Ritter Communications FCC Traced-ACT/Robocall Mitigation Information

Ritter Communications knows it's annoying to receive unwanted, nuisance calls and even worse to be plagued by suspected illegal robocalls to defraud you of your hard-earned money.

To help reduce the number of suspected illegal calls that may originate from our network, Ritter Communications has teamed up with industry leader TNS(Transaction Network Services) to deploy their Call Guardian solution at no additional charge to our customers. By doing so Ritter is in full compliance with the FCC's Traced Act.

Call Guardian Authentication Hub automatically prevents unwanted robocalls and prohibits them from every reaching your phone. Features include:

- Free to opt in
- Includes STIR/SHAKEN call authentication as well as blocking technology.
- Take control of your phone - no more unwanted calls
- Works automatically - no configuration required.
- Blocks political campaigns, charities, IRS scams, and more.
- Allows valid calls to pass.

In addition, Ritter Communications has implemented STIR/SHAKEN on our IP based Voice routing to aid in the verification of legal vs. illegal calls to our customers.

By blocking certain calls entering and exiting our network along with Stir/Shaken, Ritter hopes to reduce the amount illegal robocalls and grant our customers peace of mind to answer when your phone rings.

What do I do if I believe my calls are incorrectly being blocked?

If you suspect calls may be getting blocked by mistake, please reach out to our support teams at https://www.rittercommunications.com/contact or 1.888.659.6009 to report service interruption. Upon receiving the report, Ritter Communications will review the data and take action as needed. Additional information can be found in the Ritter Communications Terms & Conditions of Service.

What if I don't want any potential calls blocked?

Ritter has automatically opted in all voice subscribers to the call blocking service. Customers have the option to opt out of these services by contacting our support teams and formally requesting to be removed from the CGAH service.

 Contact- https://www.rittercommunications.com/contact or 1.888.659.6009

What is the definition of a robocall and spoofing?

Robocalls are automated phone calls with prerecorded or artificial voice messages. Many are legal and just simply unwanted calls while others can be illegal as the sole intent is to defraud a party of money.

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity.

- Spoofing is not always illegal. There are legitimate, legal uses for spoofing. For example, a doctor calls a patient from her personal mobile phone and displays the office number rather than the personal phone number, or a business displays its toll-free call-back number.
- Spoofing is illegal when the caller falsifies the caller ID display information to disguise their identity with the intent to defraud, cause harm or wrongly obtain anything of value.

Fraudulent Calls are calls originating from invalid, unallocated and unassigned telephone numbers, as well as calls originating from inbound-only numbers that should never make outbound calls.

How does STIR/SHAKEN help combat illegal and nuisance calls?

STIR/SHAKEN is a caller-ID authentication system using the same secure cryptographic techniques that keep your information safe when you interact with online shopping or banking websites and apps. It means that the service provider receiving a call knows how much to trust the caller-ID on the call.

By itself, it makes it harder for someone making illegal or nuisance calls to hide behind a fake caller-ID, and therefore more likely they will be caught, acting as a deterrent.

STIR/SHAKEN has other potential benefits when combined with robocall analytics and blocking services used by service providers: the fact that a call has or hasn't been authenticated is another factor that can be used to help separate good calls from bad calls, making it more likely the good ones get through and the bad ones get blocked.

Ritter Communications uses Call Guardian Authentication Hub, a best-in-class combination of STIR/SHAKEN and robocall analytics from Metaswitch and TNS that provides protection against illegal and nuisance calls to our subscribers.

How does it work?

Unlike other features that only reject calls from a specific set of callers that you select, Call Guardian validates the calling number against huge national databases of unwanted callers. Those databases are dynamically changing, and new calling numbers used by unwanted callers will be blocked within minutes of them starting to be used.

What Robocalls are legal?

- Political calls about candidates running for office - allowed without permission
- Surveys
- Robocalls that are purely informational
- Flight cancellations
- Appointment reminders
- Delayed school openings

Calls from some health care providers. This includes a robocall from a pharmacy reminding you to refill /pick up a prescription. Consumers consent to receive these calls.

Debt collection calls. A business contacting you to collect a debt can use robocalls to reach you. Robocalls that try to sell you services to reduce your debt are illegal and are almost certainly scams.

Charities asking for donations. Charities can make these calls themselves. But if a charity hires someone to make robocalls on its behalf, the robocalls can only go to members of the charity or prior donors. They also must include an automated option to let you stop future calls.

Are all unwanted calls blocked?

Call Guardian does not guarantee to block 100% of unwanted calls, but it will very significantly reduce the number that manage to get through.

Will it block any calls I do want to receive?

Call Guardian uses highly intelligent algorithms to determine what calls to block. In particular it is carefully designed not to block calls from high volume callers that you still need to receive, such as mass announcements from schools to announce snow closures or calls from hospitals to confirm appointments.

Where can I review your Robocall Mitigation Program?

In compliance with FCC requirements, you can read Ritter Communications Robocall Mitigation Program here.