Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 6

The State of Robocalls And What's Next For Carriers

By: Jim Tyrrell

Robocalling, spamming, scamming, spoofing. Whatever you want to call it, these unwanted calls invade consumers' phones. This scenario is one that plays out for consumers multiple times a week—if not every day—given that robocalls remain the number-one complaint by volume to the FTC and FCC. In fact, an FTC report indicates that the agency received 4.5 million robocall complaints in 2017, up from 3.4 million the prior year.

Subscriber frustration with robocalls is also not lost on telecom carriers. In TNS' recently released 2018 Robocall Investigation Report—which analyzed more than 1 billion daily call events across hundreds of carriers—robocall user feedback to carriers nearly doubled during the first eight months of 2018.

The fact that consumers are more proactively offering up crowdsourced feedback is an asset carriers can leverage to draw a larger data-driven picture of emerging robocall trends and tactics. The ultimate goal is to better protect subscribers (consumers and businesses alike), while also delivering an enhanced user experience. For carriers to achieve these objectives, success first requires a more thorough understanding of how robocallers are succeeding, as well as strategies and solutions available to combat robocalling, spamming, scamming, and spoofing.

Current State of Robocalls

The Telephone Consumer Protection Act, or TCPA, was passed by Congress in 1991 to regulate the use of automatic telephone dialing systems ("auto-dialers") and prerecorded voice messages. The specifics of the regulation and the courts' interpretation are complex and sometimes difficult to decipher, but the essence of the law is to safeguard consumer privacy by mandating robocallers obtain explicit consent before placing any 'non-emergency' robocall to a consumer's cell phone.

Fraud has become easier for criminals as technology, such as VoIP calling, has enabled both the spoofing of a number and robo-dialing. Neighbor spoofing in particular has proven effective, as robocall scammers wager that Americans are more likely to trust and answer calls on their mobile phone when the incoming call shows a familiar local number.

Several methods have been developed to prevent unwanted robocalls. The United States has

developed the Do Not Call Registry, which was created in 2003 and allows consumers to “opt out” of receiving telemarketing calls on their landline and mobile phones, regardless of whether they are robocalls or not.

Despite these measures, the lists have been ineffective. Consequently, a market has developed for products that allow consumers to block robocalls. Most products use methods like those used to mitigate SPIT (spam over Internet telephony) and can be broadly categorized by the primary method used. Due to the complexity of the problem, however, no single method is sufficiently reliable.

Industry Solutions to Combat Robocalling

High risk (scam/fraudulent) and nuisance robocalls are up 15 percent in the first eight months of 2018, according to the TNS report. Carriers must evaluate industry solutions to combat robocalling, as well as how they fit into industry frameworks such as STIR/SHAKEN and policy initiatives at the federal and state level.

Hardware and Software

Many robocall solutions are limited to either utilizing hardware or software, such as traditional copper landlines, or mobile phone contracts from a specific mobile phone operator, which limits the scope of effectiveness. Additionally, most over-the-top (OTT) software solutions aren’t integrated with a carrier network. Therefore, they can only rely on the use of honeypots, blacklists and whitelists.

Blacklists and Whitelists

Many mobile apps prevent robocalls with a user-generated blacklist, but a major issue of these lists is the growing practice of caller ID spoofing. The low barrier to entry in the VoIP services market makes this tactic less and less effective over time.

Landline Call Blockers

Several physical products have been developed for use with landlines, which are typically installed in-home and employ a hard-coded or irregularly updated blacklist. Newer devices for landlines can use cloud-based data to resolve the hard-coded blacklist issues and allow you to create your own whitelist/blacklist.

Crowdsourcing

Robocall user feedback has nearly doubled. Growing consumer frustration with robocalls has translated into users more proactively providing crowdsourced feedback to carriers. According to the TNS study, subscribers report 57 percent of robocalls as spam, 22 percent as scam-fraud, 14 percent as telemarketers, and 7 percent as other.

Using crowdsourcing feedback allows the analytics provider to fine-tune algorithms and layer in context. Supplementing the unstructured data provided by the machine learning methods, crowdsourced data enables the analytics layer to provide information at a more granular level, such as whether a telephone number is being used as a claim to offer free cruises or is a legitimate call from a bank with a fraud alert related to a credit card.

Access to customer contacts, however, can be problematic. Many OTT software solutions require users to provide access to their personal whitelist of genuine contacts in exchange for access to the larger database. For their part, carriers can leverage industry-leading solutions that allow end users to provide direct feedback on robocalls, including the ability to classify robocall by type (spam,

scam/fraud, telemarketer, etc.).

Do Not Originate

Do-Not-Originate (DNO) involves the management of an outbound-calling blacklist consisting of telephone numbers that should never originate phone calls, such as government agencies, financial institutions and the 911 Do Not Call list. While implementation of DNO is straightforward from a technical perspective, the challenges lie in the creation, maintenance, and security of the list server. Once established, future additions to the list will have to be authenticated, and similar telephone numbers will not be included in the database. This omission poses the risk of it being used for fraudulent purposes.

STIR/SHAKEN

STIR/SHAKEN employs the same type of public/private key structure that has been used on the Internet to prevent the spoofing of websites. This process can attest to the authentication of the calling party telephone number—and is indisputably an essential foundational layer to combat spoofing—but is not able to address the question of intent. Bad actors will be able to make malicious calls from numbers that they have been assigned by a provider and will be able to burn through those numbers and then move on to the use of new numbers to avoid detection.

Real-time Analytics

If those whose work has been focused on detecting and addressing nuisance and illegal robocalls know one thing, it is that bad actors change tactics quickly. Use of spoofed numbers is one of those tactics, as robocall scammers believe users are more likely to answer the phone if Caller ID shows a familiar number.

Advanced machine learning methods for blocking robocalls using real-time AI in combination with big data gleaned from the network addresses the constantly changing identities of robocallers and can help carriers rapidly spot emerging trends and tactics. Machine learning is a method used to devise complex models and algorithms that lend themselves to predictive analytics. The analytical models allow data scientists to produce reliable and repeatable decisions while also uncovering hidden insights through learning from historical relationships and trends in the data.

And as referenced, crowdsourced feedback is another valuable data input for carriers. By supplementing the unstructured data provided by the machine learning methods, crowdsourced data allows the analytics layer to provide information at a more granular level to differentiate a call, for instance, from a financial institution about a fraud alert from a call asking a consumer to claim a free cruise.

Branded Calling For Enterprises

Consumers are not the only customer segment impacted by robocalls. Enterprises, particularly those whose business relies heavily on contact centers and calling campaigns to customers and prospects, must also navigate this new reality where their legitimate efforts are undermined by robocall bad actors.

Carriers should evaluate enhanced enterprise-focused tools such as Branded Calling, through which a logo and other business information may be displayed when the call is authenticated. There are also emerging solutions carriers can offer to provide aggregators and enterprises with a lens into their call centers' practices and allow them to understand what will and will not trigger negative reputational scores. The registration of calling campaigns, for example, could yield positive results, as analytics engines better understand sudden spikes in calling traffic.

Carriers—as well as other stakeholders throughout the telecommunications industry ecosystem—recognize the risks associated with the rising tide of bad actor robocalls. If consumer trust in voice calling weakens, so does the relationship carriers have with their subscribers. At the same time,

working proactively to develop innovative solutions to reduce robocall volume offers an opportunity for carriers to enhance the user experience and maintain a strong relationship with consumers and businesses.