Highlights

» Prevents brand damage caused by fraudulent impersonators

» Reduces fraud activity by selected bad actors up to 100%

» Protects customers from imposter fraud campaigns

» Strengthens brand trust and improves contact center call completion rates

» Accurately identifies bad actors based on AI-driven communications analytics

Overview

Brand imposters that attempt to defraud consumers over the telephone can do unmeasurable damage to an enterprise. These bad actors impersonate an enterprise agent in order to steal the customer's identity, access their account, make fraudulent purchases and many more types of attacks. Their campaigns sully the enterprise's reputation and consume significant expense in remediation and prevention.

The YouMail Brand Impersonation Defender helps businesses safeguard brand investments, protect consumer trust, and minimize the drain on resources that occurs when bad actors strike. It uses AI-driven algorithms to identify and monitor imposter fraud and proven effective actions to track down and mitigate the source.

Protect Brand Investments

Enterprise brands are vulnerable to impersonators who initiate voice phishing (vishing) attacks. Bad actors can steal the brand for their own nefarious purposes, quickly diminishing the considerable investments made to build it. The customers victimized by the imposters no longer trust the brand and loudly complain using social media and other channels to multiply the damage. What's more, these attacks can occur on a massive scale as fraudsters use modern, low-cost telecommunications tools to target tens of millions.

The YouMail Brand Impersonation Defender continuously manages and mitigates the risk of brand damage posed by imposters. It combines AI-driven analytics with proven threat mitigation actions to stop bad actors before they have a chance to cause substantial damage to an enterprise brand.

The solution provides a dashboard that continuously monitors fraud activity and measures the scope and intent of each unique brand impersonation campaign. It maintains full, nationwide risk visibility and enables fast, effective management strategies. The dashboard is based on the YouMail Threat Database, the same data source relied on by the U.S. Government, telecommunications industry authorities and leading consumer brands to monitor and manage consumer robocall risk.

An AI-driven analytics engine tracks bad actors and their campaigns independent of their tactics, enabling enterprises to be constantly vigilant against attacks. It correlates campaigns with bad actors so that businesses can prioritize mitigation activities for maximum impact.

Reduce Costs and Resource Drain

When telephony imposter fraud occurs, enterprises often consume significant human resources and expense responding to customer complaints and stopping the bad actors. Identifying fraud sources, compiling evidence and filing legal procedures takes considerable time and effort. All the while, customers are falling victim, which diverts customer service teams from their primary responsibilities.

The Brand Impersonation Defender efficiently interdicts fraudsters, significantly reducing the drain on organizational resources. YouMail works on your behalf, intervening with telecommunications authorities to stop fraud at the source. When YouMail goes to work, it can slash bad actor phone fraud activity up to 100% and often reduces threats on other channels, too, as fraudsters move to less well defended targets. This frees up resources across legal, CISO, contact center and other departments.

The solution provides zero-hour threat detection to rapidly identify the bad actors driving fraud campaigns. It combines the 10M node YouMail Sensor Network with patented AI algorithms to detect new threats by bad actors within minutes and collect the audio evidence needed to shut down their activities.
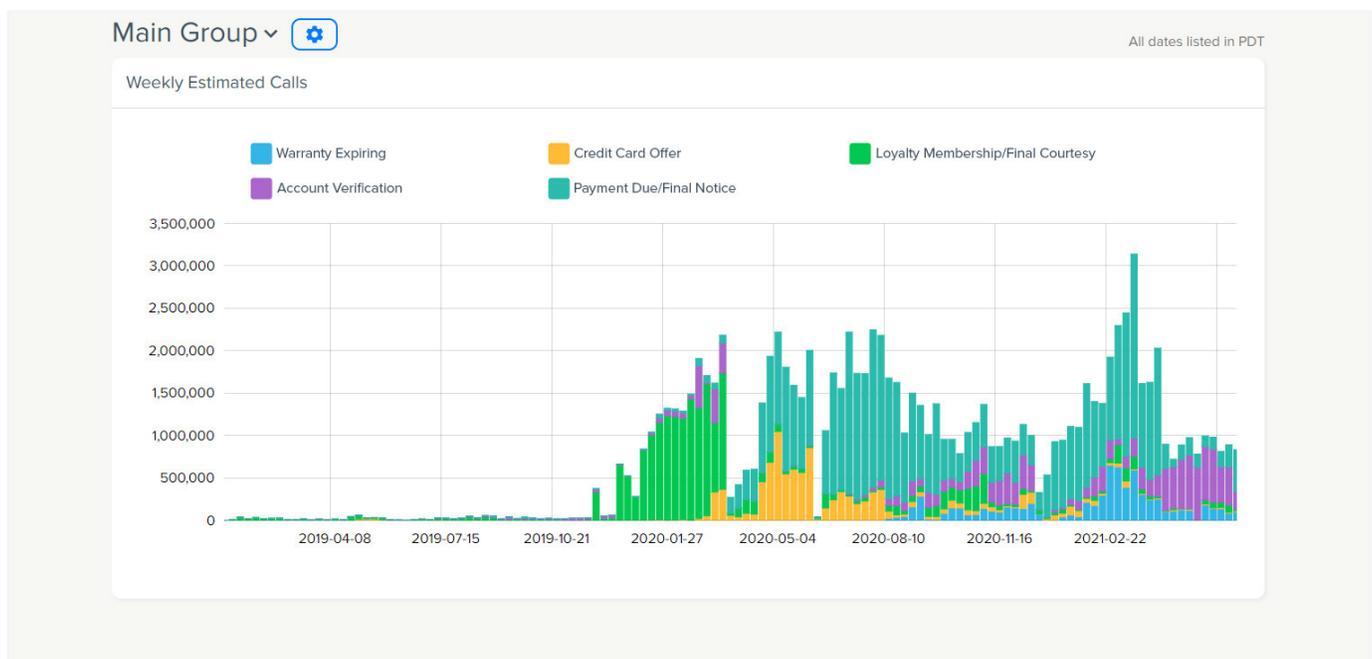
Preserve Sales Revenue Opportunities

In industries that rely on phone calls to make sales, imposters can reduce revenue opportunities. Because imposters can spoof an enterprise's CallerID, consumers may not answer a valid call from an enterprise agent, which reduces call completion rates (CCR). In addition, shady competitors may use impersonation tactics to sell customers an alternative to the enterprise's branded solution, robbing it of legitimate revenue opportunities.

The Brand Impersonation Defender stops imposter calls that cause consumers to lose trust in an enterprise's CallerID and not answer its call. In addition, the solution detects when a competitor is fraudulently using a brand to sell its own service and provides the evidence needed to stop them.

Technology Architecture

The Brand Impersonation Defender combines a live call Sensor Network with powerful AI algorithms to identify imposter calls. The Sensor Network actively listens for fraud among billions of calls received by over 10 million real users across North America.

YouMail AI algorithms analyze audio content to accurately identify imposter calls. It creates unique digital fingerprints that are matched with the telephone numbers used by bad actors. Unlike conventional honeypots that rely upon audio to text transcription, YouMail uses these fingerprints to efficiently and effectively identify subsequent attacks that are part of the same imposter calling campaign.

Fingerprints often follow bad actors wherever they go – across spoofed telephone numbers and multiple originating service providers. YouMail's adaptive algorithms are effective regardless of attack duration, frequency, and other tactics. When fraud is initially detected, YouMail autonomously identifies bad actor campaigns and all associated source phone numbers, enabling immediate and decisive action.
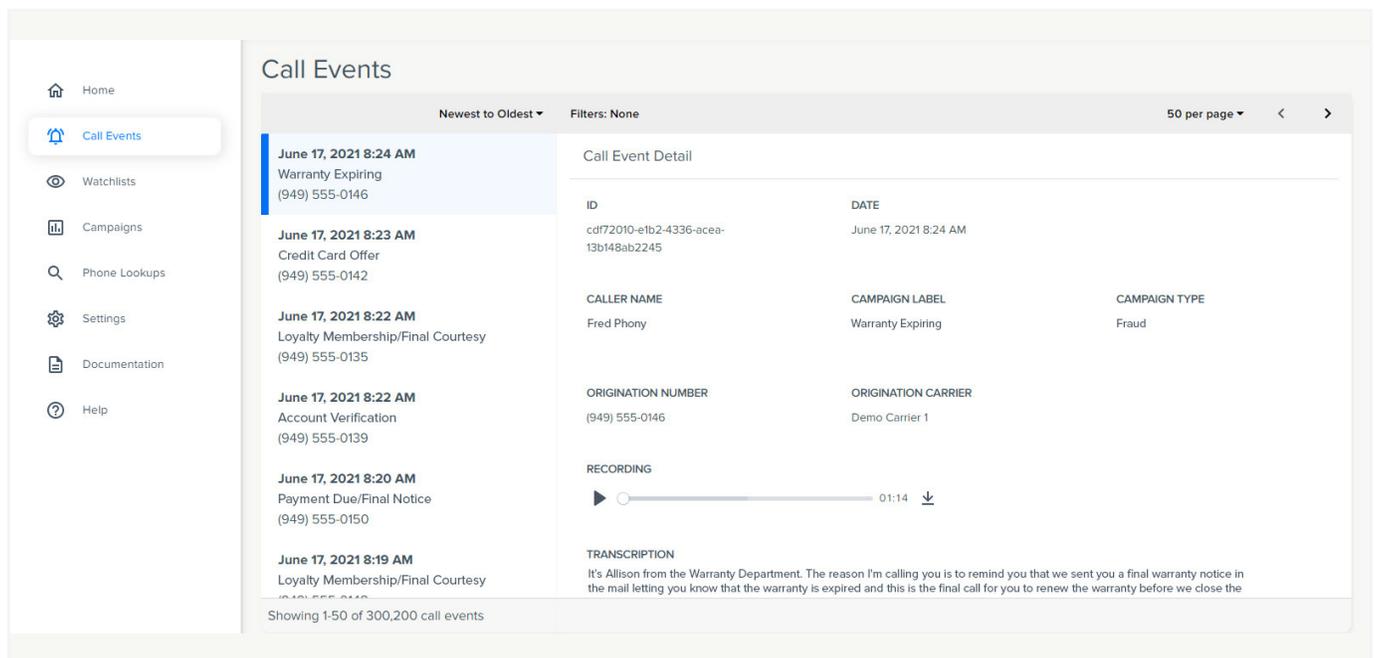
Features

AI-powered audio analytics and fingerprinting based on billions of calls in the YouMail Robocall Sensor Network.

YouMail Sensor Network with over 10M users answering live calls.

Actor and campaign-centric analytics using audio fingerprinting and intention.

Online dashboard visualizes imposter threat landscape.

Proven fraud interdiction procedures using established telecommunications industry channels.

Access media recordings and metadata from identified fraud calls.

Supplier to USTelecom Industry Traceback Group, FCC and media.

Benefits

Accurate, zero-hour detection of imposter calls mapped to enterprise brand(s) and the caller's intent (fraud, telemarketing) based on content.

New attack vectors are identified within the first 1-100 calls for zero-hour detection.

Campaigns are correlated with unique actors to help prioritize mitigation.

Analyze risks and prioritize mitigation actions.

Offloads investigations from internal resources and rapidly stops bad actors and their campaigns.

Use as evidence in legal procedures and complaints.

Leverage the same data provided to authorities to stay ahead of investigations.

About YouMail

YouMail, Inc. protects consumers, enterprises, and carriers from harmful phone calls. YouMail protects consumers with app-based call protection services. YouMail protects carriers 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'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 https://www.youmail.com