BUSINESS

‘Stop Robocalling Me!’; ‘I Didn’t!’

Americans’ battle against illegal robocallers has reached a boiling point, with victims of one form of phone-related malfeasance now lashing out at those impacted by a different form: phone-number spoofing.

By Sarah Krouse

Jeffrey Lewis Knapp saves the four to six telephone numbers his caller ID logs each day. At night he seeks his revenge, calling back the people he thinks are illegal robocallers. “How can I help you?” the Arizona-based retiree says he asks the people who answer.The problem with Mr. Knapp’s approach: He sometimes calls people who didn’t, in fact, call him first. Instead, the individuals he calls are themselves victims of a phone-related crime called malicious number spoofing, in

related crime called malicious number spoofing, in which callers falsify their number to disguise their

identities.“A lot of times they don’t know that their number was used,” said Mr. Knapp, 66. “I had one guy get a little irritated and hung up, but most are pretty positive.”Americans’ growing battle against illegal robocallers has reached a boiling point, with victims of one form of phone-related malfeasance now lashing out at those impacted by a different form of it.Hiya, one of many mobile phone applications with call-blocking features, estimates that there were 8 billion robocalls to U.S. cellphones in the final quarter of 2018, up from about 5 billion in the first quarter.

AlsoEveryone Loathes Robocalls. Some People Try to Get Even. (Dec. 20)

Why Robocallers Win Even if You Don’t Answer (June 4)

Many illegal robocalls use number spoofing to obscure their identities. The practice allows bad actors to display to recipients numbers that aren’t actually the ones they are calling from.Meir Cohen, chief executive of TelTech Systems Inc., which sells an unwanted-call blocking app called RoboKiller, said phone numbers are often misused when robocallers deliberately generate numbers that appear to be in the same area code as the recipient. It is meant to lead victims to believe the call is legitimate and answer their phone.Web-based calling technology makes it easy for robocallers to display a randomly generated number. The phone numbers spoofed, however, may belong to a real person or business that is unaware that the number is being used that way.

There is no fail-safe way for consumers to keep their numbers from being spoofed and even changing

numbers won't guarantee that the problem will go away, robocall prevention specialists say.

The Federal Communications Commission has said that combating illegal robocalls and malicious phone-number spoofing is its top consumer protection priority and that consumers and businesses impacted by the problem can file a complaint with the agency or record a voice-mail message that says they don't make marketing calls.

But clamping down on spoofing is difficult."A lot of spoofing can happen overseas and when it happens from overseas it can be very difficult to trace the origins of a call," said Christine Reilly, a partner at Manatt, Phelps & Phillips, LLP, who works with companies on compliance with consumer protection laws.

There are also legitimate uses of spoofing, which makes an outright ban on such technology problematic.

A doctor who wants to call patients back from her cellphone may want to spoof her office number to avoid giving out personal contact information. A domestic violence shelter, where privacy is paramount, may similarly wish to disguise its number when it calls the home of a client.

The FCC has so far handed hefty penalties to bad actors and allowed carriers to block calls from fake area codes as well as numbers that aren't used for outbound calls.The agency in September proposed a $37.5 million fine against a Tucson-based company for maliciously spoofing numbers in millions of telemarketing calls over a period of 14 months starting in 2016. In that case, at least one person in Arizona received more than five calls a day from people complaining that she had called them when in fact the

company had used her number.

The telecommunications industry, meanwhile, is working on a call-certifying protocol (known as STIR) as well as guidelines for implementing it (known as SHAKEN) in the coming years. Under that system, carriers on the originating end of a phone call would check to make sure that the caller has the right to use a given number while the carrier on the receiving end would certify that nothing had changed as the call was routed and received.Consumers will eventually see an indicator on their phone signaling whether a call has been verified. If a bad actor spoofed a number, that verification would not occur.Efforts to stop phone-number abuse such as spoofing have had a limited impact so far, with some victims of angry calls fearful for their safety or finding themselves taking heat from strangers.

Angela Santiago changed her phone number of 20 years after receiving an angry call from a woman accusing her of robocalling. After doing so, however, the same thing happened with her new number.

“It’s a violation and a huge inconvenience,” Ms. Santiago said.

Write to Sarah Krouse at sarah.krouse@wsj.com