Fighting Back Against the Rise of Impersonation Scams

In 2024, a staggering $1.03 trillion was lost to scams worldwide[1] with bad actors using increasingly sophisticated tactics to target unsuspecting victims. The use of tactics such as telephone number spoofing is eroding consumers' trust in the voice channel and dissipating their willingness to engage with phone calls.

In this infographic, we provide details on the prevalent scams to look out for and the solutions and technology available now to help you protect your customers' data and brand reputation.

Enterprises Under Siege

Any enterprise that does not have protection for their outbound call operations is at risk of falling victim to a spoofing scam. Even the largest, most trusted brands may struggle to prevent fraudsters from hijacking their phone numbers and putting their brand reputation at risk.

A Chase Bank customer lost over $120,000 after engaging with a spoofed 1-800 number that matched Chase's customer service.

Amazon is a frequent imposter scam target with scammers posing as sales representatives to gain remote access to their targets' accounts.

A large US bank fell victim to a large-scale, multi-pronged attack that impacted millions of their customers. They only became aware of this after the attack took place.

Financial losses to enterprises and their customers are not the only repercussions of a spoofing attack. The ramifications of these attacks extend much further:

- Loss of customer trust
- Potential penalties levied
- Reputational damage
- Reimbursing lost funds to customers

The Best Defense is a Good Offense

It has increasingly fallen to CXOs and security leaders to more aggressively secure the voice channel as part of an enterprise-wide strategy. While outbound voice communications have not traditionally been at the top of the risk chart, prioritization is now critical to mitigating the possibility of enterprises and customers falling victim to fraud.

A robust security strategy for voice communication relies on three crucial components:

Call Authentication

Proper call validation enables businesses to confirm the origin of each call, ensuring that it originates from their identified number.

Spoof Protection

Calls that are not properly authenticated should be blocked before they reach customers, ensuring fraudsters cannot establish contact.

Present Critical Call Information

By branding calls with a company's name and logo, businesses can identify themselves, giving customers a better understanding of who's trying to reach them.

When combined, these three measures ensure customers know who's trying to contact them.

Secure Your Outbound Call Operations with TNS

TNS Enterprise Product Suite has the solutions that your enterprise needs in order to stay ahead of the bad actors in the fight against impersonation scams. TNS solutions provide a range of benefits to your enterprise, such as:

TNS Enterprise Authentication and Spoof Protection

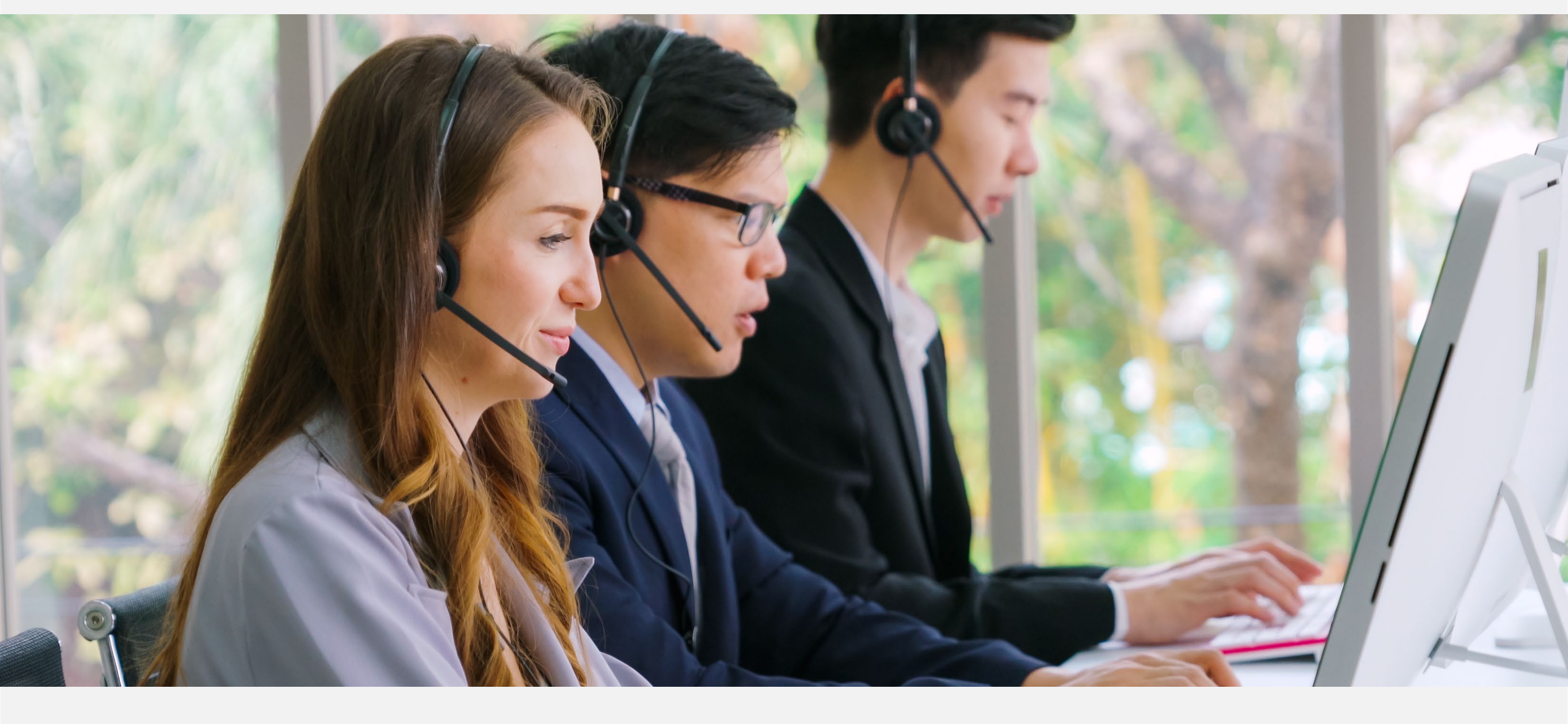
- Helps protect customers
- Helps protect your brand reputation
- Restores trust in voice calls

TNS Enterprise Branded Calling

- Helps increase call answer rates
- Grows conversion rates
- Delivers competitive advantage

Telephone Number Reputational Monitoring and TN Insights:

- Critical intelligence
- Business continuity
- Brand protection



TNS' 'A Guide to Spoof Protection' eBook provides a closer look at the solutions available to protect your telephone numbers and outbound call operations. To make sure that your enterprise stays protected, download the eBook to learn more

tnsi.com/resource/com/guide-to-spoof-protection-ebook/

TNS®

[1] Global Anti Scam Alliance, Global State of Scams Report 2024, November 2024.