Contact Center Pipeline

UNWANTED CALLS

BY VICKI SIDOR,
MUTARE

COMBATTING THE INVISIBLE ENEMY

Nuisance and nefarious calls are targeting agents and killing KPIs.

MAY 2023

ILLUSTRATION PROVIDED BY ADOBE IMAGES

COMBATTING THE INVISIBLE ENEMY

NUISANCE AND NEFARIOUS CALLS ARE TARGETING AGENTS AND KILLING KPIS.

BY VICKI SIDOR, MUTARE

Robocalls, voice spam, phone fraud, spoofers, and vishers (voice phishers) are inflicting significant damage on businesses through lost productivity, degraded customer experience (CX), missed sales opportunities, and cybersecurity threats.

While consumers have learned to simply ignore calls from unknown sources - a practice even the FCC advises - it is not a viable option for customer-facing organizations that depend on voice communications as a core service offering.

This is particularly true for the omnichannel contact center. While digital chat is a great option for simple support queries, the phone is still the preferred vehicle for customers dealing with more complex or sensitive issues. Those customers have a deep desire to be listened to and understood, and two-way conversations are often the most expedient paths to problem resolution.

In short, there is simply no substitute for the human-to-human connection that is possible through the phone. And optimizing the efficiency of your voice channel is among the most positive steps you can take to meet KPI goals.

> ***...WASTEFUL, DISTRACTING, FRAUDULENT, AND OUTRIGHT MALICIOUS CALLS ARE MORE THAN JUST AN ANNOYANCE.***

That is why wasteful, distracting, fraudulent, and outright malicious calls are more than just an annoyance. They are jeopardizing not only the overall quality of your service delivery but the security of your people and the organizations they represent.

PERFORMANCE AND UNWANTED CALLS

It's no secret that contact centers operate under significant pressure to meet their contractual obligations while making sure callers are well-served.

The success or failure of your organization is judged through a cornucopia of performance measurements, including CX, call initiation, and agent productivity.

Performance in these areas is, in turn, managed and measured via defined

KPIs and metrics, such as CSAT, FCR, FRT (First Response Time), CPC (Cost per Call), ASA, AHT, calls blocked, abandonment rate, active waiting, peak traffic, and schedule adherence.

> ***BUT WHAT IF YOU KNEW THAT AT LEAST 10% OF YOUR VOICE TRAFFIC IS NOT FROM CUSTOMERS AND PROSPECTS SEEKING SUPPORT, BUT FROM UNWANTED SPAMMERS, SCAMMERS, AND FRAUDSTERS?***

Results from these measurements drive management and resource allocations, so the integrity of your call data has a direct impact on the effectiveness and efficiency of the organization.

But what if you knew that at least 10% of your voice traffic is **not** from customers and prospects seeking support, but from unwanted spammers, scammers, and fraudsters?

- How would this skew your call data and their corresponding metrics and KPIs?
- And how would that bad data affect decisions around resource allocations?
- Finally, when a significant portion of those calls are actually nefarious in nature, do you really want your agents to be the single line of defense against skilled cybercriminals seeking to infiltrate and do harm to the businesses you represent?

The irony is the integrity of your operations is directly impacted by the integrity of the traffic traversing your networks. And the voice channel is, by far, not only the most vulnerable channel, but the most unprotected.

KNOW YOUR ROBOCALLS

To better understand the impact of unwanted traffic on your organization, it's important to recognize the problem in its many forms, starting with the ubiquitous robocall.

Robocalls are auto-dialed calls delivering a pre-recorded message to both targeted and random numbers. While many of these calls are legitimate alerts and reminders, well over half are from unwanted telemarketers or actual scammers, mostly using spoofed (digitally manipulated) caller IDs to mask their true identity.

According to robocall blocking software developer YouMail, more than 50.3 billion robocalls were placed nationwide in the U.S. last year with continued growth that, despite curbing efforts put forth by Congressional actions and the FCC, sees no signs of abating.

Robocall campaigns, themselves, vary in form and so impact call center operations in a variety of ways.

> ***...THE VOICE CHANNEL IS, BY FAR, NOT ONLY THE MOST VULNERABLE CHANNEL, BUT THE MOST UNPROTECTED.***

1 SPAM STORMS

A spam storm is a sudden influx of robocalls coming into an organization. These events are mostly generated by scammers and, if hitting a call center, have multiple impacts, including overwhelming the network and degrading response times for legitimate callers.

Many of these campaigns also target an organization's internal DID numbers with sequential dialing: so agents with internal DIDs are at risk of disruptions on their direct lines.

2 DEAD AIR CALLS

While organizations that use IVRs to route incoming calls may get some protection from common robocalls that fail to pass through the keypad prompts, for many systems, incoming calls go directly to call queues.

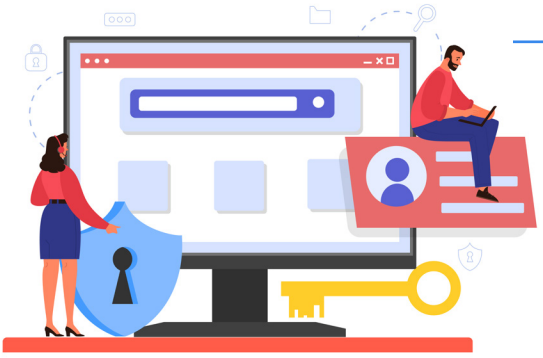
If these are robocalls, the messages have likely already played when the calls were first connected. The responding agents, then, are greeted by "dead air" but must still waste precious time confirming that there is, indeed, no person on the other end.

3 TOLL FRAUD

Bad actors using autodialers are exploiting contact center inbound and outbound call lines for illegal gains through several types of toll fraud. Toll fraud is a kickback scheme perpetrated by a threat agent or criminal organization in partnership with a rogue carrier.

High-value toll-free numbers, such as those used by call centers, are often the targets. Calls to those numbers are free to the callers, while the organization utilizing the number pays a per-minute per call fee to the number provider. That provider, in turn, distributes a portion of that fee to every carrier in the call path.

The criminal goal, then, is to simply keep the calls "alive" for as long as possible in order to generate the most revenue. In some cases, the automated incoming call is programmed to generate random keypad inputs once answered that keep the call circulating through the center's IVR.



While these calls may never reach an agent, they are wasting resources and degrading network performance. If the calls do reach agents, the messages are often deliberately recorded to be long and garbled. Which means that agents are caught up trying to get clarity from the "callers" while other legitimate calls wait on hold.

Outbound toll fraud occurs when threat actors gain access to the organization's phone system and then generate massive auto calls to premium international numbers. We know from our customers and industry contacts that outbound abuse is very prevalent because it is quite lucrative for the criminals.

In either case, many businesses are unaware that they have been victims of toll fraud until the bills arrive. And in both cases, performance metrics are impacted by the amount of illegitimate activity involved.

4 VISHING FRAUD

In addition to nuisance and nefarious robocall campaigns, contact centers are an increasingly popular target for direct calls from cybercriminals posing as customers or other trusted sources.

No doubt, customer service contact centers are a particularly enticing target for these sophisticated scammers. They are a convenient gateway to organizational and customer data and are staffed by agents who not only must answer every call: but who also are predisposed to approach those calls with a helpful attitude.

In this form of attack, known as vishing, the threat agent is highly skilled at impersonation and social engineering.

Thanks to easy access to personal information harvested through public forums or purchased on the dark web, they are well-armed with enough material to provide a convincing front. In many cases they start with a series of benign calls to a targeted associate in order to establish a rapport and gain trust prior to requesting, for instance, a transfer of funds or password reset.

We'd like to think that such deception is only successful when perpetrated on the naïve or unsophisticated. But this assumption is belied by the facts, as some of the world's most respected brands, including Robinhood, Twitter, Cisco, Uber, and Twilio, have all suffered breaches enabled through vishing intrusions.

With vishing incidents seeing a 550% increase in the past year alone, it is no surprise that 77% of companies, according to a May 2022 survey by Agari and Phishlabs, admit they, too, have been targeted.

And let's not forget that even if an attempted scammer or visher is unsuccessful, they have still taken an agent away from providing service to the callers who matter and contribute to the degradation of your KPI metrics.

> ***THE QUESTION NOW IS WHAT CAN BE DONE... NO ONE FORM OF DEFENSE WILL BE EFFECTIVE AGAINST SUCH AN AMORPHOUS ENEMY.***

TOOLS OF DETECTION

The question now is what can be done? And the answer is multi-faceted, as no one form of defense will be effective against such an amorphous adversary.

While it's a given that agents should be well-trained to recognize the signs of phone fraud, it is unwise and, in fact, unfair to place the full burden of fraud protection and organizational security on the individuals: who are already on the front lines to deliver exceptional service to their callers.

There are numerous technologies available that, for instance, provide call source analytics that detect call spoofing, or apply voice biometrics to assist with caller authentication.

The more sophisticated of these resources may integrate artificial intelligence (AI) and machine learning techniques to detect unusual calling patterns or IVR usage anomalies: and provide agents or administrators alerts when suspicious behavior is detected.

Multifactor authentication (MFA) has become commonplace for online account access. It then should also be an acceptable form of customer authentication in the call center, protecting both the organization and the customers they serve from identity fraud.

While narrowing the possibilities of a successful impersonation, MFA is, however, not foolproof. It can only be considered another layer in the organization's arsenal of fraud protection measures.

Because we are seeing unwanted calls as a threat to both your KPI metrics and the actual welfare of your agents and organizations, it makes sense to place a high priority on systems and technologies that rid the traffic itself of those damaging intrusions. Before they have a chance to infiltrate your network and reach vulnerable agent endpoints.

It is worth the time, and the time is now, to check with your contact center platform provider to see what kind of protections they offer or, alternatively, third-party voice traffic filtering technology developers that are working on solutions that keep you one step ahead of the scammers.

As Vice President, Sales and Channel for enterprise telecom software developer Mutare, Vicki Sidor guides the company's initiatives and strategies related to voice network performance and security that help clients identify and solve complex business challenges impacting revenue, efficiency, and compliance.

PREMIUM CONTENT + RESPECTED CONTRIBUTORS FOR CONTACT CENTER PROFESSIONALS

ENABLING A NEW GENERATION OF CX AND EX PROFESSIONALS to create successful customer management strategies, develop cutting-edge technologies, refine the skills necessary to advance their career, and build a culture that advances the contact center within the organization—that's what we do.

Since 2009, **Contact Center Pipeline** has leveraged the insight of today's notable CX and EX thought–leaders, along with our advisory board, expert magazine authors, blog contributors, and industry insiders; keeping our audience ahead of the trends transforming the contact center and customer sales, service, and support industries, improving outcomes, and the way companies engage with their customers.

Contact Center Pipeline Magazine is published monthly digitally and in print. For more information and to subscribe, visit our website.

Contact Center Pipeline

INSIGHT AND INSPIRATION FOR CONTACT CENTER PROFESSIONALS