Highlights

- Detect robocalls originated by owned TNs and upstream provider
- Mitigate robocalls before authorities take punitive action
- AI powered audio analytics accurately detect robocall activity
- Audio files provide irrefutable evidence of illegal bad actor behavior
- Strengthen “know your customer” programs

Overview

Service providers face a significant challenge: Stop robocalls originating or transiting their networks or face stiff government penalties and business risks, including lawsuits by affected users.

The YouMail Robocall Threat Sentry is a highly effective call analytics solution that enables service providers to mitigate and eliminate robocalls. It provides zero-hour detection of suspicious robocall behavior originating or transiting their network. Based on the same threat database used by the USTelecom Industry Traceback Group for robocall investigations, Robocall Threat Sentry immediately notifies service providers when illegal robocalls are detected, enabling quick action that minimizes risks and protects revenues.

Stop Originating Robocalls

By itself, STIR/SHAKEN caller authentication is insufficient to prevent robocalls. Bad actors can originate authenticated calls by evading customer vetting processes or hacking into poorly secured business networks. Authentication should be paired with call analytics that can detect abusive, fraudulent, or unlawful calls originating on service provider networks.

The YouMail Robocall Threat Sentry enables service providers to meet robocall do-not-originate requirements with a robocall detection solution that is easy to use. It provides reliable zero-hour detection of robocalls originated by a service provider’s owned numbers, enabling them to mitigate the illegal activity. It can be configured with a TN watchlist in minutes and managers can view threat activity on a convenient dashboard, or receive automatic notifications when issues arise.

Competing analytics based on honeypots, call metadata, and crowd sourced data aren’t completely effective. They generate false positives that consume resources on needless customer investigations, or false negatives that can leave the organization exposed to undetected bad actors.

In contrast, the Robocall Threat Sentry detects robocalls by analyzing the audio content in real consumer voicemail messages captured by the YouMail sensor network, the industry’s largest independent sensor network. The YouMail sensor network samples calls received by consumer devices across all major U.S. service providers, including Verizon, AT&T, and T-Mobile. AI-driven algorithms accurately detect bad actor behavior based on voicemail audio content.

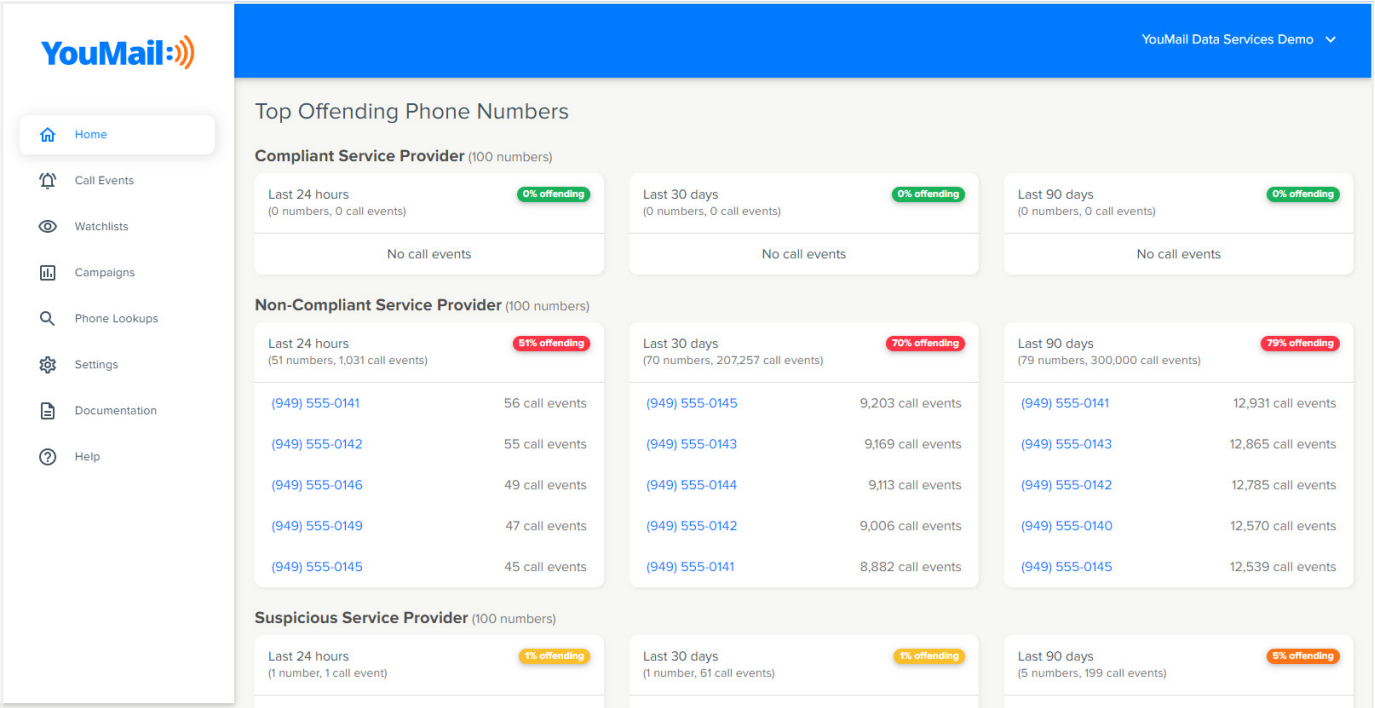
Robocall Threat Sentry operates completely outside of a service provider's network and does not require "trapping" or listening to in-network calls.

When a robocall originates on a service provider's owned number, the Robocall Threat Sentry issues an immediate notification, including the audio file as evidence. This enables the service provider to swiftly correct the suspicious behavior by confidently engaging the customer or blocking their activity.

Mitigate Robocalls from Upstream Networks

Government authorities are taking punitive action against all types of service providers that facilitate robocalls, including transit networks. Service providers offering international gateway and other transit services to upstream networks risk penalties when they carry robocalls from those networks.

The YouMail Robocall Threat Sentry can mitigate robocall risks from upstream networks. It monitors traffic samples segmented by upstream network, enabling you to quickly identify providers that are sending robocalls and take action to mitigate the traffic.

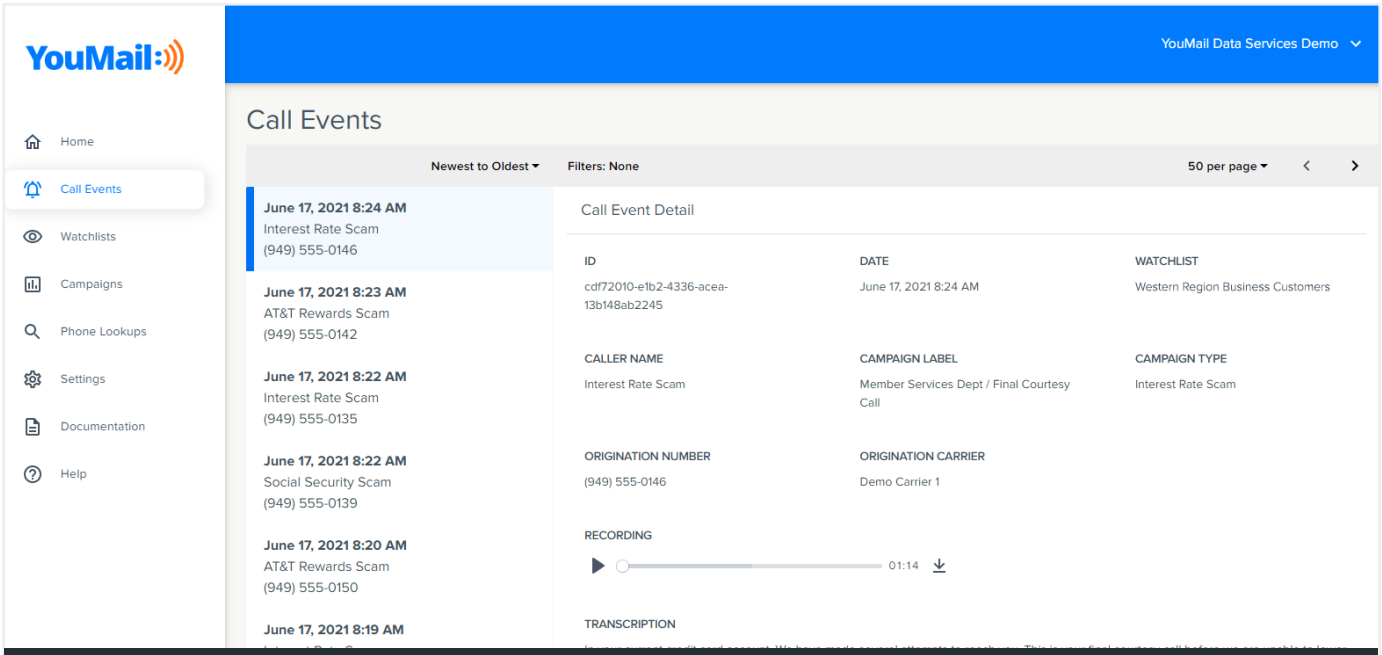


Home screen provides at-a-glance summary of robocall activity by owned TNs and upstream networks.

Strengthen Attestation with Customer Behavior Analytic

A strong "know your customer" program is essential for applying proper attestation to STIR/SHAKEN caller authentication protocols. Originating service providers can be blind-sided by bad actors masquerading as legitimate businesses, or when customer networks are hacked.

Robocall Threat Sentry strengthens know your customer programs by continuously monitoring their behavior. It protects originating service providers from gaps in customer vetting processes that can allow bad actors to originate robocalls.



Call Events screen provides details about each threatening call originated by an owned TN.

Maintain a Clean, Robocall-Free Network

Robocalls can be a drain on a service provider's business, sapping network resources, diverting personnel, smudging its industry reputation, and eroding customer trust. A single account originating robocalls can cause a terminating service provider to black list all calls from the originating network, causing widespread customer dissatisfaction and churn.

In-sourced mitigation solutions require highly specialized development resources, can be costly and time consuming to develop, and must be constantly enhanced as bad actors shift their tactics.

With the Robocall Threat Sentry, service providers can immediately deploy a cost-effective solution that leverages over 10 years of robocall analytics expertise and is field-proven.

Technology Architecture

The Robocall Threat Sentry combines the industry's largest independent call sensor network with powerful AI algorithms that analyze voicemail audio content. Designed to protect users from unwanted robocalls, it actively listens to messages and flags TNs that originate fraud, telemarketing, or other unwanted calls.

The Robocall Threat Sentry reports a reputation score for each monitored TN, indicating the risk that calls from the originating number are unwanted by users.

The service is managed through an intuitive web interface that enables administrators to configure the TNs to be monitored and visually analyze scores over time. Administrators can configure thresholds for notifications to ensure they are immediately aware when reputation changes occur.

The Robocall Threat Monitor reports a reputation score for each TN that it monitors. The score indicates the risk that calls from the originating number are unwanted by users.

The service is managed through an intuitive web interface that enables administrators to configure the TNs to be monitored and visually analyze scores over time. A RESTful API supports continuous TN updates to ensure no illegal traffic escapes the network. Notifications can be delivered via email and the API that integrates with operational support systems for automated remediation. Administrators can configure thresholds for notifications to ensure they are immediately aware when reputation changes occur.

Features	Benefits
AI-powered audio analytics and fingerprinting based on billions of calls in the YouMail Sensor Network.	Accurate, zero-hour detection of unwanted calls mapped to the caller's intent (fraud, telemarketing) based on audio content.
Industry's largest independent call sensor network, monitors calls across US service providers.	Threatening campaigns are identified within the first 1-100 calls, including campaigns that spoof a monitored number.
Intuitive web dashboard.	Perform drill down analysis on TNs with poor reputation scores, including threat type, calling frequency and audio file examples.
Email notifications when TN reputation thresholds are exceeded per watchlist.	Take action to mitigate robocalls.
REST API	Automatically update watchlists and send notifications to robocall mitigation systems.
Downloadable audio files.	Irrefutable robocall evidence that facilitates engagement with customer to modify behavior.
Originating TN file upload (.csv).	Easily configure list of TNs to be monitored.
Supplier to USTelecom Industry Traceback Group, FCC and media.	Leverage the same data provided to authorities.

YouMail, Inc. protects service providers, enterprises, and consumers from harmful phone calls. YouMail protects service providers with robocall mitigation services that detect when they are originating, carrying, or terminating bad traffic on their networks. YouMail protects consumer-facing enterprises by helping detect and shut down imposter traffic that can lead to financial or brand damage. YouMail protects consumers with app-based call protection services.

YouMail's communications platform handles over a billion calls per year for over 10 million users, and the YouMail Robocall Index™, since its launch in September 2015, has emerged as the nation's definitive source on robocalling data for telecom carriers, smartphone and app companies, and public policymakers.

YouMail, Inc. is privately funded and based in Irvine, California. For more information, visit www.youmail.com