www.pipelinepub.com
Volume 20, Issue 5

The Five Rs of the Customer Experience

Protecting Digital Identity, Preventing Fraud & Robocalls

By: Michael O'Brien

The rapid acceleration of digital transformation and automated support has shaken up businesses in a really good way—from improving efficiencies to streamlining the customer experience. In this around-the-clock era, when consumers want access at any moment, enterprises are embracing new technologies, communication channels and methods to connect with them, and they're delivering big time. Consumers, however, are being besieged by an onslaught of nefarious trickery on the part of fraudsters and spammers. Determined to violate the sanctity of digital identity, fraudsters incessantly attempt to breach the barriers of bank accounts, harvesting sensitive, personal information and becoming part of a community of digital imposters wreaking havoc for personal gain.

Among the most notorious tactics employed by this global cartel of bad actors are illegal robocalls, which emerge as a persistent annoyance, proving to be at best an inconvenience, and at worst a medium for malicious actions. Either way, the money pilfered from scammers is widely assumed to be linked to activities ranging from money laundering and financing wars to supporting weapons trafficking, terrorism, and human trafficking.

But it's not just illegal calls. It's all types of communications fraud that cast a shadow of doubt and cause problems. Spoofing, smishing, and robotexts all contribute to the chaotic and blatant misuse and abuse of the global communications network, leaving consumers wary of answering the phone and having an even further negative effect for businesses that can't reach their customers when they need to. When the high-capacity, globally ubiquitous network that connects everything and everyone is under relentless assault, businesses are faced with the increasingly challenging task of keeping commerce flowing, businesses running, and consumers engaged.

At the epicenter of trusted digital identity lies the phone number, which has experienced a storied evolution from a simple location identifier or network endpoint to a direct link embodying the unique identities of individuals and companies across the globe. Considering that the mobile phone itself is slated to become the primary source of identity for over 3 billion people this year, safeguarding this de facto digital identifier is imperative for companies seeking to expand and provide the best possible customer experience (CX). Communication service providers (CSPs), in turn, are saddled with the daunting challenge of ensuring illegal robocalls (scams) are blocked, while legal robocalls (even if unwanted) and other legitimate phone calls are labeled correctly so that they are ultimately delivered so that the recipient can make an informed decision on whether to answer the call or not.

In response to these pervasive challenges, a full-bodied, concerted initiative has unfolded, uniting regulators, CSPs and telecom vendors in a collaborative endeavor to help quell the dastardly tide of illegal robocalls. Encouragingly, recent data paints a promising picture, revealing a noticeable decline in robocall activities. December 2023 marked a remarkable milestone in the U.S., witnessing the lowest count of robocalls since February 2022—an impressive 3.8 billion calls—which stands at a noteworthy 20 percent below the monthly average for 2023.

This positive trajectory is a sign of significant progress, setting the stage for a careful exploration of the illegal robocall issue through the lens of the "5 Rs of CX": *Risk*, *Regulation*, *Revenue*, *Reduction*, and *Relevance*.

Risk: The Trust Factor - A Network Imperative

The phone number has transformed into a digital identity link that brings with it profound responsibility. Initially established as a more efficient way to communicate globally and accessible to all, the phone number inadvertently opened the door to bad actors recognizing the reach and anonymity of hiding in a digitally connected society. Seeing it as a new, evolving route to defraud, it is the 21st-century version of piracy with the added benefit of being able to conduct attacks at any time, at any magnitude while remaining mostly invisible to victims and the law. Understanding these attack vectors and their impact on businesses and consumers, CSPs are focused on addressing the monumental task of preserving trust in the communications ecosystem—going beyond conventional measures to position themselves as trusted entities and industry leaders, and appealing to consumers who prioritize security and reliability in their communication networks. Their fraud mitigation efforts reinforce the idea that these networks are a safe place to conduct business, and their ability to support emerging technologies and services safely and consistently means consumers can engage with business on their own terms.

Regulatory Compliance and Revenue Opportunities

Historically, regulation has been viewed as costly for CSPs but is increasingly being viewed differently. For example, the STIR/SHAKEN protocol—first implemented in the U.S. in 2021—was mandated by the FCC to mitigate illegal robocalls. It took several years to deploy and required collaboration around the industry.

Recent data emphasizes a decline in robocalls in the U.S. and indicates the efficacy of these collaborative efforts between regulators, telecom vendors and network operators. Forward-thinking CSPs are learning from their success and are making an intentional shift from viewing compliance as a regulatory necessity and financial burden to a strategic business move.

New offerings emerging from regulation not only help re-instill trust in their networks but also become marketable services. While STIR/SHAKEN is seeing positive results, efforts are underway to apply similar protocols internationally, aiming to verify and authenticate calls across borders to address the illegal robocall issue on a global scale.

Additionally, there are discussions to extend call authentication and verification to businesses that originate these calls, so consumers have more confidence that a business caller is who they say they are, ultimately helping consumers make an informed decision when deciding to answer the call. CSPs can also explore innovative business models beyond traditional revenue streams as well. Offering premium services related to enhanced call security, personalized authentication and advanced communication features can open new avenues for revenue generation while concurrently reinforcing the value proposition for their consumers.

Reduction of Churn: Preserving Trust to Avoid Consumer Exodus

The preservation of trust within the communications ecosystem is closely linked to the reduction of churn. Realizing that it is not just the CSP's problem to solve, the telecom ecosystem is collectively banding together to prioritize efforts to fight back against fraud and proactively identify and block the ways the fraudsters are penetrating the network.

Fraudsters understand the extreme complexity of the people, processes, tools, companies, regulations, involved. They know it is difficult to get everyone to row in the same direction, which is why when one access point is closed to them, they quickly move to the next. This leads to significant financial loss for businesses and consumers and ultimately churn. This churn, however, is not your traditional flavor of churn (i.e., one customer lost from one CSP who moves to another). Rather the concern is churn at a broader scale whereby large groups of consumers abandon traditional communication channels like voice and text altogether and move to newer, alternative channels.

Relevance: Ensuring Infrastructure Stays Current

Closely tied to relevance is adaptability, and telecom infrastructure is adapting to the changing needs of consumers and businesses, technology, and regulatory requirements. The ability to embrace change and proactively address emerging challenges ensures that the telecom industry remains a relevant and indispensable part of the digital ecosystem.

Being part of a more open community comes with both opportunities and challenges. CSPs are striking a balance between openness and security and fostering innovation while protecting the integrity of the communication network as a whole. This balance calls for collaboration with industry stakeholders, regulators, and technological innovators.

The Way Forward

While some illegal robocall mitigation efforts signal real and measurable progress, CSPs are continuing to find new ways to work with technology vendors and the broader industry to stay ahead of the network abuse that is happening now and that is expected in the future. More than just a technical challenge, the fight against robocalls is a comprehensive undertaking that encompasses trust-building, regulatory compliance, customer retention, and adaptability, all of which are critical to businesses that rely on the channel.

Using the tenets of the "5 Rs of CX" as a guidepost, CSPs have a framework for further diminishing the menace of robocalls, while ensuring trust in the communications ecosystem and strengthening the relevance of their infrastructure for a safer and more reliable digital future.