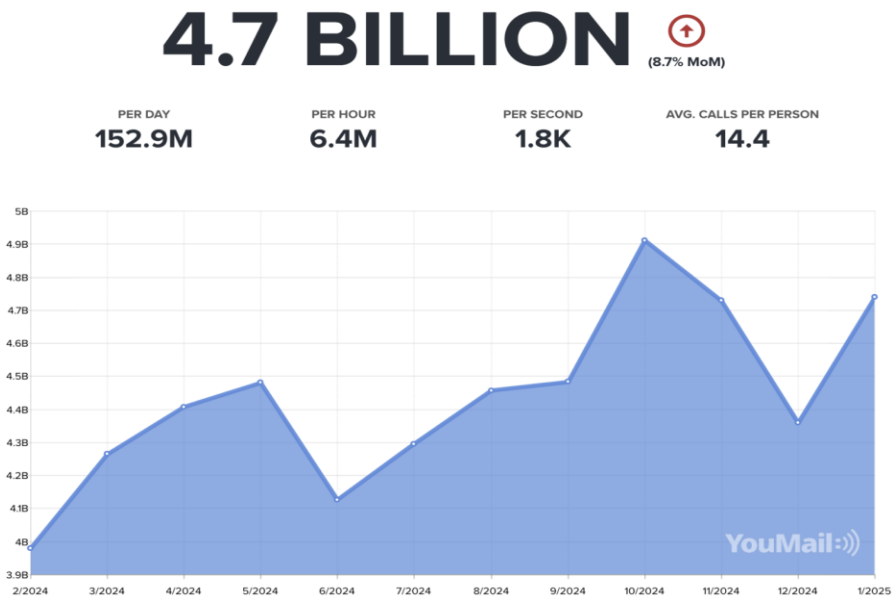
Eliminating Unwanted Sales and Spam Calls in the United States

By Charlie Malloy and Jackson Levine

Introduction:

If your phone rang 14 times today, how many calls would you trust enough to answer? For most Americans, the answer is: none. We have lost faith in the basic act of picking up the phone. In January of 2025 alone, Americans were bombarded with over 4.7 billion robocalls (YouMail, 2025). This translates to 152.9 million calls per day and 6.4 million calls per hour. These calls interrupt our work, invade our privacy, and exploit the elderly and vulnerable. Despite decades of "Do Not Call" lists and billions of dollars in fines, the problem is getting worse. This white paper explains why our current system fails, and how a realistic mix of stronger telecom accountability, smarter technology, and stricter enforcement can finally shut these scammers down.



Source: YouMail, 2025

Current landscape:

The U.S. government has attempted to mitigate the robocall problem for decades but has largely failed. The Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) regularly impose massive fines on violators. However, the vast majority of these penalties are never collected. Scam operations routinely hide behind offshore shell companies or dissolve and rebrand before regulators can enforce payment.

The National Do Not Call Registry was launched in 2003, following years of state-level experimentation and increasing consumer frustration with telemarketing. Before the national system, states like Florida, Indiana, and Missouri led the charge. Some early state laws even used primitive “black dot” symbols in phonebooks to signal that households did not want telemarketing calls. By 2002, 27 states operated separate “Do Not Call” lists. When the federal registry was finally created, it quickly became one of the most popular consumer protection measures ever implemented. By 2015, over 222 million phone numbers were registered, showing how Americans overwhelmingly hate spam calls.

Despite this massive enrollment, the system has struggled to keep pace with evolving scam tactics. Loopholes in the original Telephone Consumer Protection Act (TCPA) let bad actors mask their true identity through Voice over Internet Protocol (VoIP) technology, by spoofing fake caller IDs, or by routing calls through overseas call centers to stay beyond U.S. jurisdiction. The 2019 TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence) was designed to toughen penalties and force telecom providers to authenticate caller IDs using new technology. In practice, enforcement remains spotty and penalties are easily dodged. For example, in 2023 the FCC fined Rising Eagle Telecom $225 million for sending

hundreds of millions of spoofed robocalls, but the fine was never paid, illustrating how easily offshore or dissolving shell companies can evade punishment.

While legitimate businesses generally comply with Do Not Call rules, illegal operations adapt quickly. Many exploit new technologies to mass-dial thousands of targets for pennies, while fake caller IDs make it nearly impossible for consumers and law enforcement to trace the real source. Even when regulators tighten rules, telemarketers have repeatedly challenged Do Not Call restrictions in federal courts on First Amendment grounds. Courts have consistently upheld consumers' rights to block unwanted calls, but legal pushback and enforcement delays allow scams to persist.

The numbers show how big this failure has become. Today, about 2 billion unwanted calls and 19 billion spam texts flood U.S. phones every month. After a short-lived dip in 2022 and 2023, spam volumes rose again in 2024 as 92% of Americans reported receiving a spam call and 86% spam texts (Truecaller, 2024). The FCC's own data confirms robocalls remain the number one source of consumer complaints year after year.

This pattern of weak laws, jurisdictional loopholes, and fines that are impossible to collect makes one thing clear: protecting consumers now depends heavily on whether telecom providers, and the technology they control, can finally block scammers at the source.

Role of Telecom Providers:

Caller ID spoofing and mass robocalls are possible because outdated telephone networks still lack effective caller authentication. To fix this, regulators now require telecom providers to deploy the STIR/SHAKEN protocol (short for Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using tokeNs). STIR/SHAKEN verifies a caller's identity by attaching a digital certificate to each call, allowing phone carriers to confirm the number hasn't been spoofed. If there's a mismatch, the system can flag or block the call before it reaches the recipient.

In theory, universal implementation of STIR/SHAKEN would make it far harder for scammers to disguise their real phone numbers. In practice, progress has been challenging. Smaller carriers, VoIP providers, and overseas routes often bypass these safeguards entirely. This gap lets criminals continue to blast out millions of fake calls for pennies, while legitimate telecom companies face little accountability if they fail to enforce caller ID rules aggressively.

Telecom providers (companies like Verizon, AT&T, T-Mobile, and the dozens of smaller regional and VoIP carriers) control the infrastructure that routes calls and verifies caller information. They are the gatekeepers. Without their active participation, any technical solution to robocalls becomes meaningless. Right now, many of these providers are not fully complying with STIR/SHAKEN or actively screening for abuse, and they face almost no consequences for it. If regulators held telecoms accountable for the traffic that moves through their networks, these companies would have a strong incentive to block suspicious calls before they ever reach the consumer. Active enforcement on the carrier side would immediately reduce the volume of robocalls and restore trust in phone communication because ultimately, it is these providers who allow scam calls to go through in the first place.

Advances in AI offer an additional layer of protection on top of basic caller authentication. While STIR/SHAKEN can verify whether a number is real, it does not detect whether the caller's content is a scam. Modern AI tools can screen incoming calls in real time by analyzing voice patterns, repeated scam scripts, or robotic tones, and block suspicious calls before they reach the user. For example, Google's AI-powered call screener can filter spam, transcribe conversations, and even reject calls automatically based on risk signals. Other third-party apps use AI to learn from user feedback, flagging new scam tactics as they emerge.

Combined, strict caller authentication and AI-driven screening could finally close the loopholes that make mass robocalling profitable. But without holding telecom providers accountable, these tools alone will not solve the problem.

Consumer Protections:

As telecom providers continue to find ways to combat unwanted spam and sales calls, it is important that consumer privacy is not sacrificed in the process. AI driven tools can be effective but also introduce new risks, especially when they are deployed without transparency or user control.

One major concern is false positives: AI could block legitimate calls from medical offices, job recruiters, and schools. According to the Electronic Privacy Information Center (EPIC), AI filters often mistakenly flag legitimate numbers due to overreaching algorithms or insufficient context, leading to missed opportunities or critical communication failures. This diminishes public trust in the very tools meant to protect them.

Additionally, many AI screening systems log user interactions and caller data, which raises serious privacy concerns. Information like voice patterns, call behavior, and user responses may be collected and analyzed without user consent. When these systems are operated by third-party tech firms, users are left with little control over where their data goes or how it is used.

To mitigate these risks, it is super important to build consumer control and transparency into the system. Opt-in frameworks should be the default: users should actively choose whether to enable AI-based filtering and be given options to adjust sensitivity based on their risk tolerance. This model should mirror existing digital privacy protections used in web browsers and ad targeting platforms, giving users autonomy over their communications.

Beyond opt-in controls, the FCC and telecom providers should develop a standard set of transparency tools including clear explanations for why a call was blocked or flagged, simple ways to report false positives or whitelist trusted numbers, and provide feedback loops that allow AI systems to learn from user corrections. These tools should be part of telecom carriers' apps and websites and presented in a simple manner to support older and less tech-savvy users. Making these options easy to access and see increases trust in the system and reduces the chance of disengagement.

Lastly, public awareness is crucial. The FCC should partner with carriers to launch nationwide education campaigns that explain how call-blocking tools work, what data is (and is not) collected, and how to use available privacy settings. Without this layer of communication, even an extremely well-designed protections risk being unused or misunderstood.

Overall, AI and advanced caller ID tools can help solve the robocall crisis if deployed responsibly. Giving users control over filtering, ensuring transparent, and protecting their data are critical when it comes to building a system that is both effective and ethical.

Enforcement and Penalties

Despite years of federal attention, current enforcement against robocalls remain largely ineffective. The Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) regularly issue fines to robocall operators; however, most of these fines go uncollected due to the use of offshore entities, shell corporations, and complex legal loopholes that allow scammers to escape punishment. Many of these operations reappear under new names, making enforcement challenging. Repeat offenders continue to exploit the system, taking advantage of limited oversight and jurisdictional gaps.

Another major failure in the current approach is the absence of a centralized, publicly accessible database of persistent violators. Without it, there is little transparency for consumers, and no consistent guidance for telecom providers to block high-risk numbers. There is also a significant lack of coordination between federal regulators, telecom carriers, and law enforcement agencies, resulting in slow and weak responses to an issue that requires aggressive action.

To fix this, the federal government should implement a robocall offender database. This would be a public, frequently updated list of individuals and entities who violate telemarketing laws. Telecom providers would be legally required to block numbers linked to repeat offenders, helping to prevent repeat abuse. Additionally, the FTC and FCC should be granted expanded authority to crack down on these operations through criminal referrals and fast-tracked investigations. Penalties must also be modernized. Fines should be scaled based on both the

volume of calls made and the level of deception involved (e.g., impersonating government agencies or financial institutions).

Further, telecom carriers themselves should face penalties for failing to implement baseline protections like STIR/SHAKEN or for allowing repeat offenders to operate on their networks. To support these efforts, a federally funded robocall task force should be established to lead joint investigations across the FCC, FTC, and Department of Justice. These investigations must be proactive, not just reactive, targeting the origin of spam traffic, especially those that operate internationally.

Finally, telecom carriers should be mandated to report key enforcement metrics monthly, including: total robocalls detected, percentage of false positives, and percentage of calls from known violator numbers successfully blocked. This level of transparency will increase accountability across the industry and provide regulators with the real-time data needed to act decisively. Without stronger enforcement backed by real consequences, bad actors will continue to exploit regulatory weaknesses which undermine public trust and clog our communication systems with fraud.

Implementing these solutions will help build trust in phone communication by making it much harder for scammers to disguise themselves. With STIR/SHAKEN technology, callers must verify their identity through their carrier network, significantly reducing the number of spoofed calls used to trick people into answering fraudulent calls. Over time, as these systems are adopted more widely, both the volume and effectiveness of spam calls will decrease, leading consumers to feel safer and more confident when answering their phones.

Projected Outcomes and Impacts:

If these recommendations are implemented, the expected impacts will be substantial for both consumers and legitimate businesses. Widespread deployment of STIR/SHAKEN caller ID authentication, stronger telecom accountability, and modern AI screening tools would collectively reduce the total volume of illegal robocalls. According to recent FCC estimates, full rollout of STIR/SHAKEN alone could prevent millions of spoofed calls each day by verifying caller identity across networks (Federal Communications Commission, 2024). When paired with stricter enforcement, updated penalties, and a centralized database of repeat violators, the total number of unwanted calls and spam texts is likely to decline measurably within the first year.

For consumers, this reduction means greater trust in answering the phone without the constant risk of fraud or harassment. Fewer scam calls would directly lower financial losses, which currently run into billions of dollars each year. In 2024 alone, the Federal Trade Commission received 2.6 million fraud reports, with total losses reaching $12.5 billion. Phone calls were the second most common method scammers used to reach victims (Federal Trade Commission, 2025).

Improved call reliability would especially benefit older adults and vulnerable populations who are often targeted by phone scams. Many of these individuals are contacted by scammers posing as government agencies, financial institutions, or family members in distress, making them more at risk of deception and financial exploitation. Through cutting off these avenues of contact, STIR/SHAKEN and AI-based call screening can directly reduce harm to these vulnerable people.

Expanded use of AI call screening, when combined with clear opt-in controls and user transparency, would give individuals more confidence that important calls, from medical offices, schools, or employers, will not be mistakenly blocked. These systems also offer an opportunity to make spam protection more responsive, as users can correct false positives to help the AI adapt to new and evolving scam tactics in real time.

Beyond fraud prevention, reducing robocalls also has proven to improve the quality of life of individuals. Research has shown that persistent, unwanted phone interruptions increase stress, anxiety, and reduce productivity, especially among older adults or those living alone. These effects can be felt on a daily basis and compound over time, worsening frustration and mental fatigue (CallBlockerUSA, 2024).

Over the long term, stronger robocall protections would restore trust in phone communication itself. Many Americans now instinctively ignore unknown numbers, even when the call could be important. This is due to the sheer volume of spam calls people receive. A phone system that people can trust again would reduce the instinct to ignore unknown numbers, encourage timely response to important calls, and restore phone calls as a reliable means for day-to-day communication.

Conclusion

Unwanted robocalls remain one of the most persistent consumer protection challenges in the United States. Despite decades of regulation and billions of dollars in fines, scammers

continue to exploit technological loopholes and weak enforcement to target millions of people every day. With billions of robocalls placed every month, the public has lost trust in the most basic form of communication: answering a phone call. This paper has shown that the core of the problem lies in weak accountability from telecom providers, outdated technical infrastructure, and a lack of cohesive enforcement. While tools like STIR/SHAKEN and AI call screening exist, they are only as effective as the systems and companies implementing them. Establishing clear consequences for non-compliance by telecom providers is essential to ending spam calling at the source.

The path forward requires more than scattered fixes. It demands full-scale efforts to close legal loopholes, hold telecom providers responsible for the traffic they allow, and give consumers control over how their calls are filtered. Increased enforcement mechanisms, opt-in privacy protections, transparent AI tools, and a centralized robocall offender database are all necessary to regain control of our phone networks.

Ultimately, these reforms are not just about blocking calls. They are about restoring confidence in everyday communication. By rebuilding a phone system that people can trust, we can protect vulnerable populations, reduce fraud, and bring integrity back to the way Americans connect.

Sources Cited:

CallBlockerUSA. The Impact of Spoof or Spam Calls on Mental Health and Productivity. 2024, www.callblockerusa.com/blogs/nuisance-and-scam-news/the-impact-of-spoof-or-spam-calls-on-mental-health-and-productivity.

Federal Communications Commission. “FCC Issues Annual Robocalls Report.” In Compliance Magazine, 2024, incompliancemag.com/article/fcc-issues-annual-robocalls-report/. Federal Trade Commission. National Do Not Call Registry Data Book for Fiscal Year 2024. FTC, 2024, www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2024/.

Federal Trade Commission. New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. 2025, www.ftc.gov/news-events/news/press-releases/2025/01/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

Electronic Privacy Information Center (EPIC). AI and the Risks of Call Screening. 2024, www.epic.org/issues/ai/ai-call-screening-privacy-risks/

Smith, Jane. “Google’s AI Call Screener: A Glimpse Into the Future of Automated Call Management?” The Verge, 17 Nov. 2024, www.theverge.com/google-ai-call-screener-future.

Truecaller. U.S. Spam and Scam Report 2024. 2024, www.truecaller.com/blog/insights/us-spam-scam-report-2024. YouMail. January 2025 Robocall Report: A Look Into the 9% Nationwide Surge in Spam Calls. YouMail Blog, Jan. 2025 www.youmail.com/blog/january-2025-robocall-report