

Voice security and voice assurance landscape

White paper


**Mark Voorheis, Voice Security Product
Manager, Verizon Business Group**


**Donald E Spaulding, Sr Principal Business
Strategy, Verizon Business Group**

A man with short brown hair, wearing a blue button-down shirt and khaki pants, is looking down at a black smartphone in his hands. He has a black bag slung over his shoulder. He is standing next to a dark-colored car, with the side mirror and rear light visible. The background is a blurred, textured wall.

verizon
business

Over the past several decades, the movement from traditional public switched telephone networks (PSTNs) to Voice over Internet Protocol (VoIP) technology has increased the capabilities of the voice channel. But these advancements have also created a new attack vector for bad actors to exploit. Two of the main exploits employed against VoIP include the following:

 **Spoofing.** Involves modifying call header information to make a call appear to come from a different phone number or location


 **Robocalling.** Leverages auto-dialing capabilities to generate large volumes of traffic


While spoofing and robocalling can have legitimate applications, their illegitimate use constitutes the broadest array of voice security issues.

Within the industry, many hoped and believed these problems would be addressed by mandates like the Telephone Consumer Protection Act (TCPA) and the Secure Telephone Identity Revisited and Signature-based Handling of Asserted information using toKENs (STIR/SHAKEN) framework. STIR/SHAKEN is a technology framework comprised of interconnected standards intended to combat spoofing. However, limitations exist in the global telephone network that still relies on legacy equipment that cannot transmit the STIR/SHAKEN signing data until end-to-end IP interconnections exist more widely. Of course, there are also the obvious limitations that bad actors do not always abide by government regulations.

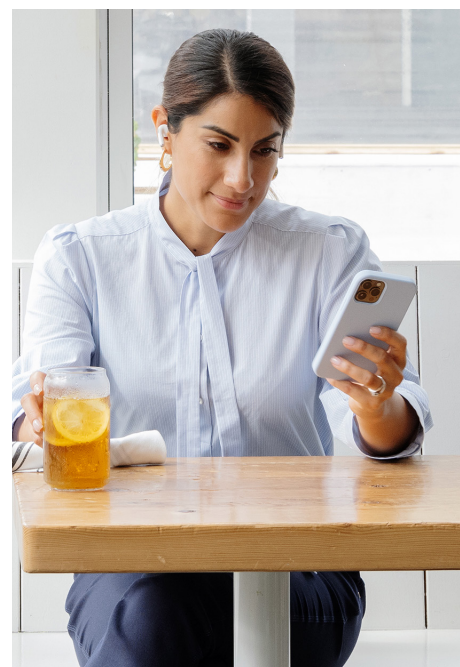
Even so, carriers take measures to try to identify obvious bad traffic. They also work to comply with standards and evaluate customer traffic for any unlawful use. Still, they are limited in their ability to identify all bad traffic since sorting out bad calls from good calls is often subjective. To enhance their ability to identify bad calls, carriers partner with analytics vendors to layer additional capabilities on top of their standard practices. These efforts can provide consumers with a relative legitimate call score, but these services are also limited.

Voice security tools and services vary. Plus, no single tool can address each and every type of voice security threat. Available tools can be broken down into two main categories:

 **Inbound.** Protects the organization from direct threats and includes voice firewalls, anti-fraud and voice authentication tools

 **Outbound or voice assurance.** Helps address the external environment of distrust most consumers have about answering calls and includes things such as call branding, attestation elevation and anti-spoofing services

With all of today's current threats, it's important to follow solid risk management practices that assess the most imminent threats to your business and then identify the most effective tools to help you address those threats. A trusted advisor like Verizon can help you navigate the variety of threats and tools, as well as assist you in implementing specific solutions to address your specific needs.



Combatting threats against one of your most strategic business tools

Your phone just rang, and the immediate thought of something important or exciting is gone as soon as you hear, “Hi, this is Debra with some important information about your car’s extended warranty.” Some people may remember a time when they would actually run to answer the phone, fearful of missing an important call. Not today. Survey after survey shows the vast majority of people simply won’t answer their phone, citing anxiety about who is really on the other end of the line – and what their intentions are.

For legitimate organizations that rely on the telephone to operate and grow their business, this level of distrust hurts business. Organizations expend an enormous amount of time and resources to build a brand experience that is seen as trustworthy, secure and highly responsive. These brand-building efforts suffer when customers harbor a pervasive suspicion about incoming calls.

Telephony technology has evolved significantly in the last few decades. Unfortunately, cybercriminals and fraudsters have evolved alongside that technology, growing ever more sophisticated in their methods. Customers aren’t the only target. Your employees are just as attractive to phone-based bad actors looking to make a quick buck or much more.

While the threats are real, you still shouldn’t deprioritize telephony as a strategic channel for commerce and customer communications. This white paper explores a variety of things you can do to reinstall confidence in the telephone as a strategic business tool.

75%
of Americans will never answer calls from an unknown number.¹

Where are we and how did we get here?

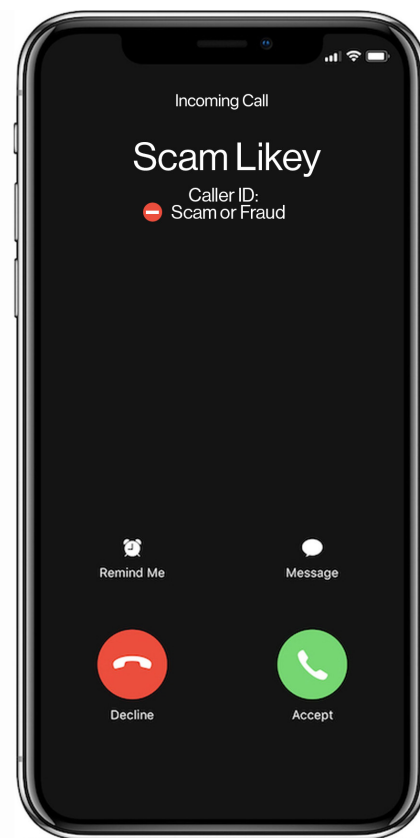
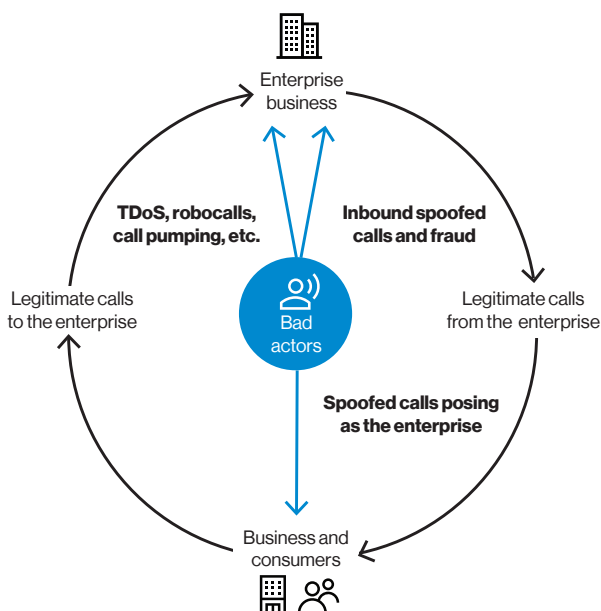
The advent of VoIP telephony a few decades ago started the transition of transmitting voice communications the same way that we transmit data traffic – through a series of packets that travel the internet and get reassembled on the other end. Like any new technology, this meant that you could choose from an array of new applications and capabilities in addition to traditional telephony, which also meant that bad actors could now use the same exploits that they had long used against organizations’ data traffic to attack voice traffic as well.

As these exploits started to appear, it became clear that there were two main ways that bad actors could impact voice traffic:

- Spoofing to attack identity
- Robocalling for volumetric attacks

Spoofing and attacks against identity

Spoofing involves modifying some part of a call header to mask or modify the appearance of the caller to make the recipient believe the call is coming from a different party. Legitimate applications of spoofing exist, such as if you want outbound calls from your call center to display your toll-free number in the receiving parties' caller ID. This can encourage your customer to answer or call back. Additionally, you might have multiple VoIP internet connections that you use for redundancy, but you want all your calls to display the same number even if you are using different providers for the outbound call.



However, this same capability allows bad actors to falsify the identity of their outbound calls. A call that appears to be from your bank might instead be a fraudster that's trying to gain information about your bank accounts, including access credentials.

Robocalling and volumetric attacks

Robocalling uses technology to automate the origination of multiple outbound calls according to a defined schedule based on the calling party's available capacity for a calling campaign. One legitimate use of robocalling could be when local school districts need to reach parents about student emergencies or sudden school closures due to heavy snow. Another example could be outbound call centers using robocalling to connect agents quickly and easily with customers who answer calls.

Just as robocalling can assist call centers in providing better customer experiences, bad actors can use it in the same way to connect with potential victims quickly and easily. Additionally, when bad actors combine robocalling with spoofing, they can increase their effectiveness at connecting with prime targets for their fraudulent calls.

Robocalling can also be used to aggressively create large volumes of traffic as part of a Telephony Denial of Service (TDoS) attack. The large volume of inbound calls a targeted organization might receive from such an attack can disrupt or overload its voice infrastructure. This can prevent it from taking in legitimate calls. A TDoS does not need to physically or precisely take down an organization's telephony infrastructure to be damaging either. Even a small increase in illegitimate traffic can increase customer wait times and impact customer satisfaction.

Impact of illegitimate use

Most, if not all, consumers can identify the negative impacts caused by bad traffic. According to the Federal Communications Commission (FCC), U.S. consumers receive more than 4 billion robocalls a month.² Those robocalls can also be directed at an organization's telephone numbers. But these organizations face two additional issues beyond unwanted robocalls: They deal with the problem of not being able to have their legitimate calls answered, and they have concerns about the effects of fraudulent calling on their brand.

Consumer impacts	Organization impacts
Answers calls that are unwanted	Enables inbound fraud, spoofing and volumetric attacks (TDoS)
Answers calls that are fraudulent and can lead to becoming fraud victims	Potentially creates liability to reimburse consumers for losses if they become victims of fraud (regulated or service-oriented liability)
Ignores or doesn't answer voice calls due to increased antipathy	Experiences brand erosion or loss of trust when consumers receive fraud/spoofed calls that claim to be the organization
Misses calls they should have answered because of habit of ignoring/not answering	Decreases productivity when consumers don't answer legitimate calls

“U.S. consumers receive more than 4 billion robocalls a month.”
 – Federal Communications Commission (FCC)²

To some degree, consumers can rely on government regulations to provide some advocacy associated with these threats. However, those same regulations can create added burdens for your organization if you don't have the same advocacy to help you. Organizations have to rely on other tools looking to combat this threat, including working with carriers on creating an ecosystem that can restore consumer confidence in the voice channel.

Regulatory and carrier action

Government regulation

As implied above, the FCC provides consumers some advocacy. The FCC created the Telecommunications Consumer Protection Act (TCPA) over 30 years ago to set guidelines for telemarketing. More recently, the FCC introduced the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, which mandated the implementation of STIR/SHAKEN. STIR/SHAKEN implements a framework for VoIP carriers to attest to the validity of traffic originated on their networks by digitally signing those calls.

While both of these acts put in place some needed regulations and safeguards, they both have in common the basic premise that bad actors will either not abide by them, or circumvent them altogether. STIR/SHAKEN has specifically been the source of a lot of questions since its implementation, which were largely due to a misunderstanding of what it could and could not accomplish.

What STIR/SHAKEN can accomplish is to provide insight for a recipient about the relative legitimacy of the origination of a call. In other words, it can identify a legitimate spoofing call by telling you if the originating carrier knows the originator of the call, as well as if that originator is known to have the right to originate calls using the originating telephone number.

However, STIR/SHAKEN cannot provide any insight into the intentions of a caller. Put another way, a call can have a clean or legitimate STIR/SHAKEN signature, but the person making the call could still be a bad actor with malicious intent. Think of online shopping. When you see the padlock icon in your browser, you have some assurance that the connection between you and the owner of that website is encrypted, and your credit card number or other credentials can't be sniffed by somebody looking at the traffic crossing the wire. But that padlock can't tell you if you should trust the website owner with your credit card number.

Today, STIR/SHAKEN has other and perhaps more significant limitations due to the nature of VoIP telephony itself. As a newer form of telephone communications, VoIP traffic has to interact with the PSTN. This interoperability is required to ensure that all parties can call one another. It also means that when a VoIP call is originated by one carrier, it may cross TDM switches before it reaches its destination. When this happens, the STIR/SHAKEN signatures and other data that was part of the SIP packet are lost. As a result, the terminating service provider and, ultimately, the recipient of that call won't be able to receive the data that would otherwise validate that call. This limitation will likely persist for the near term as major carriers work to create IP interconnections between themselves to facilitate end-to-end IP transport.

It's also important to understand that STIR/SHAKEN is not itself a blocking mechanism. Different terminating carriers, analytics providers and tools would need to interpret the STIR/SHAKEN information on a call to make any decision about blocking it. However, at its current stage, most of these providers recognize that STIR/SHAKEN is best viewed as one factor in an algorithm that can help determine the relative merit of a call, and not an exclusive reason to block a call.



Carrier action

Verizon, as well as many other originating carriers, have started taking independent action to combat the rise of fraud and robocalling. These actions can take several forms. For example, carriers might perform analysis of their traffic as part of a “know-your-customer” initiative. These initiatives are designed to make sure that customers themselves are following standards set by the FCC or the carrier itself. This kind of analysis can make sure that customers who are not compliant can be identified and their traffic removed.

Other efforts include ongoing research into what types of fraudulent calls take place to help identify obvious bad traffic. Traffic that comes from illegitimate numbers or numbers that have been identified as ones that do not originate (DNO) can be blocked. Many carriers also implement honeypots throughout their network to simply receive calls, allowing fraud analysts to assess what types of threats are new or simply more prevalent, where those calls come from, and what actions can be taken to prevent them.

All of these efforts are an important core step to the basic hygiene of the voice network. But there are limitations to what actions carriers could or should take. Since carriers have different spectrums of customers and their customers have different business needs, it prevents a universal implementation of some blocking methods across a network due to potential impacts on legitimate calls from a carrier’s customers. For example, even if a specific country code appears to be the source for a large amount of fraud, blocking that country code could impact customers who do legitimate business with that country. So, widespread blocking rules won’t typically be part of a carrier’s charter.

Analytics and voice spam efforts

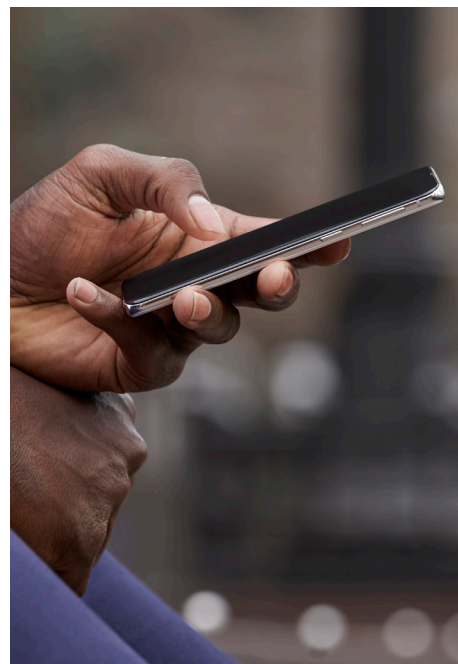
Since carriers can’t undertake widespread blocking without impacting legitimate businesses, most terminating service providers have partnered with analytics providers. These analytic providers can use complex algorithms to determine the likelihood of a particular call being wanted or unwanted based on a variety of factors. Some factors might include the originating carrier, originating ANI, other originating parameters, presence or absence of a STIR/SHAKEN signature, customer feedback concerning that calling number, and the comparison of the calling number against any lists of known fraudulent callers.

These algorithms and their resulting scores can be used by the called parties phone to either display spam warnings or even block calls based on the score. Analytics providers and carriers regularly assess the types of fraud in the ecosystem to adapt these algorithms to better identify and alert customers based on new threat patterns.

As these analytics providers have progressed, they have also looked at ways to offer additional enhanced services to both consumers who receive calls, and organizations whose legitimate calls end up being analyzed.

These services may include the following:

- Reputation monitoring that allows an organization to be alerted if one of its registered phone numbers becomes flagged with a high spam rating
- Branded calling that enables an organization to add a name and possibly even a logo to its customers display when receiving a call
- Anti-spoofing services that in limited circumstances can block a call from reaching a targeted consumer when the call comes from an organization’s registered telephone number but didn’t originate from the organization itself



These additional features can be extremely valuable to organizations, but at times the relationship between analytics providers and carriers can have a narrow scope. This forces organizations to establish relationships with multiple analytics providers in order to reach all of their end users spread across a variety of different carriers with each one serviced by a different analytics provider.

In order to address some of the silo issues described above, some aggregation services have appeared that allow organizations to contract with a single vendor who can manage the branding, anti-spoofing or reputation service between multiple analytics providers.

Voice security and voice assurance tools

With all of the various items discussed above, it should be clear that the need to protect the organization from these threats in the voice channel is similar to the need to defend against more traditional information security threats. In fact, VoIP is really just another application riding on top of the traditional IP stack. But for all of the ways that these issues are similar, the voice channel presents unique challenges that require special attention and special tools to properly address the different types of issues that can arise.

We can separate these tools into two main categories:

- Voice security for inbound voice traffic
- Voice assurance for outbound voice traffic

Voice security (inbound)

Many people use the term voice security to exclusively describe any threat that impacts the voice channel or any tool that addresses threats within the voice channel. But for our discussion, we use the term voice security exclusively to refer to the treatment of inbound calls. This is because inbound call traffic directly impacts the organization in terms of confidentiality, integrity and availability in real and tangible terms. On the other hand, outbound call traffic topics only impact these in a peripheral sense, which we will discuss in the next section.

Voice security threats can run the full gamut of issues, including:

- Confidentiality issues, such as a bad actor impersonating a user and accessing account data
- Integrity issues, such as that same impersonator being able to transfer funds or make changes based on their elevated access
- Availability issues, such as potential TDoS attacks



The following table outlines some of the various types of tools and the types of attacks they specifically are designed to address:

ANI validation	ANI validation tools use the information in the call header to determine if the call was spoofed. These are useful for a base-level determination that the call is legitimate, but it should be noted that it does not determine whether the call is a good or bad call. It simply verifies that the call appears to be from who it claims.
Voice firewall/ intrusion detection system (IDS)	Voice firewalls and voice intrusion detection systems look at all traffic coming into a specific network, location or device. They evaluate those calls based on a set of rules or policies. Similar to traditional firewalls, these tools can take different types of actions, such as allow, block, log or alert. Many of these tools can also apply rules based on anomaly detection, such as looking at specific traffic patterns that are normal and acting on calls that deviate from those patterns.
Fraud detection	<p>Fraud detection can go beyond voice security, but here we limit this description to tools specifically designed to go beyond simply detecting the likelihood of fraud and spoofing based on the call header. It can actually listen to the call audio and apply advanced machine learning to detect patterns of audio from the caller's voice, touch-tone device acoustic signature and even the network originating the call. It can use all of these factors to determine if the call is legitimate and the likelihood of the caller being fraudulent, and then alert the called party to its findings.</p> <p>Contact center environments often use these tools when the audio can be analyzed while the call is still in the interactive voice response (IVR). Then the agent presented with the call can see the likelihood of fraud and even be given different scripts or procedures to handle the call.</p>
Voice authentication	Voice authentication tools often use anti-fraud technology to verify legitimate callers. For example, contact centers can use voice biometrics and device identification technology in voice authentication tools to positively enroll, identify and authenticate legitimate customers/callers (subject to applicable regulations). These capabilities can save time for agents and customers, and more accurately authenticate a customer beyond multiple knowledge-based assessment (KBA) authentication practices.

In most instances, determining the right tool to deploy begins with identifying the area of the organization impacted most by the traffic you are trying to protect. For example:

- ANI validation tools can be used as a general line of defense across most areas of the organization
- Voice firewall and IDS solutions look at a wider view of all traffic coming into a site
- Anti-fraud and authentication tools are used more for contact center traffic due to the unique role that contact centers play in handling the most targeted assets within the organization, such as user credentials and the ability to complete transactions

Voice assurance (outbound)

The term voice assurance refers to the subset of issues related to an organization's outbound dialing. The distinction here is that the nature of these issues is typically less of a direct threat, and more of an indirect one. That doesn't mean these threats don't exist. Rather, the threats come from an atmosphere of distrust created by high volumes of fraudulent calls in the wild.

These issues create a virtual kind of denial of service. If an organization's calls are not answered because bad actors have created an environment of apathy, then they have an issue with availability. The service they use is no longer effective at achieving the goal it was built to reach. Even though the source of the issue happens outside of the organization's control, it still has an impact. And there are ways an organization can take action to combat issues of public perception of what good calls look like.

Organizations can use different types of tools to provide voice assurance to their customer. These include call branding and anti-spoofing.

Call branding

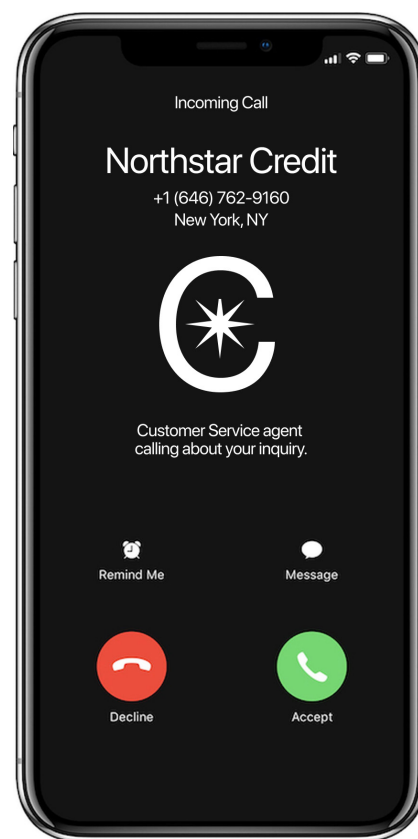
Call branding employs coordinated efforts to associate calling numbers with a combination of information related to name, number, logo and reason for the call. Its goal is to present this information to called parties on their mobile devices in order to increase the likelihood of them answering the call.

Call branding solutions require some form of communication to the branded calling provider in order to confirm the legitimacy of a given call before it can receive branding. This communication is necessary to make sure a fraudulent call spoofing a registered number does not benefit from branding and appear more legitimate.

Call branding solutions typically use either out-of-band call branding or in-band rich call data (RCD) for this communication:

Out-of-band call branding

Out-of-band solutions utilize an API call to communicate with the branding provider. These solutions are widely available today but can create challenges due to the need to integrate with multiple vendors for each terminating service provider. However, some vendors provide the ability to aggregate the service to provide one contact point for the organization.



In-band rich call data

In-band solutions take advantage of RCD, which is a set of additional headers that are part of the SIP standard that can be signed or attested to using STIR/SHAKEN. In this scenario, the call itself receives its primary STIR/SHAKEN signing or attestation, while the additional RCD components are signed as part of an extended SHAKEN header.

The primary advantage of the in-band method is that all of the validation or communication regarding the validity of the call is included in the call itself. However, it has the same limitations as STIR/SHAKEN with regards to full adoption and end-to-end IP connections as described earlier.

Anti-spoofing

In the context of voice assurance, anti-spoofing services are specifically designed to coordinate with terminating service providers (TSPs) to stop calls that purport to be from an organization but are actually fraudulent. They do this by using API functionality similar to that used by out-of-band call branding. But instead of telling the TSP to not apply a brand to a registered call, it tells the TSP to drop the call. Although this is a powerful capability, precautions need to be taken to prevent false positives. False positives can occur when legitimate calls reach the TSP ahead of the API registration, which can cause a legitimate call to get dropped.

The key consideration for voice assurance services is to ensure careful implementation in a way that illegitimate calls don't get treated in an elevated manner. The goal with voice assurance is to restore consumer trust in the voice channel. One way to achieve that trust is by providing accurate branding information on legitimate calls. Any branding that gets applied to fraudulent calls can destroy the rebuilding of that trust and further erode the efficiency and efficacy of the voice channel.



Trust Verizon as your voice security and voice assurance advisor.

A variety of threats puts the voice security landscape at risk. Successfully addressing those threats requires a diverse set of solutions and tools that will differ based on specific circumstances. Regardless of where an organization exists in its solution adoption life cycle, it should follow solid, time-proven risk management practices that assess the most imminent threats and identify the most effective tools. Identifying a trusted advisor, like Verizon, can help organizations navigate the variety of threats and tools available. We can also help you follow a phased approach to addressing your most critical needs first, and then moving into longer-term strategic planning.

To learn how Verizon can help you address your voice assurance and voice security risks, visit us at [verizon.com/business/products/contact-center-cx-solutions/voice-security/](https://www.verizon.com/business/products/contact-center-cx-solutions/voice-security/) or contact your Verizon Account Manager.



1 "TNS Survey: 75% of Americans Will Never Answer Calls from Unknown Numbers," Business Wire, July 26 2002. <https://www.businesswire.com/news/home/20220726005226/en/TNS-Survey-75-of-Americans-Will-Never-Answer-Calls-from-Unknown-Numbers>.
 2 "Robocall Response Team: Combating Scam Robocalls & Robotexts," FCC, August 18 2022. <https://www.fcc.gov/spoofed-robocalls#:~:text=U.S.%20consumers%20receive%20approximately%204,hide%20a%20caller's%20true%20identity>
 Network details & coverage maps at [vzw.com](https://www.verizon.com). © 2023 Verizon. WP1290323