ibtta
INDUSTRY ADVISORY
www.ibtta.org/ibtta-insights

NEW SMS TEXTING SCAMS EMERGE IN 19 U.S. STATES

February 4, 2026

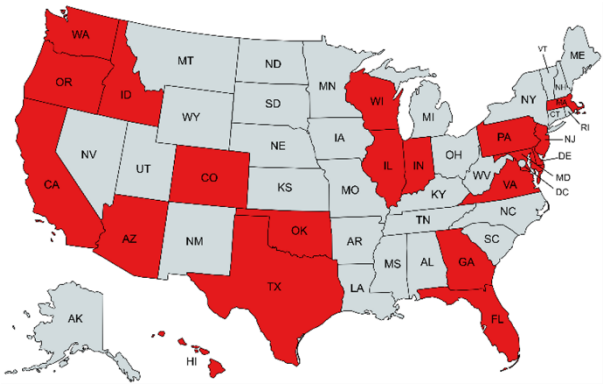
Overview

Over the past week, we have been made aware of 437 new toll scam sites that are actively targeting 19 states.

Affected states & organizations

Arizona	Massachusetts
California	New Jersey
Colorado	Oklahoma
Delaware	Oregon
Florida	Pennsylvania
Georgia	Texas
Hawaii	Virginia
Illinois	Washington (Seatle)
Indiana	Wisconsin
Maryland	E-ZPass

States with New SMS Toll Scam Sites



How the scam works

The nature of the attacks involves the creation of domains that are primarily posing as state government sites, state motor vehicle administrations, and E-ZPass. The actions taken to shut these scams down at their source should limit the impacts to the public. But toll operators, back-office operators, motor vehicle departments, and state governments should be aware of the matter in case questions arise from residents and customers and to refresh communications on how to manage suspicious text messages.

What the Public Should Know

Agencies and service providers can warn the public to be attentive to unsolicited messages, particularly those addressing unpair toll transactions.

Important reminders include:

Toll agencies never seek immediate payment or urgent actions via text message.
Drivers should always contact toll agency customer services independently and directly and not rely on third-party text messages.

Never click on a link in text message and never offer personal or financial information through unsolicited messages.
Individuals who receive unsolicited text messages should delete them without clicking on any links.
Secure personal information and financial accounts if any links were clicked and dispute any unfamiliar charges.

Tolling Industry Response

Since 2024, toll agencies have seen a rise in SMS-based scams in various forms and have moved quickly to strengthen coordination across the industry. IBTTA supports peer-to-peer collaboration through its Cyber Security Working Group, helping agencies coordinate with their internal technology and cybersecurity teams, law enforcement partners, and national research organizations to identify emerging threats, disrupt fraudulent activity, and limit impacts to customers.

These coordinated efforts include shutting down fraudulent sites, addressing software vulnerabilities, tracking evolving scam tactics, and proactively communicating with customers through account portals, websites, social media, and direct outreach. Together, these actions help protect a system that processes approximately ten billion transactions annually and generates roughly $25 billion in revenue across U.S. toll facilities.

Special thanks to the leadership of the Illinois Tollway in responding with the IBTTA Cyber Security Working Group. **Learn more at IBTTA.org.**