Trusted Calls in an Era of Robocalls and Scams

Protect Subscribers and Help Businesses Optimize Engagement
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal Robocalling and Caller ID Spoofing are Rampant, and the Impact</td>
<td>04</td>
</tr>
<tr>
<td>is Huge on Consumers and Businesses</td>
<td></td>
</tr>
<tr>
<td>People, Power and Professionals Demand Action</td>
<td>07</td>
</tr>
<tr>
<td>Regulators Ask Telecom Providers to Take the Lead</td>
<td>08</td>
</tr>
<tr>
<td>Businesses Speak Out</td>
<td>09</td>
</tr>
<tr>
<td>Effectively Mitigating Illegal Robocalling and Caller ID Spoofing</td>
<td>10</td>
</tr>
<tr>
<td>Restoring Trust to the Call Experience</td>
<td>12</td>
</tr>
<tr>
<td>Neustar Trusted Call Solutions</td>
<td>13</td>
</tr>
<tr>
<td>About Neustar</td>
<td>14</td>
</tr>
</tbody>
</table>
Illegal Robocalling and Caller ID Spoofing are Rampant, and the Impact is Huge on Consumers and Businesses

In today’s highly connected digital world, phone calls remain an important way to communicate. Consumers call to connect with family and friends, make appointments and get support for the products and services they use. Businesses rely on phone calls to relay important account information, confirm scheduled deliveries and share sensitive information with customers. But the explosion in illegal and unwanted robocalls, and the ever-evolving scams fraudsters use to target victims, mean that people no longer trust answering the phone.

Fraud by Phone on the Rise

One of the first phone scams, reported on by the Electric Review in 1888, was in Chicago where a smartly dressed man knocked on the front door of a home and asked the butler if he could use the house phone. Once inside, the man called the home owner at his business and told him “your cook, chambermaid and wife are lying here bound and gagged” and asked for $20,000 in ransom. The ransom was quickly paid, and the husband rushed home to find his wife, cook and chambermaid were fine and unaware of the ransom demand.

Seemingly, phone scams have been in existence since the birth of the telephone, but scammers are getting more sophisticated with their tactics. Estimates from a Harris Poll put 24.9M Americans losing $8.9B to phone scams from March 2017 to March 2018\(^1\) and consumer fraud reports to the FTC that indicated contact by phone totaled just over 770,000 with $290M lost in 2017.\(^2\)

---

\(^1\)Harris Poll survey sponsored by TrueCaller, March 2017
\(^2\)Consumer Sentinel Network Data Book 2017, FTC, March 2018
Phone Top Channel for Scammers

With VoIP, robocalls can be launched relatively cheaply or even for free. In the U.S. 3.4 Billion robocalls were sent in the month of April 2018\(^3\) alone — a 34% increase over April 2017. While some of these automated calls are legitimate – originating from schools, pharmacies, airlines and financial services organizations – at least one-quarter are reported as scams.\(^4\)

By spoofing the caller ID to look like it’s from another number, a known and trusted brand or even a government agency, fraudsters dupe people of all ages. Surprisingly, tech-savvy millennials have now become the most targeted group.\(^5\) And while the majority of scam calls were to mobile phones, one out of four reported scam calls were made to a landline.

To date, anti-robocall solutions have worked in a limited and siloed fashion addressing wireline, mobile and VoIP separately over different carriers and networks. The universal scourge of robocalls has led to the development of 500+ mobile apps designed to filter them out, but with less than ~3% adoption rate, it is not enough to solve this colossal problem. And landline phones have few options. Also adding to the problem, approximately 50% of households\(^6\) still own landline phones with few options available to stop robocalls.

By spoofing the caller ID to look like it’s from another number, a known and trusted brand or even a government agency, fraudsters dupe people of all ages.

---

\(^3\)April 2018 Nationwide Robocalling Data, Robocall Index
\(^4\)Senate Testimony, National Consumer Law Center, April 2018
\(^5\)Robocall scams are costing us billions – and millennials are a prime target, NBC News, April 21, 2017
\(^6\)Landline Phones Are a Dying Breed, Statista, January 2018
But All Business Communication is Digital, Right?

Outbound calls by businesses and contact centers continue to hold an important place in the customer experience lifecycle. It’s estimated that 65% of people prefer to contact a business by a phone call versus 24% who prefer to fill out an online form. This is why 93%⁷ of customer service teams still utilize the phone as a service channel, far exceeding digital platforms such as online chat (56%), social media (65%) and mobile apps (60%).

Even with so many digital support options, consumers still prefer phone calls for urgent notifications, or to discuss complex issues or sensitive information, reflecting nearly half the outbound activity by contact centers today. Research by ContactBabel⁸ found that 44% of outbound calls are related to proactive customer service (i.e. notification of delivery, delays, or problems) or call-backs and follow-ups. And those proactive notifications are often the ones consumers really don’t want to miss.

⁷State of Service, Salesforce Research, 2017
⁸US Contact Centers 2018-2020 – The State of the Industry and Technology Penetration, January 2018
People, Power and Professionals Demand Action

Regulators, consumers and businesses are looking to communications service providers (CSPs) to step up the fight against scammers. With advances in industry standards, analytics and advanced caller ID management systems, CSPs are in a prime position to mitigate the illegal robocall epidemic, safeguard consumers against phone scams and help get business calls answered.

**The People Have Spoken**

- **7.1 Million** complaints to the FTC\(^9\)
- **77%** of consumers “highly annoyed” by robocalls\(^10\)
- **75%** of consumers report missing important calls
- **88%** of consumers more likely to answer if the caller is identified

**Regulators Are Involved**

- **#1** complaint to FTC is robocalls
- **$51 Million** in civil penalties ordered by courts
- **$198 Million** in other recovery ordered by courts
- **FCC & CRTC** have mandated timelines to block robocalls and improve caller authentication

**Businesses Weigh In**

- **20% decrease** in outbound call center answer rates in 2017
- **88%** of business calls go unanswered
- **$1 Trillion** of consumer spend is influenced by phone calls

---

\(^9\)National Do Not Call Registry Data Book FY2017, Federal Trade Commission, December 2017

\(^10\)Advertising tactics that bug Americans the most, Consumer Reports, April 2014
Regulators Ask Telecom Providers to Take the Lead

North American regulators, the Federal Communications Commission (FCC) and the Canadian Radio-television and Telecommunications Commission (CRTC), have prioritized the eradication of unlawful robocalls and caller ID spoofing.

In addition to implementing a number of anti-robocalling regulations, the FCC established the Robocall Strike Force in 2016 to bring players from across the industry together to address the issue. In November 2017, the FCC announced new rules that allow voice service providers to proactively stop ‘likely fraudulent’ robocalls. The rules include blocking calls purporting to be from telephone numbers that are invalid, unallocated, unassigned and those designated by the subscriber as numbers that Do-Not Originate (DNO) calls (i.e. in-bound only numbers). The FCC announced a Further Notice of Proposed Rulemaking to address:

- Potential mechanisms to ensure erroneously blocked calls can be unblocked quickly
- Ways to measure effectiveness of robocalling efforts, as well as those of the industry

In May 2018, the FCC accepted the recommendations of the North American Numbering Council (NANC) to institute a governance authority to oversee implementation of caller authentication standards.

“The FCC has made consumers’ top priority with stopping unlawful robocalls one of the agency’s top priorities.”

— Ajit Pai, FCC Chairman

Meanwhile in Canada

The CRTC has stepped up its fight against fraudsters announcing new measures focused on reducing caller identification spoofing. In January 2018, they mandated that all Canadian telephone service providers:

- Implement authentication and verification of caller ID information for Voice over Internet Protocol (VoIP) calls no later than March 31, 2019
- Establish an industry administrator to issue the certificates required to authenticate and verify IP-based voice calls
- Develop a call traceback process for the CRTC to review and approve

The CRTC also asked for six-month progress reports, demonstrating the importance they are placing on these new measures.

The CRTC and the FCC are working collaboratively to combat illegitimate robocalls and caller ID spoofing by facilitating research and education. And both are mandating CSPs to taking a larger role in resolving these issues.

“Telecommunications service providers are in the best position to develop and implement call-management solutions for the millions of Canadians tired of receiving nuisance calls, just as they have done for email and text messaging.”

— Jean-Pierre Blais, CRTC Chairman
Businesses Speak Out

While "just block the robocallers" is a popular battle cry to rid the world of illegal robocalls, innocent and legitimate enterprises are being caught in the crosshairs. Industry groups have raised concerns about the impact that inadvertent call blocking and spam tagging is having on their business members’ ability to contact their customers. Their legitimate, and important, business calls are being blocked or their caller ID is being replaced and mislabeled as "Spam Likely" – often without them even knowing why no one is answering their call.

According to the Professional Association for Customer Engagement (PACE), a trade association representing companies that engage with customers via contact centers, the robocalling epidemic has led to a significant decrease in their contact center contact rates. Declining contact rates translates to increased costs from multiple call-backs but they also impact customer satisfaction.

To tackle these issues, PACE convened together carriers, analytics companies, app developers, trade associations and regulators to create the Communication Protection Coalition. While ensuring the intent of the robocalling mitigation initiatives are upheld, the key objective of the Coalition is to make sure that every legal call that a company places to customers gets through unencumbered, without incorrect labeling or being blocked. For example, the Coalition envisions a two-pronged approach for when a call is blocked, whereby:

- Both the caller and receiver receive a notification in real time. This could be in the form of a signaling cause code or an intercept pre-recorded message that is played when a number is disconnected.

- A standardized process is agreed and implemented by carriers and mobile application developers to quickly resolve blocking errors via a centralized contact point.
Effectively Mitigating Illegal Robocalling and Caller ID Spoofing

There is No Silver Bullet

Identifying the right robocalls to block and ensuring that the legal calls are not unintentionally blocked or mislabelled as SPAM is complex. Ridding the world of robocalls cannot be done with a broad stroke, so carriers need to assess multiple attributes when mitigating the risk of illegal robocalls. To accurately detect, block and reduce unlawful robocalls and prevent caller ID spoofing, communications service providers need:

- **Authoritative Data:** A variety of data sources are required to develop an appropriate risk profile of a call. Looking beyond single-sourced or crowd-sourced data helps to determine if a call is illegal versus reported as unwanted. Authoritative data from call lists, FCC complaints, Do-Not-Call Registries, external ‘bad lists’, line change detail, phone attributes, VoIP attributes and name and address demographic attributes should be used to gather insight, along with registered and verified outbound and inbound only Do-Not-Originate business numbers is a key consideration to prevent inadvertent blocking or spam-tagging of legitimate calls.

- **Advanced Analytics:** Behavior analysis and tracking of abnormal and unexpected calling patterns, along with insight into seasonal peaks and new or different types of campaigns for businesses, is necessary to accurately detect high volume robocalling, spoofing and suspicious call activity. By combining call analytics with authoritative data in near-real time, it can be effectively determined whether the call is potentially fraudulent or unlawful and should be blocked or tagged as spam.

- **Fraud Notification Tools:** Utilizing the caller ID display to warn about suspicious calls with a visual signal, or by prepending the 15-character display text with “SPAM”, helps to better inform the subscriber whether to answer the call or not. This universally adopted service provides access to a broad reach of subscribers without the need to rely on specific device features or enhancements.
- **Call Authentication**: The ability to authenticate the caller identity means being able to verify the caller certificates between the originating and terminating carrier in near real-time. As part of the risk assessment process, verifying caller identity requires the originating carrier to generate a private/public key pair for signing, request a STI certificate from the Certification Authority, receive the signed public key certificate and propagate the certificate as part of the signaling stream. The terminating carrier then verifies caller data by matching the public key certificate.

The STIR/SHAKEN standards have been identified by international regulatory bodies in the U.S., Canada, UK and Australia as a leading viable technology that can provide consumers with a measure of additional trust in call authentication. Solutions should be based on these standards to ensure they are future proofed. As adoption gains traction, testing planned implementations against implementations successfully aligned to standards frameworks ensures operability and increases success of system-wide rollouts.

- **All-inclusive Ecosystem**: Consumers and businesses expect the same level of protection against unlawful robocalls and inadvertent blocking of legal calls no matter if calls are to wireline, mobile or VoIP devices, regardless of the carrier of the caller or the person being called. It’s vital to ensure that solutions are in place to support all subscribers and business customers to deliver a truly trusted call environment.

### Caller Authentication Standards

**STIR**: Secure Telephone Identity Revisited (STIR), a technical standard developed by the Internet Engineering Task Force (IETF), provides a means to certify the identity of originating calls.

**SHAKEN**: Signature-based Handling of Asserted information using toKENS (SHAKEN), a framework developed by the Alliance of Telecommunications Industry Solutions (ATIS), provides a way to authenticate, verify and aid the identification of illegitimate uses of telephone numbers.
Restoring Trust to the Call Experience

For Subscribers

Consumers are becoming increasingly frustrated by the accelerating rate of robocalls hitting their phones. But the risks go much deeper when we see the billions of dollars that consumers are losing to phone scams each year. Regulatory authorities are flexing their muscle with heavier fines – but they are sorely outnumbered by the amount of illegal robocallers and are powerless when robocallers are based outside of their jurisdiction. Robocalls are the #1 complaint to the FTC each year, therefore customers will reward the CSPs that proactively invest in their robocall mitigation strategies.

For Enterprise, SMB and Public-Sector Business Customers

Enabling a more trusted call environment improves efficiency of business operations, outbound contact rates and ultimately customer engagement. Proactive calls during the various stages of the customer lifecycle, help to effectively deliver products, services and support, build relationships and provide greater satisfaction to improve Net Promoter Scores and customer loyalty.

Making Progress in the Fight on Robocalling

Advances in robocall detection, caller authentication and caller display technologies and standards now make it possible for CSPs to respond authoritatively to unlawful robocalls and scammers. In addition, CSPs can now provide customers greater confidence that the caller has been authenticated, and if not, empower them with visual warnings or notifications that the caller’s identity cannot be verified. And greater interoperability means that consumers will get the same experience across their wireline, mobile and VoIP communications. For brands, they benefit by being safeguarded from being inadvertently blocked or spam-tagged.

CSPs have responded with many solutions in place already, but with robocalls and scams still on the rise much more is needed to make a dent in this gigantic issue. CSPs are in a prime position to reduce the risks of unlawful robocalls and caller ID spoofing dramatically, for which your residential and business customers will thank you.
Neustar Trusted Call Solutions

**Neustar Robocall Mitigation** solution combines behavioral analytics, caller authentication and verification to help accurately identify robocalls, caller ID spoofers and call scammers.

Leveraging multiple data sources (e.g. call lists, FCC complaints, carrier feedback, and Neustar’s unrivaled proprietary data, which includes line change detail, phone attributes, VoIP attributes, name and address demographic attributes and our repository of verified numbers), Neustar helps CSPs determine in near real time the risk profile of each call placed and if potentially fraudulent to apply the corresponding policy to block the call or display a ‘BAD ROBOCALLER’ warning.

**Neustar Certified Caller** solution goes one step further to support and provide an extra layer of trust to consumers by authenticating and verifying caller identity. Incorporating the STIR/SHAKEN framework, Neustar automates the end-to-end process of generating, requesting and signing public key certificates and submitting them to the fraud score database. The terminating carrier is then able to verify its caller data by matching the public key certificate in the fraud score database and then apply the relevant digital signature to phone calls. Consumers can therefore trust a verified caller is authenticate and can make an informed decision whether or not to answer a call if the caller’s identity is unable to be verified or is identified as suspicious.

Neustar is the market leader in caller identity solutions. We provide 90% of Caller ID infrastructure in the U.S. and are a co-author of the STIR industry standard. In addition, the Neustar Trust Lab is the official host of the ATIS Robocalling Testbed, giving us unprecedented insight into the implementation of the STIR/SHAKEN standard and framework and the development of future-proof caller ID solutions.

For more information please visit [www.callerid.neustar](http://www.callerid.neustar)
Neustar, Inc. is a leading global information services provider driving the connected world forward with responsible identity resolution. As a company built on a foundation of Privacy by Design, Neustar is depended upon by the world’s largest corporations to help grow, guard and guide their businesses with the most complete understanding of how to connect people, places and things. Neustar’s unique, accurate and real-time identity system, continuously corroborated through billions of transactions, empowers critical decisions across our clients’ enterprise needs.

More information is available at www.home.neustar