product brochure

Combating Illegal Robocalling and Spoofing in the United States

iconectiv is the U.S. STI Policy Administrator

Answering the call in the United States

Your telephone is constantly by your side – an essential tool for interacting with the world. It is an extension of your identity and of your life. Despite the constant accessibility and desire to access and exchange information simply, seamlessly and securely, consumer confidence in the phone continues to wane because of bad actors who misuse and abuse communication networks.

Research shows that 76% of calls are left unanswered when the call comes from an unidentified or unfamiliar number, which means that we are no longer answering many of the calls we want from schools, doctors, business associates and others because we fear that it's a fake call. Wrought with inefficiencies and frustration for consumers and businesses, this is compromising the way we communicate.

How did this happen?

The situation was exasperated with advances in VoIP technology, which allow a massive number of phone calls to be initiated very cheaply and where the calling party can manipulate what appears on the caller ID. Known as 'spoofing,' the technique, which cannot easily be traced to the originating call center, can mislead people by displaying a text string such as "Free Money," or provide an 800 number.

However, spoofing can cause more harm than just mere annoyance. Criminals use spoofing to present themselves as something they are not, such as impersonating law enforcement, financial institutions, schools, creditors or government entities to obtain sensitive personal data or extract credit card "payments" and wire transfers, defrauding consumers for billions each year.

Combatting Robocalling and Spoofing

What can be done? Authentication and verification breakthrough

In the United States, the Federal Communications Commission (FCC) and the telecommunications industry have taken decisive action to protect consumers by halting illegal robocalls and Caller ID spoofing.

Academic researchers and leading telecom associations, industry members and standards organizations such as the Internet Engineering Task Force (IETF) and the Alliance for Telecommunications Industry Solutions (ATIS) who is working jointly with the SIP Forum, are developing solutions to help the industry mitigate illegal robocalling and spoofing.

Together industry leaders such as iconectiv, ATIS and the SIP Forum developed SHAKEN (Signature-based Handling of Asserted information using toKENs), a set of specifications that provides a framework for service providers to implement new certificate-based anti-robocalling and spoofing measures.

SHAKEN uses encrypted digital signatures for each call that provides authentic and more complete information to the terminating service provider about the calling party. SHAKEN gives service providers the tools needed to sign and verify calling numbers as well as where the call originates. This information will be used by call blocking and analytics applications to determine what to do with the call and enables consumers to know, before answering, that the calls they receive are from legitimate parties.

Legislative and regulatory initiatives

The FCC has released rules as well as additional Notices of Proposed Rulemaking and Congress has introduced several pieces of Legislation to combat illegal robocalling and spoofing.

In September 2018, the STI-Governance Authority (STI-GA), an industry group that was created to support the timely deployment of SHAKEN. Since SHAKEN relies on digital certificates to ensure that the CallerID is cryptographically authenticated, a Secure Telephone Identity Policy Administrator (STI-PA) was required. In May 2019, the STI-GA selected iconectiv as the STI-PA to ensure that the certification authorities implement appropriate certificate management practices and that only authorized service providers are issued certificates for signing calls.

Ready for implementation

iconectiv will work with service providers and the certificate authorities to deploy this solution, which is the foundation for securely enhancing the information provided to call blocking and analytics apps and ensuring that consumers can trust what they see and thus make informed decisions when answering a call. Uniquely positioned to lead in the mitigation of illegal spoofing and robocalling, iconectiv's core competencies include highly scalable software as a service (SaaS) based information management providing authoritative numbering services, trusted communications and fraud prevention for the telecommunications industry.

Part of the iconectiv Trusted Communications portfolio, this anti-spoofing solution allows caller ID information to be authenticated and the origin of the call captured and securely conveyed between service provider networks. Together, these will make a significant difference in reducing illegal robocalls and ensuring that consumers have the information they need to make an informed decision as to whether or not to answer a call.

To find out more

If you are a service provider, enterprise or partner who wishes to establish a trusted environment for subscribers to communicate with commercial entities, contact us to learn more.

make the connection

For more information about iconectiv, contact your local account executive, or you can reach us at: +1 732.699.6800
info@iconectiv.com www.iconectiv.com

about iconectiv

Your business and your customers need to access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services and its unmatched numbering intelligence helps you do just that. In fact, more than 2B people count on our platforms each day to keep their networks, devices and applications connected. Our cloud-based Software as a Service (SaaS) solutions span network and operations management, numbering, trusted communications and fraud prevention. For more information, visit www.iconectiv.com. Follow us on Twitter and LinkedIn.

iCOL-BR-TRA-E-LT-001, July 2019

iconectiv®