White Paper

GlobalData

Taking on the Unwanted Robocall Challenge

Comparisons and Testing of Operator Solutions

White Paper developed by GlobalData

Sponsored by T-Mobile

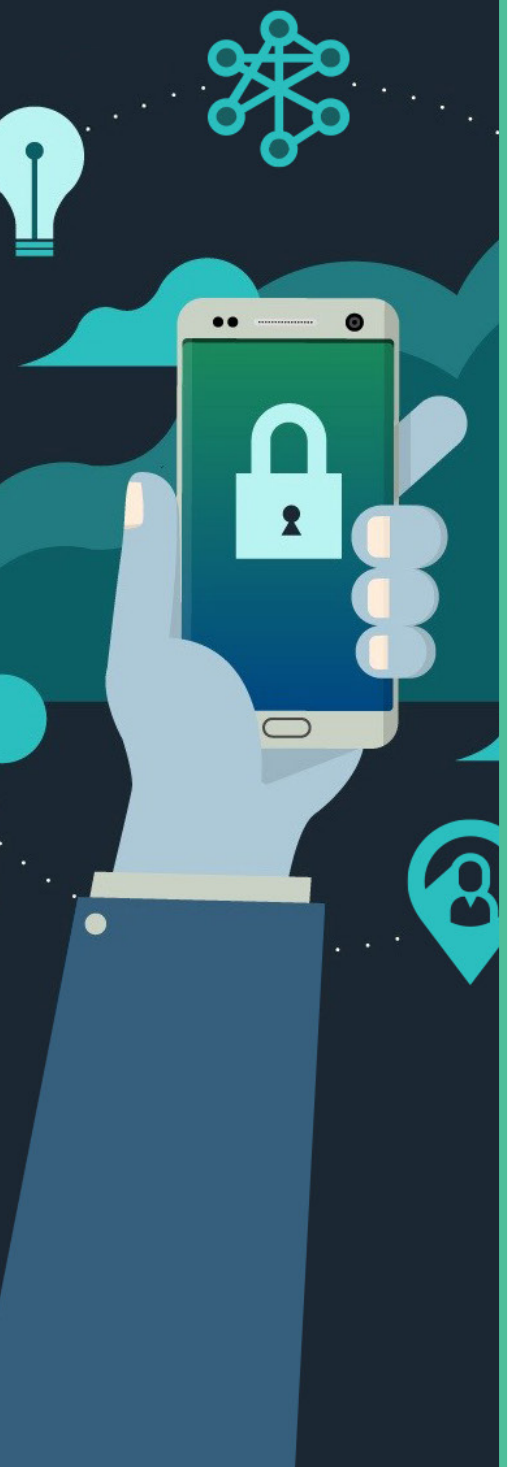


Table of Contents

1. Summary

U.S. phone users face a tsunami of unwanted calls, and the onslaught continues to worsen. The Federal Communications Commission (FCC) states that unwanted calls are its top consumer complaint. These calls are more than an annoyance, as many are categorized as high-risk scams or frauds that pose financial risks to unwitting victims or even result in identity theft. Furthermore, consumers and small businesses waste considerable time and money dealing with such calls. Though the FCC and federal government have recently undertaken high-profile actions to target this pain point, for several years T-Mobile has proactively deployed solutions to aggressively protect its customers from unwanted calls. In its latest initiative, Scam Shield, T-Mobile has added five new free scam protections for customers. These include free network-based scam protection tools to every T-Mobile and Metro by T-Mobile customer. Sprint, now a part of T-Mobile, can expect the same benefits when the networks are integrated. Today, Sprint customers will receive the premium Call Screener app with scam protection tools for free until they are on T-Mobile's network. Additionally, all T-Mobile, Sprint and Metro by T-Mobile consumers and small businesses receive Caller ID for free. Customers can also get a free second number to use as a "spam folder" and give out publicly while reserving their personal number for trusted callers; a free number change; and a new free app called Scam Shield (previously called Name ID) that activates these protections and lets customers enable Scam Block, access free Caller ID and more.

2. An Ongoing Battle

The term 'robocall' refers generally to any call processed by a computerized auto-dialer to deliver a recorded or, less often, live message.

There are numerous categories that fit under the 'unwanted call' umbrella. Some are legal and legitimate calls from entities such as bill collectors, political parties, market research companies and non-profits. In fact, the FTC's DNC registry permits those types of calls as well as purely informational calls that do not include a sales pitch. In addition, many robocalls are necessary and helpful – such as medical appointment confirmations or notifications of school closures – and customers usually want those calls delivered.

Today, the telecom industry is struggling with the unprecedented exponential growth in unwanted and often illegal robocalls. The recently enacted Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act and other existing initiatives undertaken by leading telephone companies and third parties are primarily aimed at ending illegal calls from fraudsters and others. However, to satisfy consumer demand, anti-robocalling solutions are increasingly targeting many categories of calls that consumers find bothersome, even if they are legal.

COMMON TYPES OF UNWANTED CALLS	
Spam	Nuisance call from categories not specified below or, alternatively, any unwanted call
Scam / Fraud	Call designed to steal property, identity, etc.
Telemarketing	Call to sell a product or service
Debt Collection	Call regarding outstanding debt
Political	Call touting political messages or candidates
Survey	Call to gather data / opinions
Non-profit / Charity	Call from a non-profit entity to inform or solicit money
Informational	Call regarding established business relationship, such as a prescription reminder
Public Information	Call from local government or emergency services regarding situations of interest to the community
Prison / Jail	Call originating from incarceration location

A February 2019 FCC report noted that third-party analysis showed the number of robocalls reaching U.S. consumers had exceeded more than 5 billion per month, including legal, illegal, wanted and unwanted calls. Given that most consumers do not pay for Caller ID service, many, if not most, U.S. consumers do not answer calls from unknown callers. This is more than an inconvenience, as it means people may be missing important calls from schools, employers and even first responders.

The ongoing COVID-19 crisis has given scammers new opportunities, and while scam call volume has gone down, the pandemic has led to a rash of scams focused on taking advantage of people's fears, ranging from bogus virus treatments, cheap health insurance and nonexistent work-at-home schemes to fake government messages regarding Medicare benefits, loans, cash grants and more. According to a March 2020 article published by Fast Company, coronavirus scam calls have included messages regarding the pandemic's impact on student loans, the marketing of questionable "safety and medical kits" and free at-home testing for Medicare recipients. A separate March article from the Washington Post noted that by one estimate consumers had been receiving 1 million coronavirus-related robocalls per day at the start of the pandemic. Through the end of June 2020, the Federal Trade Commission (FTC) estimated there had been $75 million in total fraud losses due to COVID-19 and stimulus payment scams that targeted consumers through websites, phone calls, emails and other contact methods. Total fraud losses from these types of scams grew 70.5% during the month of June.

The Telephone Consumer Protection Act of 1991 and the FTC's National Do Not Call (DNC) Registry, created in 2003, are among federal legal and regulatory initiatives undertaken over the years to slash the number of unwanted calls. These solutions were created many years ago, before most voice traffic moved to VoIP, before massive privacy data breaches, and before changes in technology that made it easy for scammers to engage in cheap, automated robocalling campaigns. Today, these outdated policies have done little to rein in bad actors. The FTC notes that during fiscal 2019, it received 5.4 million complaints about callers violating the DNC registry, with 71% of complaints reporting a robocall was received. Calls from imposters (spoofing) were the most-reported type of unwanted call. Of course, those official complaints represent a mere drop in the bucket of the actual number of unwanted calls being received by consumers on an annual basis. In addition, the FTC notes that consumers reported losing more than $1.9 billion to fraud in 2019, with imposter scams representing nearly $667 million of that loss. Phone calls are the most common method of scam communication by fraudsters, and the consumers who said they lost money due to being defrauded over the phone reported a median individual loss of more than $1,000.

3. Solutions Abound

In the U.S. wireless market, the three largest national wireless operators have taken similar approaches to addressing the issues of scam calls and unwanted robocalls.

Each currently offers a basic call identification service to warn against potential spam, scam or other nuisance calls, which may also provide some level of blocking options. Each also offers a premium service, which may cost extra each month but also provides services such as call blocking by additional categories.

One of the earliest operators to address the robocalling scourge is T-Mobile. Recognizing the negative impact of scam calls on its customers, the operator made aggressive moves early on to tackle this industrywide challenge. Over three years ago, in March 2017, T-Mobile rolled out Scam ID and Scam Block – free, network-level scam solutions that do not require a customer to download an app to their phone for its postpaid and Metro by T-Mobile wireless customers.

In 2020, T-Mobile has announced it is rolling out free scam identification and blocking to every T-Mobile, Metro by T-Mobile and Sprint customer, removing any plan requirement, which is a first in the wireless industry.

T-Mobile's scam detection technology operates within its network, not on the device and is therefore able to be device agnostic. It employs artificial intelligence and machine learning to analyze several aspects of the call data in order to detect calls that are likely fraudulent.

The system looks at call behavior, not just known bad numbers, and data is validated and updated every six minutes, helping ensure customers are protected from the latest scams around the clock.

The first product, Scam ID, is on by default and alerts a customer when a call is likely to be scam, labeling it "Scam Likely" on the caller display, and enabling them to decide whether to answer or decline the call. To block all "Scam Likely" calls, customers can dial #662# to activate free Scam Block, which, true to its name, automatically blocks any call identified as "Scam Likely" and stops them at the network level, so they never reach a customer's device. Scam ID and Scam Block are now available free to all T-Mobile and Metro by T-Mobile customers. Additionally, as part of T-Mobile, Sprint customers now get the highest level of protections for identifying and blocking scam through the Call Screener app for free.

Also new in 2020 is the provision of free Caller ID to all T-Mobile, Sprint and Metro consumer and small business customers. This sets T-Mobile apart as its competitors require their customers to sign up and pay for premium call solutions to get Caller ID. Furthermore, T-Mobile now offers its Magenta customers a free second line to use as a 'virtual spam inbox.' This extra line, called PROXY by DIGITS, is operated through T-Mobile's DIGITS app and can be shared across several lines on an account and can be set to "do not disturb" so the user(s) can check the texts and voicemail when it's convenient to them. By giving customers a free second number, T-Mobile enables customers to provide that number publicly while only giving out their personal number to friends, family, and other trusted parties.

Furthermore, T-Mobile now lets T-Mobile, Sprint and Metro by T-Mobile customers change their phone number for free if they just want a fresh start. T-Mobile's free number change option is a positive move, as some customers' phone numbers have become so widely distributed among spammers that starting fresh with a new number is their best option. Rival operators often charge customers to change their number.

The new, free Scam Shield app activates all of T-Mobile's new protections enabling a customer to turn on and control some of these features and learn more about the others. T-Mobile also offers Scam Shield Premium as a value-added monthly subscription service that offers advanced call control and management features for unwanted legal robocalls. This includes being able to control which robocalls can reach you by category: telemarketing, charities, surveys, etc.

Other large U.S. wireless operators have also recently broadened the reach and capabilities of their robocall products. Following is a table comparing the robocall solutions offered by the nation's three largest operators.

Selected Features of Carrier Call Filtering Solutions

Operator	AT&T		T-Mobile			Verizon	
Product(s) Name	***Call Protect***	***Call Protect Plus***	***Scam ID***	***Scam Block***	***Scam Shield Premium***	***Call Filter***	***Call Filter Plus***
Cost	*Free*	*$3.99/month*	*Free*	*Free*	*$4/month*	*Free*	*$2.99/m/line; $7.99/m/account*
Caller ID		✓	✓	✓	✓		✓
Reverse Number Lookup		✓			✓		✓
Spam Detection	✓	✓	✓	✓	✓	✓	✓
Personal Block List	✓	✓			✓	✓	✓
Call Block/Redirect Controls	✓	✓		✓	✓	✓	✓
Custom Categories for Blocking / Redirect							
Fraud / Scam Risk	✓	✓	✓	✓	✓	✓	✓
Spam - All Risk Levels	✓	✓	✓	✓	✓	✓	✓
Spam - Medium and High Risk						✓	✓
Incoming International Calls						✓	✓
Nuisance Calls					✓		
Unknown Callers (not in Contacts)	✓	✓					
Private Calls		✓					
Account Services		✓					
Telemarketers		✓			✓		
Surveys		✓			✓		
Political Calls		✓			✓		
Nonprofit / Charity		✓			✓		
Jail/Prison Calls					✓		

Note: as of March 2020

4. Robocall Solutions Testing

GlobalData recently tested operator-offered robocalling solutions from AT&T, Verizon and T-Mobile over the span of four weeks, looking primarily at their ability to identify and alert the customer of calls that were considered likely to be spam, fraudulent/scam, or telemarketing. Some of this testing was conducted independently while some was conducted in cooperation with First Orion, which is one of T-Mobile's robocalling-solution vendors. The test involved a total of 205 incoming calls, the majority of which were categorized as spam, fraudulent/scam or telemarketing calls.

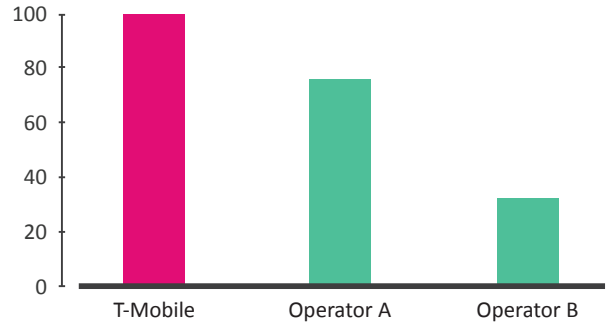
Incoming calls were classified via alerts displayed on receiving phones or by answering the calls and identi¬fying the caller. Other calls were generated for testing purposes by First Orion and GlobalData, using technology that spoofs numbers which are commonly used for known spam and scam/fraud calls.

Some calls generated by First Orion and GlobalData spoofed numbers identified as being used by likely scam callers but were recognized as telemarketing calls by an operator. GlobalData credited those as scam alerts, as the definitions can vary and the end user was alerted that there was an issue with the call.

The tests revealed that T-Mobile's Scam ID and Scam Block services sent 'Scam Likely' alerts to users' phones 100.0% of the time when calls were received from likely scam numbers, and the operator's premium Name ID (becoming Scam Shield) service sent 'Telemarketing' alerts 100% of the time when calls were received from likely telemarketers' numbers. The next closest competitor's solutions blocked or issued alerts for 76.5% of likely spam or fraud calls, but its premium solution issued alerts for only 33.3% of calls from likely telemarketing numbers.

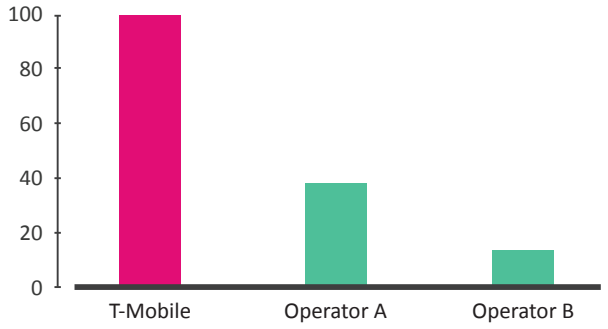
Overall, T-Mobile's free Scam ID and Scam Block were 30.8% more effective at identifying and catching scam/spam calls than the next closest competitor's solutions. Looking at the percentage of spam, scam and telemarketing calls identified and blocked across the operators' basic and premium robocalling possible solutions, as well as unprotected lines, T-Mobile still came out ahead of its rivals.

% Spam & Scam Calls Identified and Blocked

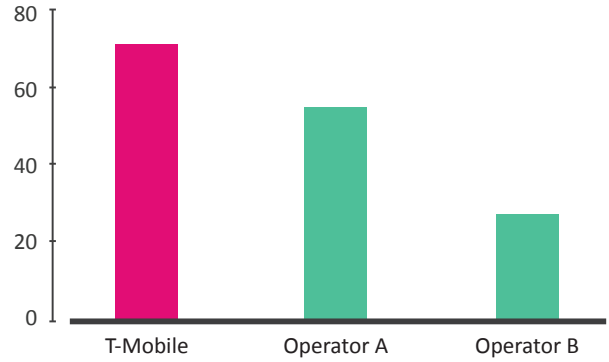


Telemarketing Calls Identified and Blocked*

*Only calls ID'd / blocked by operators' premium solutions



% of Spam & Scam plus Telemarketing Calls Identified and Blocked



5. Third-Party Approaches

Wireless customers also have other options outside of their service providers for taking on robocallers. Android and Apple iOS each have options that let a user block specific numbers as well as 'do not disturb' modes that can block all calls and notifications. However, many of these solutions are device specific and often a user must block each number individually.

There is also a growing number of third-party applications that can provide control over unwanted calls. Chief among these are apps from companies such as Nomorobo, RoboKiller, Truecaller, Hiya and YouMail. Some have free versions that are supported by in-app advertising as well as paid premium versions that do not have ads and offer more features. Consumers who want to use a third-party app to manage and block calls should ensure they are dealing with a reputable company, because these apps need permissions to access phone features such as one's private contact list. Apps from unknown providers might include spyware or other malicious software which could expose a user's private data to bad actors.

In addition, many of these apps include value-added features that are unique to the app provider and may not be desirable to the average consumer. For example, in the case of YouMail, users set up YouMail as their default voicemail service, replacing their carrier-provided voicemail, for use in filtering and blocking incoming calls. Truecaller offers three versions of its app, with the Premium and Gold versions adding features unrelated to incoming robocall identification and blocking, such as 'premium badges' that are designed to make the user's Caller ID persona stand out when they make calls. Rather than providing network-based solutions or apps customized for their users, some smaller wireless service providers, such as Comcast's Xfinity Mobile, promote third-party apps to their customers, who are encouraged to download the same apps that are available to the general public.

Pricing and Selected Features of Third-Party App Solutions

App Provider	NOMOROBO	ROBOKILLER	TRUECALLER		
Cost	$1.99/month or $19.99/year	$2.99/month or $29.99/year	Basic Free (with banner ads)	Premium $2.99/month or $27/year	Gold $249/year
			✓		
Spam/Scam Identifier	✓	✓	✓	✓	✓
Call Block/Route to Voicemail	✓	✓	✓	✓	✓
Block Callers Not on Contact List	✓	✓	✓	✓	✓
No banner ads in app	✓	✓		✓	✓
Caller ID		✓	✓	✓	✓
Block Spam Texts	✓	✓	✓	✓	✓
Call Recording		✓		✓	✓

Note: as of March 2020

Despite positive reviews for many of the third-party anti-robocalling apps, consumers might be more comfortable turning to their wireless service providers for robocall protections, since they already have the customer's account information, billing details and call data.

Customers should consider the benefits of a network-based approach to scam identification and blocking. Technology that sits inside the network can analyze call behavior and be updated constantly, unlike app-based approaches which sit outside the network and can become outdated between app updates. This drawback to app-based approaches applies not only to third-party app services, but app-based robocalling solutions offered by operators as well. Furthermore, network-based technologies that examine call behaviors across the entire data set of the network can be used to quickly determine new spam call techniques and shut them down.

T-Mobile is one of the few operators that deploys a network-based approach with its Scam ID and Scam Block tools. This approach enables T-Mobile to offer its incoming call solutions to all its customers, even those customers of T-Mobile MVNOs that choose to offer these solutions. With its Scam Shield initiative, T-Mobile is the first operator to provide free protections across its branded customer base, including every customer at T-Mobile, Sprint and Metro.

That is not possible with the app-based approach with the best features reserved for customers on the most expensive plans or whose capabilities can be significantly impacted by the phone being used. For example, Verizon has a list of eligible devices on its website that can use its basic and premium anti-robocalling services. However, some devices are only capable of identifying unknown callers, while others support a mix of spam filtering and blocking capabilities. Yet, because all are considered eligible devices, a customer can download Verizon's anti-robocalling app to a device and even pay for the operator's premium service but still not have access to the app's most desired features, such as call filtering and blocking.

6. Looking Ahead

There are promising developments ahead as regulators, lawmakers, and service providers band together to limit the negative impacts of unwanted calls. T-Mobile and other network operators have been working diligently to roll out cross-network number authentication based on STIR/SHAKEN (also called 'SHAKEN/STIR') standards to protect consumers from unwanted robocalls. STIR/ SHAKEN authenticates the phone number of incoming calls to let people know when a call has been verified as really coming from the number listed on the Caller ID display rather than from a scammer that has spoofed a number to conceal their identity. This is one more key tool in the battle against unwanted calls that will benefit all consumers over time.

STIR/SHAKEN technology is mandated in the recently enacted TRACED Act, which is aimed at reducing the number of annoying and unsolicited robocalls that target U.S. consumers. Part of the new law requires phone companies to offer free scam blocking tools and become more active in blocking robocalls and ensuring calls are coming from verified numbers. STIR/SHAKEN is now an industry mandate. All operators must be in compliance by June 2021. Some operators such as T-Mobile began testing and deploying this new technology as early as Nov 2018 and have already launched a number of industry interoperability partnerships while others are still working on deployment. When all the major operators have deployed STIR/SHAKEN and are able to verify the majority of numbers, we should see an improvement in the fight against number spoofing as a scammer tactic.

7. Conclusion

Consumers have many choices among apps and services that can aid them in escaping the annoyance and threats posed by these intrusive and sometime dangerous calls. Network-based approaches such as those employed by T-Mobile can serve more of an operator's customer base because they do not require users to download apps. Furthermore, they have been shown to deliver superior results. Not all robocalling solutions are created equal, and consumers should educate themselves about the differences in order to select the best option that suits their needs.