calling number verification service for international calls

answering the call

The misuse of communication networks is a problem for communication service providers (CSPs) worldwide with bad actors exploiting networks to misrepresent their identity and place illegal robocalls to consumers. Case in point: In 2025, subscriber losses to fraudulent robocalling are anticipated to exceed $76 billion globally, rising from $64 billion in 2023.

To combat this type of fraud, in the United States, Canada, and France, the Secure Telephone Identity Revisited (STIR)/Signature-based Handling of Asserted information using toKENs (SHAKEN) framework helps mitigate illegal robocalls and helps consumers once again trust the number displayed on their caller ID. It does so via Know Your Customer (KYC) policies, as well as by enabling more reliable traceback of problematic callers. As a result, these authentication requirements and traceback efforts, help with enforcement actions.

The catch, however, is that legitimate calls from overseas to the US are at risk of a gateway "C" SHAKEN attestation, which is the lowest level of attestation, due to the lack of authentication at call origination. This is because oftentimes a provider uses a C-level attestation when it is the point of entry to the IP network for a call that originated elsewhere but has no relationship with the initiator of a call, such as when a provider is acting as an international gateway. Other countries are also imposing new regulations on international calls entering their countries.

This a big problem for those callers who rely on this channel for their business operations as well as individuals wanting to connect with others internationally. Specific to the U.S., the CSPs terminating calls in the U.S. need to contend with the nation's STIR/SHAKEN-based Calling Number Verification Service, which ultimately could result in legitimate international calls not getting answered and potentially labeled as spam, or even blocked.

Take the example of a multinational enterprise. When employees in its Germany or U.K. offices call their U.S. colleagues, customers or business partners, it's possible that the country's service will not accurately present some of those caller IDs as verified. The same is true of any overseas consumer calling the U.S. from their fixed or mobile line.

## Cross Border Call Authentication (CBCA) takes on the international challenge

Now, for some good news. iconectiv has developed a solution for international carriers to deliver traffic across international borders to the U.S. with the proper attestation of the originating carrier. As part of the iconectiv TruReach Certify trusted communications platform, Cross Border Call Authentication (CBCA) is a market-leading solution that facilitates CSPs' participation in the caller ID verification ecosystem by helping legitimate callers get their callerID shown as authentic to recipients in countries that have deployed the SHAKEN robocall mitigation framework. CBCA can also help participating CSPs to identify calls between themselves to make more informed call labeling and blocking decisions.

Cross Border Call Authentication

With CBCA, the SHAKEN framework could also be used for calls that originate in one country, such as the United States, and terminate in another country that also uses this type of framework. This is especially important for international businesses that need to connect with other companies and consumers across multiple countries. Every time a call gets blocked or mislabeled as spam when sending traffic to a partner or country within the SHAKEN ecosystem, such as Canada or France, it means a missed customer engagement or business opportunity or potential customer satisfaction issue. iconectiv's CBCA can increase the likelihood that global service provider customers' calls will be delivered, and that business customers can continue to rely on outbound calls to generate revenue and maintain business operations.

Cross Border Call Authentication (cont.)

Using the United States as an example, since many businesses employ offshore contact centers that make calls to their local markets, often these calls will use a local caller ID, which falls under the scope of the FCC's Robocall Mitigation Database and the current SHAKEN standard. When these calls are placed, they enter the local ecosystem with a "C" attestation since the call will be flagged as suspicious because it appears to be a spoofed number versus an authorized one. For global service providers that have these large contact centers as customers, CBCA allows the contact centers to have a greater likelihood that their call answer rates will increase, which drives productivity and improves customer experiences as their calls will be delivered with the proper attestation in countries within the SHAKEN ecosystem and, therefore, they will be known to the recipient.

Why CBCA Trust Model Works for Calls to the US
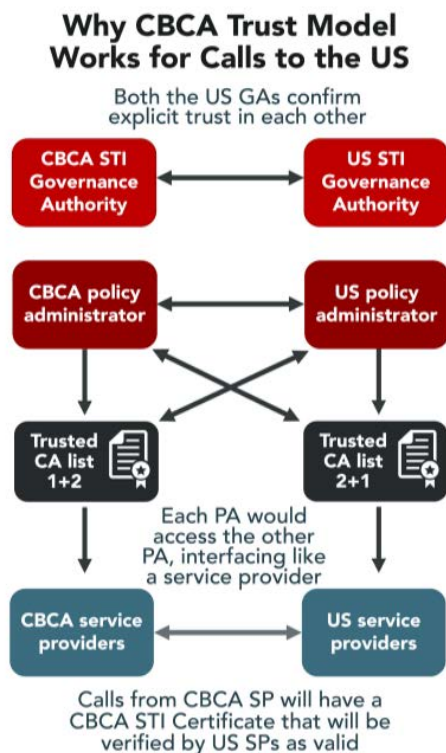
restoring trust – some more on SHAKEN

Using SHAKEN is the result of an industry-led initiative to mitigate illegal robocalls. Developed by the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum, SHAKEN uses Secure Telephone Identity Revisited (STIR) standards from the Internet Engineering Task Force (IETF). SHAKEN outlines the tools for signing and verifying calling party information, which can help trace these calls and stop them at their source.

For businesses, the service helps improve customer satisfaction and employee productivity. For example, by only assigning legitimate calls with an "A" attestation, businesses can verify the legitimacy of incoming calls, ensuring employees do not ignore important calls from clients or partners due to suspicion of fraud. At the same time, employees can spend less time answering fraudulent or spam calls, allowing them to focus on important tasks.

iconectiv's leading administrative role in SHAKEN

Within the U.S., iconectiv is the Secure Telephone Identity Policy Administrator (STI-PA) for the Calling Number Verification Service. As the STI-PA, iconectiv verifies, confirms, manages and supports the issuance of digital certificates for use in the SHAKEN framework and ensures that only authorized service providers and RespOrgs (which essentially act as intermediaries between toll-free number users and the national database) are able to obtain digital certificates from authorized Certification Authorities. These Certification Authorities are vetted, verified and approved by a Policy Management Authority (PMA) to perform the security functions necessary to maintain the integrity of the SHAKEN framework. iconectiv additionally serves as the director of the PMA, which is comprised of industry stakeholders, including members of the STI-GA technical committee.

iconectiv®