

THE WALL STREET JOURNAL.

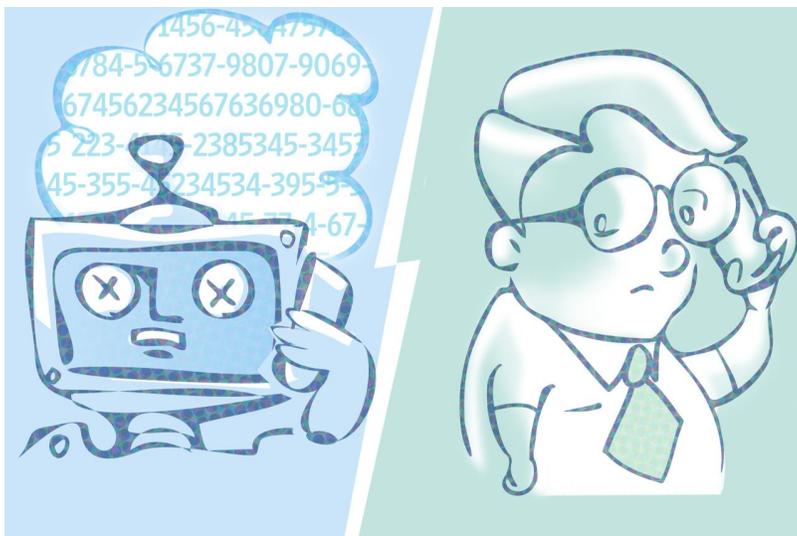
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/why-there-are-so-many-robocalls-heres-what-you-can-do-about-them-1530610203>

PERSONAL TECHNOLOGY: REVIEW

Why Are There So Many Robocalls? Here's What You Can Do About Them

Robocalls won't vanish soon, but carriers are working on a spam filter and other fixes



By *Katherine Bindley*

Updated July 4, 2018 1:30 p.m. ET

Remember when phone calls meant people wanted to talk to you about something other than lowering your interest rates? These days, the phone rings so often with recorded robocall messages—You qualify! You owe! You've won!—answering feels like a hazard.

I hit my own robocall breaking point a month ago. I was grabbing a quick shower before catching a flight. My phone rang. Fearing I'd miss a call from my boss, who had been trying to reach me, I jumped out. But no, it was a recording instead.

Newsletter Sign-up

Technology

A weekly digest of tech reviews, headlines, columns and your questions answered by WSJ's Personal Tech gurus.

SIGN UP

PREVIEW →

I resisted the urge to throw my phone across the bathroom and went looking for answers. Why can't anyone stop this madness? When will it end?

First, the bad news: Almost every person I talked to about robocalls used the phrase, "There's no silver bullet."

But developments in the works should get the robocall problem more under control. And there are steps to take on your own that actually do reduce calls.

Where did this evil come from?

Back when phone calls were transmitted over copper wires, businesses paid a lot of money for phone systems that allowed 1,000 employees to make calls without needing 1,000 phone lines. These systems inserted caller ID so, for instance, customers all saw the same business number, regardless of which employee made the call.

With the internet, businesses don't need expensive hardware. Anyone can start a mini call center with software that auto-dials numbers and spoofs caller ID. They also need a provider to "originate" the call, that is, connect the internet call to the phone network.

Some robocalls are legitimate—your pharmacy, your bank—but not the ones that change numbers constantly to appear local and avoid detection. Robocallers even spoof numbers held by ordinary phone customers like you and me (so don't call them back to yell at them.)

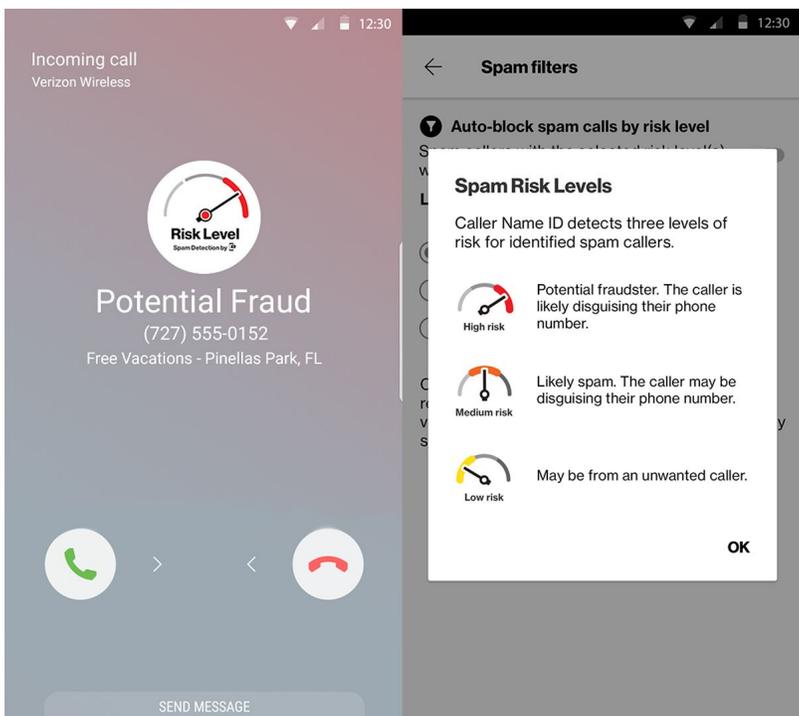
A real fix is coming?

With caller ID basically broken, developers have proposed a call-certifying protocol (known as STIR) and guidelines for implementing it (known as SHAKEN). The names behind these acronyms are long and confusing.

With it, an originating phone carrier could check that a caller has the right to use a number and create a digital fingerprint for the call. The carrier on the receiving end could verify that nothing was messed with in transit.

"They're actually not saying that the call comes from the phone number. What they're saying is this user is entitled to use this phone number," says Jim McEachern, a principal technologist with the Alliance for Telecommunications Industry Solutions, a technical working group that helped develop guidelines for this call-certification protocol.

If a bad guy tries to spoof the caller ID, the call would go through, but it wouldn't be verified. Eventually, users would see a check mark or other indicator for verified calls.



Verizon's Caller Name ID service can send spam numbers to voice mail. PHOTO: VERIZON

Mr. McEachern likens the current state of robocalls to the days before email spam filters. "I think something similar will happen with this," he says. "Suddenly people will say, 'Remember how bad that used to be?'"

Mr. McEachern estimates that could take two to five years. Verizon plans to start rolling the system out later this year and other carriers are expected to follow.

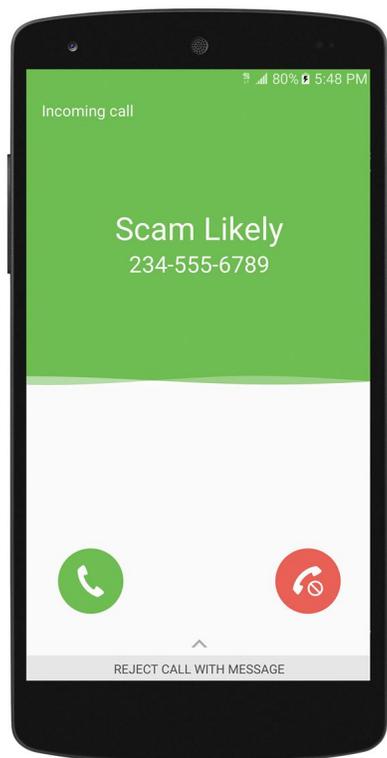
"We are optimistic it will have an impact but again, this alone is not going to solve the problem," says Matthew Berry, chief of staff at the Federal Communications Commission, which comes up with rules for the industry, fines people and companies for violations and develops public policy initiatives.

The 'Do Not Originate' list

Before then, other weaker measures are appearing. Last November, the FCC adopted rules that let phone companies block calls from area codes that don't exist, numbers that aren't assigned to anyone and entries on a "Do Not Originate" list, which consists of numbers that aren't used for outbound calls.



Mr. Berry says the rules have been effective in stopping IRS scam calls. Scammers had been spoofing an IRS hotline number that is now on the Do Not Originate list.



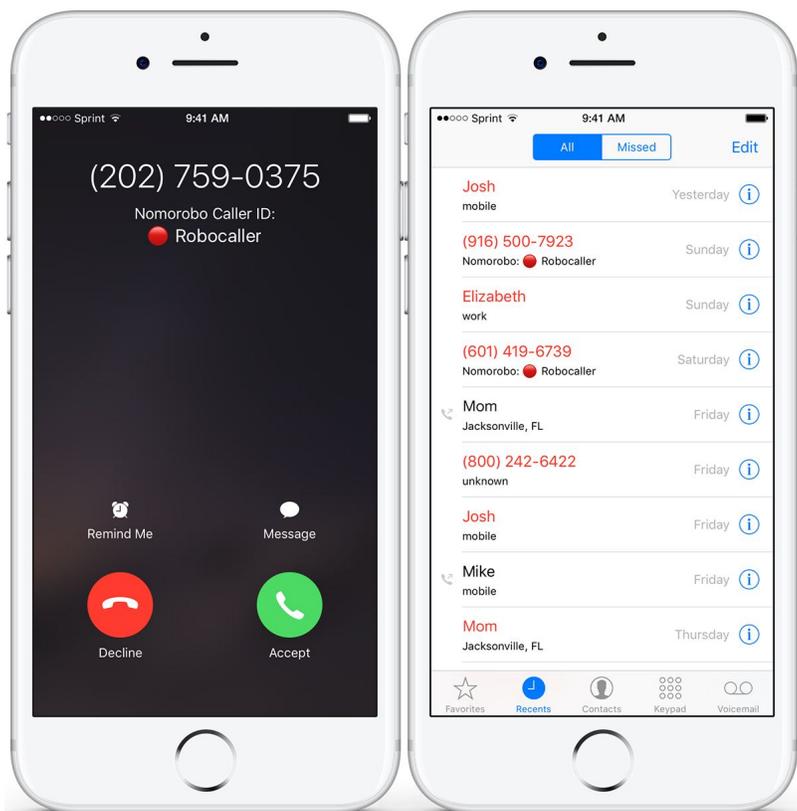
But IRS scam calls can come from a variety of numbers. Aaron Foss, founder of the call-blocking app Nomorobo, says his app identified 75 different numbers peddling IRS scams in just one day.

What you can do now

When you get a robocall, hang up. Don't say anything, don't press buttons and don't call back. Once scammers know a number works, they can sell it and your call volume could increase.

It can feel like there's no point in blocking numbers in your

T-Mobile provides scam ID and automatic scam-call blocking free. PHOTO: T-MOBILE



Nomorobo identifies likely scam calls and can send them straight to voice mail PHOTO: NOMOROBO

phone—I blocked one peddling chronic pain management and got the same recording from another within 48 hours. But do it anyway, because there are plenty of repeat offenders out there. Here's how to do it on iOS and Android.

Also, add yourself to the Federal Trade

Commission's Do Not Call Registry.

Just know that you will still get unwanted calls, because scammers don't obey rules. Also, keep filing robocall complaints. It helps the FTC spot evildoers.

Carrier protection

Service providers have upped their robocall-protection offerings recently so check in with your carrier. They include features to identify possible scam calls—and even gauge the likelihood it is a scam—as well as block them or send them to voice mail.



Hiya is a free call-blocking app. PHOTO: HIYA

calls based on the likelihood they are scams. Android users will get this feature later this summer.

Call-blocking apps

You can also try apps made by outside developers.

Nomorobo, \$2 a month, identifies likely scam calls and can send them straight to voice mail. Unlike some other services, you don't have to share your contact list for it to work.

Its algorithm uses multiple data sources, including complaints from the FTC and the FCC and real-time data it gets from its landline customers. The company also owns about 250,000 phone numbers, and monitors their incoming calls for scammers.

Hiya is a free call-blocking app that works by analyzing data from complaints made to the FTC and the FCC, and information it collects from its Android users. Hiya is the technology behind the call-identifying feature that powers AT&T's Call Protect service.

T-Mobile provides scam ID and automatic scam-call blocking free.

AT&T call-protection services are also free, and include blocking suspected fraud. It also offers a \$4-a-month service that lets you block specific categories of calls, and includes reverse phone-number lookup.

Verizon's recently improved \$3-a-month Caller Name ID service for wireless can now send spam numbers to voice mail.

Sprint's newly updated Premium Caller ID, also \$3 a month, lets iOS users automatically reject

Whether iOS or Android, you do need to share your contact list with Hiya, but the service doesn't upload or store it. It also says it won't sell any data from your phone to third parties.

After this article was published online, Hiya clarified its privacy policy and some of the language on its website to reflect that people can use a limited version of its app, including the core features, without granting access to contacts. Granting that access is only necessary to access all of the app's features, it said.

Appeared in the July 5, 2018, print edition as 'Here's What You Can Do About Robocalls.'

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.