovative, value-added services portfolio for thousands of organizations across more than 60 countries.

Our solutions come together in infrastructure-as-a-service platforms, creating trusted hubs for secure, flexible managed connectivity and data interoperability with global reach.

For more information on TNS' products and solutions, please email **solutions@tnsi.com**

About Juniper Research

Juniper Research specialises in providing high-quality data and fully researched analysis to manufacturers, financiers, developers and service/content providers across the communications sector.

Consultancy Services: Juniper Research is fully independent and able to provide unbiased and reliable assessments of markets, technologies and industry players. Our team is drawn from experienced senior managers with proven track records in each of their specialist fields.

For more information on Juniper Research's portfolio, please email **info@juniperresearch.com**