Existing Robocalling and Spoofing Mitigation Techniques

ANONYMOUS CALL REJECTION

Benefit: Blocks any call not providing Caller ID information

Limitation: May block legitimate calls lacking Caller ID information

Dependent on: User initiated network service

Currently available: Yes

BLACK LISTING (Service Provider Specific)

Benefit: Blocks calls from unwanted numbers

Limitation: Spoofers can circumvent black listing by using alternate numbers

Dependent on: Network supported application

Currently available: Yes

DO NOT ORIGINATE

Benefit: Can make a significant initial impact when implemented in a limited number of large gateways

Limitation: Provides no protection against international VoIP originated calls

Dependent on: Network supported application

Currently available: No

FILING LEGAL COMPLAINTS

Benefit: Consumers are legally entitled to Federal Trade Commission (FTC) protection

Limitation: Filing an FTC complaint is only an option after robocalling/ spoofing has already negatively affected a consumer

Dependent on: User initiated non-network service

Currently available: Yes

HONEYPOTS

Benefit: A proactive approach for luring and identifying spoofers

Limitation: Requires substantial resources for development, maintenance and ongoing data monitoring

Dependent on: Network supported application

Currently available: Yes

MALICIOUS CALL TRACING

Benefit: Uses a star code (*) to record call details including source, date and time

Limitation: Collected data cannot be utilized until a later time

Dependent on: User initiated network service

Currently available: Yes

NATIONAL DO-NOT CALL REGISTRY

Benefit: Reduces the instances of unwanted telemarketing calls

Limitation: Provides no protection against international VoIP originated calls or deliberate fraudsters

Dependent on: User initiated network service

Currently available: Yes

SELECTIVE DISTINCTIVE RINGING

Benefit: Allows consumers to assign a specific ringtone to user selected numbers

Limitation: Numbers must be pre-selected from a contact list in order to provide notification of incoming calls

Dependent on: User initiated network service

Currently available: Yes

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 confidently access and exchange information simply, seamlessly and securely. iconectiv's extensive experience in information services, digital identity and numbering intelligence helps you do just that. In fact, more than 5K customers rely on our data exchange platforms each day to keep their networks, devices and applications connected and 2B consumers and businesses protected. Our cloud-based information as a service network and operations management and numbering solutions span trusted communications, digital identity management and fraud prevention. For more information, visit www.iconectiv.com. Follow us on X and LinkedIn.