MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☑ IN SUPPORT OF ☐ IN OPPOSITION TO ☐ FOR INFORMATIONAL PURPOSES

WITNESS NAME

INDIVIDUAL:

WITNESS NAME: **ARNIE C. AC "HONEST-ABE" DIENOFF-STATE PUBLIC ADVO**	PHONE NUMBER:	
BUSINESS/ORGANIZATION NAME:	TITLE:	
ADDRESS:		
CITY:	STATE:	ZIP:

EMAIL:	ATTENDANCE: **In-Person**	SUBMIT DATE: **1/28/2026 11:20 PM**

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

Let's get ride of Spoofing, Bad-Actors and terrible Characters with added No Caller Lists and Huge Fines.

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☑ IN SUPPORT OF ☐ IN OPPOSITION TO ☐ FOR INFORMATIONAL PURPOSES

WITNESS NAME

REGISTERED LOBBYIST:

WITNESS NAME: **HEIDI SUTHERLAND**		PHONE NUMBER:	
REPRESENTING: **MO CHAMBER OF COMMERCE**		TITLE:	
ADDRESS:			
CITY: **JEFFERSON CITY**		STATE: **MO**	ZIP: **65101**
EMAIL:	ATTENDANCE:	SUBMIT DATE: **1/28/2026 12:00 AM**	

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☐ IN SUPPORT OF ☑ IN OPPOSITION TO ☐ FOR INFORMATIONAL PURPOSES

WITNESS NAME

INDIVIDUAL:

WITNESS NAME: **SARAH BERRY**	PHONE NUMBER:	
BUSINESS/ORGANIZATION NAME:	TITLE:	
ADDRESS:		
CITY:	STATE:	ZIP:
EMAIL:	ATTENDANCE: **Written**	SUBMIT DATE: **1/26/2026 12:12 PM**

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

HB 2472 is marketed as consumer protection, but it's mostly duplication and optics.

Missouri residents already live under a comprehensive federal regime governing robocalls and spoofing (TCPA + FCC rules, including the STIR/SHAKEN authentication framework).

This bill largely re-states what's already required, then adds another layer of penalties and procedures without solving the one thing that actually matters: attribution—who actually originated the call across modern VoIP routing and intermediary networks.

Instead of targeting the source of harm, HB 2472 expands enforcement tools that will predictably be used against the easiest in-state targets, not the actual fraud operations that churn numbers, mask identity, and operate across jurisdictions.

And then it does the part that should embarrass anyone calling this "anti-spoofing":
It bans spoofing—except when the government does it.

HB 2472 explicitly exempts law enforcement and intelligence/security agencies. That means the bill's moral premise is: spoofing is dangerous deception… unless you have a badge or a federal seal.

That exemption destroys credibility. If caller ID manipulation is inherently harmful, it should be restrained and audited—not immunized.

It creates punishment without precision.

The bill authorizes fines and encourages private lawsuits/class actions, but the enforcement mechanism still leans on the same systems already mandated federally. In practice, this becomes punitive volume over targeted enforcement, and it hands regulators a bigger stick without requiring better proof.

It also risks collateral damage.

Provider blocking mandates and compliance frameworks can misfire. When you incentivize blocking to avoid penalties, you increase the risk of legitimate calls getting blocked—medical systems, schools, pharmacies, small businesses—especially when caller ID data is messy and frequently misclassified.

Missouri should not pass laws that feel satisfying while failing the basic test: will this measurably reduce fraud calls, or just create more paperwork, more lawsuits, and more discretion?

HB 2472 is what happens when lawmakers confuse "we wrote a law" with "we solved a problem": it largely mirrors federal requirements, adds state penalties without improving attribution, and then exempts government and intelligence agencies from the conduct it claims is dangerous—turning a public-trust issue into a two-tier permission structure.

If it's illegal because it's deceptive, it shouldn't be legal for the people in charge of deception. Vote NO on HB 2472.
-Rev. Sarah M. Berry

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☐ IN SUPPORT OF ☐ IN OPPOSITION TO ☑ FOR INFORMATIONAL PURPOSES

WITNESS NAME

BUSINESS/ORGANIZATION:

WITNESS NAME: **JAKE LESTOCK**	PHONE NUMBER: **202-412-3556**	
BUSINESS/ORGANIZATION NAME: **CTIA**	TITLE: **DIRECTOR, STATE LEGISLATIVE AFFAIRS**	
ADDRESS: **1400 16TH ST. NW, SUITE 600**		
CITY: **WASHINGTON**	STATE: **DC**	ZIP: **20036**
EMAIL: **jlestock@ctia.org**	ATTENDANCE: **Written**	SUBMIT DATE: **1/28/2026 8:05 AM**

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

Chair Bromley, Vice-Chair Simmons, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this informational testimony for the record regarding House Bill 2147, House Bill 2472, and House Bill 2658. These bills look to expand existing telemarketing rules that try to stifle illegal and unwanted robocalls and texts and codify federal rules and requirements into state law.

CTIA members are committed to protecting consumers from illegal and unwanted robocalls and texts. The wireless industry works tirelessly to block illegal robocalls and texts messages and label them to be a spam risk to minimize the negative impact of robocalls and texts. While we wholeheartedly agree with the state's interest in protecting consumers from unwanted calls and texts, we have general concerns about the creation of conflicting state telemarketing/automated call laws that do not conform to federal regulations could create compliance challenges for carriers that operate interstate networks. For this reason, CTIA supports uniform federal regulations on these issues rather than a patchwork of varying state requirements.

For years, CTIA and our member companies throughout the wireless industry have been working hard to protect consumers and foster trust in both text messaging and voice calling platforms. As text messages and voice calls continue to be vital communication tools, the wireless industry has taken proactive measures to address the growing threat of robocalls and robotexts. Through a multi-layered approach, including industry best practices, up-front registration and vetting, cutting-edge call- and text-blocking technologies, and robust consumer reporting, we've made significant strides in combating unwanted non-consumer communications. For example, in 2024 alone, wireless providers blocked nearly 55 billion robotexts.

Combatting Illegal Robocalls with Tools and Technology
On the voice side, wireless providers and their ecosystem partners have developed and deployed a wide range of powerful tools to protect consumers. While some robocalls are useful – like the ones you receive from pharmacies, airlines, and schools – many are illegal, intrusive, and annoying. Stakeholders across the wireless ecosystem are working to help consumers combat these problematic instances. Indeed, a multi-pronged effort is already underway to combat illegal robocalls. Wireless providers have developed and deployed a wide range of powerful tools to protect consumers, including – but not limited to – developing robust know-your-customer practices, deploying innovative call-blocking technologies, tracing back illegal robocalls to identify bad actors at the source, and

establishing and implementing robust robocall mitigation programs. Last year, Americans spent more than 2.4 trillion minutes on voice calls. Unfortunately, bad actors also know how much consumers value and rely on wireless voice services. As they have increased their efforts to target consumers through robocalls, the wireless industry has also enhanced its efforts to protect consumers through new initiatives, technologies, and partnerships, which are detailed below.

In addition to the numerous sophisticated analyses wireless providers use daily to block unwanted calls and investigate bad actors, the industry has developed new initiatives and technologies to address the issue further. Wireless providers, including AT&T, Verizon, and T-Mobile, have helped develop and deploy caller ID authentication technology that works to combat illegal telephone number spoofing. STIR/SHAKEN, or Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using toKENs, is a framework of interconnected technical standards developed by industry where wireless providers digitally validate a variety of calls, allowing a provider to verify the caller and the caller's right to use the phone number. The idea behind STIR/SHAKEN is to enable consumers to trust their Caller ID again by enabling voice service providers sign their subscribers' telephone numbers with a digitally encrypted signature to ensure the calling number of a telephone call has not been tampered with. In other words, the STIR/SHAKEN framework helps confirm the call is from the person the caller ID says it is from. The Federal Communications Commission (FCC) adopted rules requiring voice service providers to implement STIR/SHAKEN in the IP portions of their voice networks since 2021 and has since expanded the implementation obligation to additional providers with the goal of achieving ubiquitous STIR/SHAKEN adoption.

While masking one's identity or spoofing caller ID information is often associated with malicious intent, there are important exceptions that serve a critical public interest objective. For instance, domestic violence shelters may intentionally shield their identity to protect victims when conducting outreach via telephone to those victims. Public health agencies, legal service organizations, or law enforcement might use similar measures to protect sensitive information or ensure the communication recipient's safety.

To complement these solutions, innovative branded calling solutions are being developed and deployed in the marketplace. CTIA developed a branded calling solution that leverages the STIR/SHAKEN framework to deliver trusted visual information from enterprises to consumers using standards-based Rich Call Data or "RCD", so consumers can be confident that a call is coming from a verified source. We refer to this solution as Branded Calling ID™ or BCID™. BCID delivers more robust—and secure—information to consumers' smartphones, including a calling enterprise's verified: (1) caller display name (e.g., "Home Depot"); (2) caller logo; and (3) call reason (e.g., "Order Ready for Pickup"). By receiving additional, trusted, branded caller information, consumers can make more informed choices about whether to pick up the phone, reducing the risk of being bothered by spam or harmed by scam calls.

To help enhance enforcement against bad actors behind illegal and unwanted robocalls, wireless providers coordinate with each other to help identify illegal callers for referral to the appropriate federal and state enforcement authorities at the FCC, the Federal Trade Commission (FTC), the Department of Justice (DOJ), and at the state level to stop illegal robocalls. To aid enforcement efforts, wireless companies participate in the Industry Traceback Group, that works to identify the source of illegal calls. Additionally, nationwide wireless providers, along with other voice service providers, have partnered with 51 state attorneys general to adopt eight principles to fight illegal robocalls. This partnership is a reaffirmation of the commitment made by wireless providers, such as AT&T, T-Mobile, and Verizon, to protect consumers. Specifically, those providers agreed years ago to incorporate, or continue to incorporate, the following anti-robocall principles into their business practices:

- **Offer Free Call Blocking and Labeling;**
- **Implement STIR/SHAKEN;**
- **Analyze and Monitor Network Traffic;**
- **Investigate Suspicious Calls and Calling Patterns;**
- **Confirm the Identity of Commercial Customers;**
- **Require Traceback Cooperation in Contracts;**
- **Cooperate in Traceback Investigations;**
- **Communicate and cooperate with state attorneys general about recognized scams and trends in illegal robocalling**

Stopping Illegal and Unwanted Text Messages
In the text messaging space, wireless providers and their partners throughout the wireless text

messaging ecosystem are on the frontlines of defending consumers from illegal and unwanted text messages. These protections are multi-layered, including (i) up-front vetting and verification of business message senders nationwide, (ii) filtering and blocking billions of harmful text messages to prevent them from reaching wireless consumers each year, and (iii) partnering with law enforcement agencies to target bad actors. First, the ecosystem's up-front vetting and verification systems help stop bad actors before they can send scam or spam text messages. As a threshold protection, wireless messaging technologies require valid originating information, such as a legitimate telephone number. As a result, number spoofing has not plagued text messaging as it has with robocalling. Instead, impersonation scams – where bad actors try to trick consumers into thinking that a trusted entity like their bank is contacting them – have been more prevalent. We have devised a specific action plan to address brand impersonation issues.

Wireless providers and their messaging partners also deploy vast security and fraud prevention teams using the latest innovative technologies, machine learning and AI, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions. With these tools, wireless providers successfully block billions of spam text messages from ever reaching consumers each year. In 2024 alone, wireless providers blocked more than 55 billion scam and spam robotexts. And blocking is only one part of the broader effort to make sure the wireless industry's playbook evolves to keep up with bad actors' changing tactics.

To enhance these protections, wireless providers have established a common means for consumers to report unwanted text messages – forwarding the message to 7726 (SPAM) – and have partnered with Apple and Google to make it easier for consumers to "Report Junk" directly through the wireless messaging applications that are built into most wireless phones. Wireless providers use this reported data to evolve spam mitigation tools in real-time and keep pace with the constantly changing tactics of bad actors. And when wireless providers receive complaints about texts with suspicious links, their teams investigate the website to determine if the link is intended to support fraudulent efforts. If so, wireless providers can share that link with ecosystem partners so it can be blocked by most internet browsers.

As a complement to wireless industry tools and best practices, CTIA formed the Secure Messaging Initiative (SMI) to bring stakeholders together to share information so they can quickly stop spam and target bad actors. The SMI helps messaging industry stakeholders identify bad actors, share information with each other and with law enforcement agencies, and develop best practices to address emerging threats on the messaging platform. To trace the origins of spam and scam text messages and report on those to law enforcement for investigation, CTIA's SMI convenes the messaging ecosystem and partners with YouMail Protective Services (YPS). To date, CTIA's SMI has delivered more than 20 referrals to law enforcement partners at the FCC, the FTC, DOJ, and the state anti-robocall task force, which they can use to take action against these spammers and shut them down.
CTIA and its member companies understand the importance of investing in proactive, multi-layered measures that include sophisticated tools, industry best practices, and public-private partnerships to protect consumers from fraudulent text messages. At the heart of these protections are CTIA's Messaging Principles & Best Practices, which set clear guidelines for non-consumer message senders on issues like consent, privacy, and security, and preventing unwanted messages. Our guiding principle is consent: Consumers should have control over the texts and calls they receive, with the ability to opt out at any time. Through this and other principles, we help prevent consumers from getting messages they do not want, while helping ensure consumers get the messages they do want.

In closing, the wireless industry recognizes the need to fight unwanted and illegal robocalls and text messages. We are working collaboratively with federal and state stakeholders to protect consumers from being harassed and scammed. A multi-pronged, multi-faceted approach is essential as illegal actors are working around the clock to deceive consumers and carriers. We look forward to continuing our work with states to combat unwanted and illegal robocalls and text messages and avoid any unintended consequences that a patchwork of varying state requirements could result in unintended consequences on good actors.

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☐ IN SUPPORT OF ☐ IN OPPOSITION TO ☑ FOR INFORMATIONAL PURPOSES

WITNESS NAME

BUSINESS/ORGANIZATION:

WITNESS NAME: **JEREMY KETTERER**		PHONE NUMBER: **573-301-5550**	
BUSINESS/ORGANIZATION NAME: **AT&T MISSOURI**		TITLE: **EXTERNAL AND LEGISLATIVE AFFAIRS**	
ADDRESS: **1010 PINE STREET- ROOM 19W-E-01**			
CITY: **ST. LOUIS**		STATE: **MO**	ZIP: **63101**
EMAIL:	ATTENDANCE:	SUBMIT DATE: **1/28/2026 12:00 AM**	

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☐ IN SUPPORT OF ☐ IN OPPOSITION TO ☑ FOR INFORMATIONAL PURPOSES

WITNESS NAME

REGISTERED LOBBYIST:

WITNESS NAME: **PATRICK FUCIK**		PHONE NUMBER: **913-687-5548**	
REPRESENTING: **T-MOBILE**		TITLE:	
ADDRESS: **6204 BRIDLE BEND DRIVE**			
CITY: **COLUMBIA**		STATE: **MO**	ZIP: **65201**
EMAIL:	ATTENDANCE:	SUBMIT DATE: **1/28/2026 12:00 AM**	

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.

MISSOURI HOUSE OF REPRESENTATIVES

WITNESS APPEARANCE FORM

BILL NUMBER: **HB 2472**	DATE: **1/28/2026**
COMMITTEE: **Utilities**	

TESTIFYING: ☐ IN SUPPORT OF ☐ IN OPPOSITION TO ☑ FOR INFORMATIONAL PURPOSES

WITNESS NAME

REGISTERED LOBBYIST:

WITNESS NAME: **SCOTT SWAIN**		PHONE NUMBER: **573-230-8138**	
REPRESENTING: **VERIZON**		TITLE:	
ADDRESS: **104 CLAY STREET**			
CITY: **JEFFERSON CITY**		STATE: **MO**	ZIP: **65101**
EMAIL:	ATTENDANCE:	SUBMIT DATE: **1/28/2026 12:00 AM**	

THE INFORMATION ON THIS FORM IS PUBLIC RECORD UNDER CHAPTER 610, RSMo.