Testimony before the

SENATE COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION

Subcommittee on Communications, Media & Broadband

Protecting Americans from Robocalls

October 24, 2023

Testimony written and presented by:

Michael Rudolph
Chief Technology Officer
YouMail, Inc.

Michael Rudolph
YouMail, Inc.
43 Corporate Park #200
Irvine, California 92606
(800) 374-0013
mrudolph@youmail.com

www.youmail.com
www.youmailps.com
www.robocallindex.com

Protecting Americans from Robocalls

October 24, 2023

Chairman Lujan, Senator Thune, and Members of the Committee, I thank you for the opportunity to appear and testify today regarding the current state of the operations, investigations and enforcement actions relative to omni-channel robo-communications – both robocalls and robotexts as well as phishing tactics and platforms including vishing, smishing, and generative AI.

I provide my testimony today as Chief Technology Officer of YouMail, a privately held company whose mission is to protect the public from harmful communications and to restore trust in our communications networks.

I. Introduction

YouMail is often recognized for its role providing data in the behind-the-scenes battle against unwanted voice calls. The company's origins, as its name suggests, trace back to being one of the innovators and first providers of visual voicemail and cloud-based voicemail answering services in the United States.

As early as 2009, YouMail recognized that the demand for its solutions was linked to individuals who relied heavily on receiving dozens to hundreds of daily live, inbound calls to their personal mobile phone number. These individuals spanned a wide range of high-touch professions that are considered very small businesses (VSBs) in America: fitness trainers, tutors, repairman, electricians, plumbers, exterminators, realtors, interior designers, handymen, contractors (floor, paint, tile, carpentry, construction), appraisers, notaries, mobile mechanics and detailers, dog sitters/walkers, photographers, event planners, florists, babysitters, caterers, bakers, accountants, financial planners, landscapers, movers, stylists, barbers, beauticians.

It's important to acknowledge that professionals such as these find their success and income depends on how they respond to incoming calls from unknown numbers. Before unwanted and illegal calls from unknown numbers invaded our phone network, these calls from outside of contact lists typically meant a potential new customer for this VSB. For sole proprietors, unknown calls signaled an opportunity to connect with a prospective local customer to generate income to provide for themselves and their families. Failure to answer the live incoming call often meant the potential lead for their small business would move on to call the next highest rated provider, discovered on search engines or websites such as Yelp, that may have a lower rating, but were available at just that moment to answer the live call and interact with the caller. At one time, and still perhaps today, answering live calls from unknown numbers was a critical path to success for small businesses.

As any good business asking its customers what they needed next, YouMail recognized the need to silence the ringer for these subscribers when the call was almost certainly spam, but also to ensure real local customers calls would ring through to be answered live to then ideally become appointments and customers for very small businesses. As a visual voicemail and answering service, and not just a device

ring blocker, YouMail provided a fallback as voicemail audio is converted into readable text and a small business, like any user, could quickly determine the purpose of the call.

In 2009, YouMail began investing in technology and techniques to identify calls as spam or unwanted, both in order to prevent ringing and also to move unwanted messages into a Spam folder, as most users are accustomed to experience with email.

Eventually, as unwanted robocalls became an evidence signal in everyone's voicemail box, YouMail launched the Robocall Index in 2015, which over time has become recognized as the standard for industry metrics on robocalls occurring nationwide, as well as per-state and per-metro region.

YouMail's role as an over-the-top app, trusted to provide answering services to millions of telephone numbers across all major US and Canadian carriers, provided it with unique capabilities to respect consumer privacy while tracking and grouping unlawful communications throughout the mobile phone networks. It is worth noting that YouMail data is nearly entirely based on what reaches consumer handsets, and does not extend to communications blocked at the network of the underlying carrier, which certainly would indicate even more by way of voice and SMS communications attempting to reach consumers.

In late 2019, YouMail launched its YouMail Protective Services division, which assists law enforcement, financial services, enterprises, and communications providers with its data, evidence, intelligence, and investigative services.

As YouMail's role in industry has expanded, innovative bad actors behind unlawful and unwanted communications have become aware of YouMail's industry role. YouMail is already observing efforts by both telemarketing and threat actors to evade YouMail's methods of detection by minimizing calls and voice evidence to YouMail users or by trying to directly obtain access to YouMail data for similar evasive purposes.

II. Caller and Call Recipient Relationships

As many state and federal agencies have reported over the years, unwanted communications, particularly robocalls and robotexts, rank among the top complaints received by their offices.

One of the difficulties in analyzing communications is determining whether a communication is spam, generally unwanted by most recipients, or is perpetrating a scam or committing fraud. This is particularly challenging as the content of a communication may be nearly identical when it comes from an enterprise such as a bank, utility, or government agency as it is when it originates from an imposter.

It is helpful to consider different classes of originating callers from the perspective of an average person, as this classification helps to understand a common, generally desirable experience based on the relationship between that average call recipient and the calling party.

In the examination of types of caller relationships, we may consider why an individual may be at a moment in their life that would affect their susceptibility to answering a live, incoming communication from an unknown, non-contact telephone number.

- **Personal** – these are communications between two individuals who know each other and may or may not yet be saved contacts on the device. These are friends, family, colleagues, co-workers, classmates, acquaintances who usually have a direct, personal relationship, or may be introduced through a mutual acquaintance. If you or your child have joined a new school or club, you may be expecting a call or text message from a teacher or coach from an unknown number. While it's nearly universal, personal calls are not always wanted such as cases of harassment or stalking, but any desired blocking in this case is between two individuals for personal reasons.

- **Local Business** – these are not often personal relationships, but between an individual or household and small local businesses or services. This would include your dry cleaner communicating your garments are ready, or a local restaurant confirming a reservation, or your handyman, gardener, babysitter, dogwalker, trainer, or healthcare professional discussing an appointment, problem or matter. These are sometimes saved contacts, but often when someone has an urgent need, they may be expecting calls from several potential unknown numbers that provide a local service in order to address that time-based matter or need. While this is also nearly universal, sometimes disputes between a customer and service provider may lead to an individual wishing to block these communications. Or, if a local business has crossed a line from communicating about appointments/inquiries/problems into using the communication channel for marketing or lead generation, these calls may drift into unwanted and blocked territory. Once again though, these types of calls are almost universally wanted apart from the situation where two parties have a personal conflict.

- **Non-Local Business** – these are communications between a national, regional or online business and an individual and are also where most universally unwanted communications occur, although not all communications between individuals and households and non-local businesses are unwanted. These interactions typically fall into a few sub-categories:
    - Essential: these would be appointment reminders and confirmations, one-time or password reset events, critical account/emergency alerts where the individual's interaction is necessary (password reset or transaction confirmation) or the individual would be impacted based on their assumption of a time/place/occurrence.
    - Marketing, Originated by Individual/Household, Follow-up: these communications rely on a triggering event typically where the individual expressed an interest in the business, ideally directly through a communication initiated by the individual/household that occurred online, in-person or by phone.
    - Marketing, Originated by Non-Local Business, Goal-Driven: these communications usually begin with a sales, marketing or operations team at the business that is interested in demand generation to stimulate sales or engagement in products or services, regardless of any recent interaction by the individual/household.

- **Scam / Fraud** – these are communications which can be disguised to look like **<u>any of the above</u>** as they reach an individual or household and rely on TTPs (tactics, techniques, and procedures) that emulate a real individual, local, or non-local business, as described previously, as closely as possible in order to maximize their success.

III. Call Recipients Want To Know Who Called

Society has been shifting away rapidly from voice calls, as the voice communications network has become filled with unwanted and unlawful voice calls.

When someone receives a call from an unknown number, they want to know **who called** and **the reason** the call was made.

Individuals and households are particularly susceptible to answering calls from unknown numbers based on time and situation-based events in their lives. The originators of unwanted and unlawful calls make repeated call attempts, hoping to get their timing right for these live answer opportunities.

Call recipients generally fall into one of two camps during these moments of answering susceptibility – those who will answer all unknown numbers during these windows of vulnerability, and those who allow the calls go to voicemail, hoping to identify the anticipated call and to call it back if it matched an expected call. In the case of returning a call based on a voicemail, this can mean having to wait on hold and navigate an interactive voice response (IVR), and a loss of time simply due to a best practice of screening incoming calls from unknown numbers.

When a legitimate caller has a significant enough situation to merit a voice call as the chosen medium of communication and places a call, they have no good reason to not leave a message.

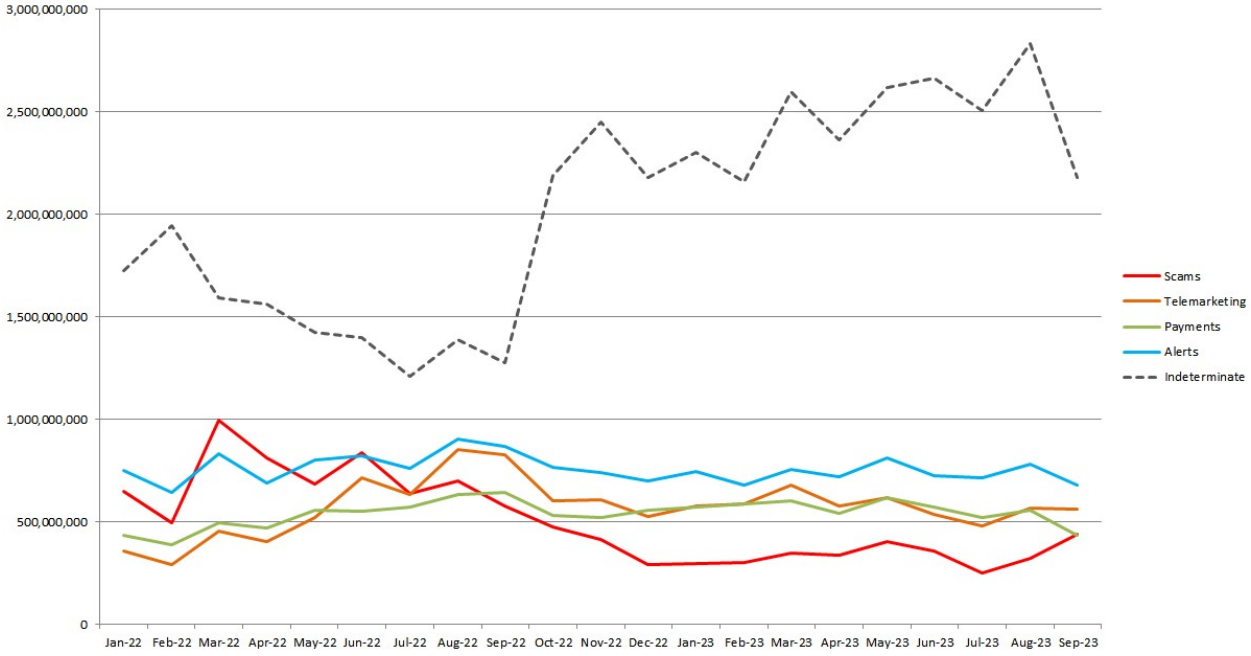
Consider all the potential relationships and legitimate reasons for a call between a lawful caller and call recipient. If the caller suspects the call recipient doesn't know who it is based on the high likelihood it is not a personal contact saved to the device, the caller would want to identify themselves and their reason for calling to encourage engagement from the called party, since there was an important reason for initiating a voice call.

As we expand into the "Marketing, Originated By Non-Local Business, Goal-Driven" relationship and use case above, the company that is using the voice channel to engage in telemarketing, if they possess the conviction that their marketing offer is worth initiating the voice call, should maintain that conviction that the call is important enough to identify themselves and the purpose of their call initiation in a voicemail message.

By not leaving a message, the call initiator could suggest their additional attempts, making many more calls to the recipient, are because they are still trying to deliver the message. The subsequent attempts may not be necessary if the message was left on the first attempt and the individual was able to make a decision based on this evidence to respond to the communication by any indicated, allowable channels.

YouMail attempts to classify calls received by consumers into several categories and has been tracking this data for several years. YouMail relies on lawful, legitimate call originators, or bad actors imitating those call originators, obeying this societal protocol that if it was important enough to initiate a voice call, it was important enough to indicate who you are and why you called.

YouMail, via the Robocall Index[1], observed a significant increase in indeterminate, non-categorizable robocalls beginning in September 2022.



Because the telephone numbers linked to indeterminate robocall behavior do not possess a history of delivering desirable/wanted communications, YouMail infers that they are linked to unwanted and undesired behavior, as they do not provide audio evidence of their identity or reasons for calling recipients.

This increase in indeterminate calls also correlates to a decline in observable calls linked to scams and telemarketing, so it is reasonable to assume some of the parties behind those calls have shifted their tactics to call and hang up in order to evade consumer recognition, as well as detection by services such as YouMail that utilize audio evidence in voicemail to prevent and support enforcement against unwanted and unlawful communications.

Present enforcement and traceback efforts often rely on the audio content of the call in order to wield it as evidence of unlawful activity in an investigative process. If a robocall operation is sophisticated enough to use evasive strategies such as utilizing attested calls made in very low volumes across an inventory of real numbers, and across a span of enabling providers, while leaving no audio evidence (permitting access to CPNI under the Communications Act Section 222-d-2), it becomes much more difficult to track, investigate, and prevent.

Establishing a requirement for business communications to leave a voicemail when they introduce a new originating number to communicate with a specific call recipient not only serves the interest of consumers

[1] https://www.robocallindex.com

who want identity and purpose to accompany unanswered, unknown calls, it also serves the legitimate business to solicit reciprocal engagement from the recipient, assuming this communication achieved the litmus test of having been worth initiating a call in the first place.

Further, voice service providers can track this behavior in new and existing accounts, ensuring that their logs of calls from accounts that have identified as a business that need to make hundreds, thousands or millions of calls are making calls of a duration long enough to permit them to convey their identity and reason for calling. Accounts refusing to follow this policy would have no reasonable explanation, as their communications are either not valuable enough to pay for the extra 5-30 seconds per call (and thus were not valuable enough in the first place to disturb and disrupt the recipient's day), or they did not want recorded evidence by way of voicemail of their operations and were likely unlawful or illegal.

IV. Omni-Channel Marketing & Communications

Marketing technology, communications technology, and their subsequent integration into consolidated platforms have made significant advances in the past decade. A litany of acronyms from the tenured CRM (Customer Relationship Management) and CPaaS (Communications Platform as a Service) to more recent upstarts such as CDP (Customer Data Platform) and CEP (Customer Engagement Platform) highlight the rapid innovation and convergence of automated omni-channel marketing applied to integrated recipient data.

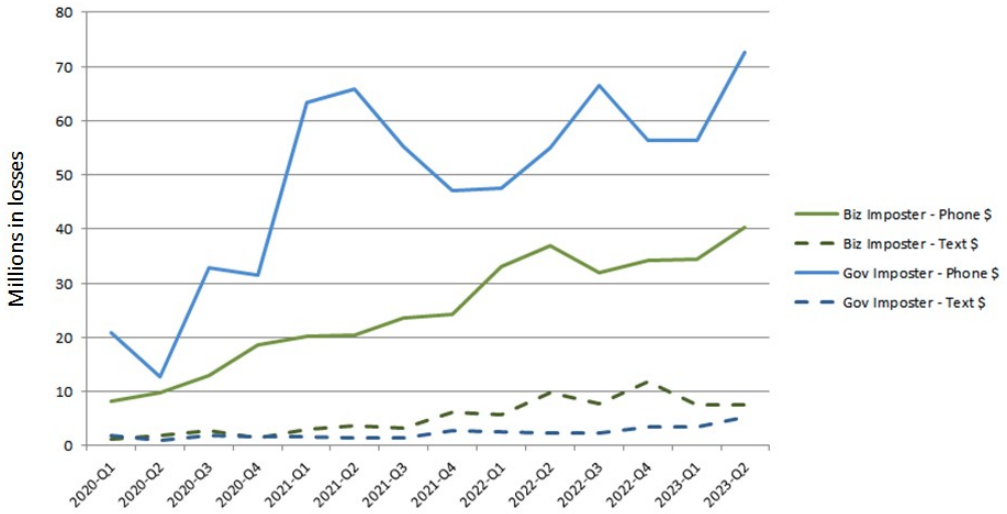
Omni-channel marketing engages a single recipient through many media, sometimes simultaneously, sometimes as a scripted sequence of conditional events. A good omni-channel marketing platform allows the marketer to upload a list of recipients and to buy ad placements on search engines or websites, send emails, generate calls and send TXTs, engage in messaging conversations and host a telephone number with a menu for incoming calls. Domain registration and website building has become trivial enough that some tools can be given a domain and create a similar looking website with a few clicks for under $20.

A competent individual can invent a company and deploy a sophisticated omni-channel marketing operation in hours and at low cost, choosing from hundreds of vendors, ranging from fledgling start-ups to publicly traded firms. Some platforms, seeking to accelerate their own growth through streamlined onboarding, allow communicating with a customer list on trial plans with no financial transaction (or vetting) necessary. The barriers to "looking big" and "communicating wide" have never been lower, which is tremendous for encouraging new entrepreneurial ventures in competitive markets, but also enables a tremendous opportunity for bad actors mimicking these real businesses to gain access to these advanced tools.

Though YouMail and its Robocall Index have observed that robocall volumes have declined slightly from 58 billion in 2021 to an estimated 53 billion by end of 2023, the FTC and FBI both indicate rising reported losses in the complaints gathered from consumers. These are only the losses reported to these specific agencies, and significantly understate the true consumer harm, as only a subset of losses is ever reported.

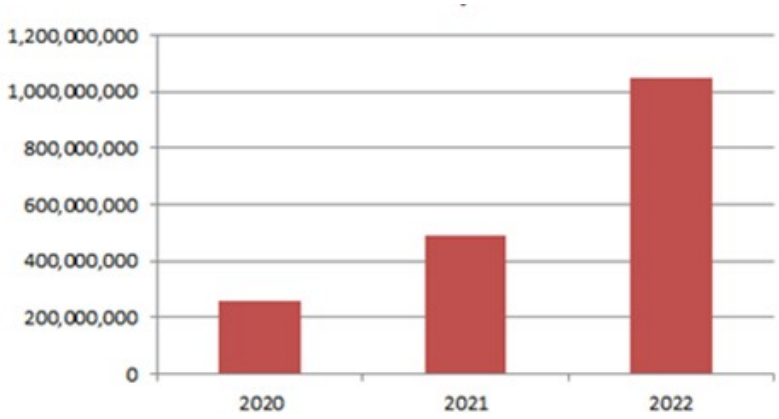
The FTC Consumer Sentinel Network Tableau site[2] shows a 400% increase in Business Imposter dollar losses reported since Q2 2022.

FTC – Reported Losses (in Millions) to Business, Government Imposter By Medium



The FBI IC3 Data[3] shows a rise in reported financial harm from Government Impersonation and Tech and Customer Support losses. These are the categories of losses in which voice or SMS were used to impersonate a known organization.

FBI IC3 – Losses to Government Impersonation + Tech and Customer Support Imposter



Legitimate enterprises have shifted to omni-channel marketing as it is more effective in soliciting customer engagement and inducing more transactions. Advanced threat actors who wish to successfully

[2] https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts

[3] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

impersonate an organization study the organization's current practices and, recognizing the user of omni-channel communication (ads, online, web, email, voice, SMS, app), it should be no surprise that the threat actors embrace similar tactics and platforms to increase their success rates with victims.

Even more advanced threat actors take advantage of APIs provided by these platforms and entrench themselves across multiple accounts and multiple platforms to reduce the impact of a single disruption or take-down. As astute recipients/targets report the attempt by the threat actor, only one of hundreds or thousands of accounts are deactivated, and criminal operation continues with minimal operational impact.

V. Generative AI & Pig Butchering

Since 2022, many omni-channel marketing and communications platforms have been rapidly introducing and announcing the benefits of integrating capabilities of LLMs (large language models) and generative AI.

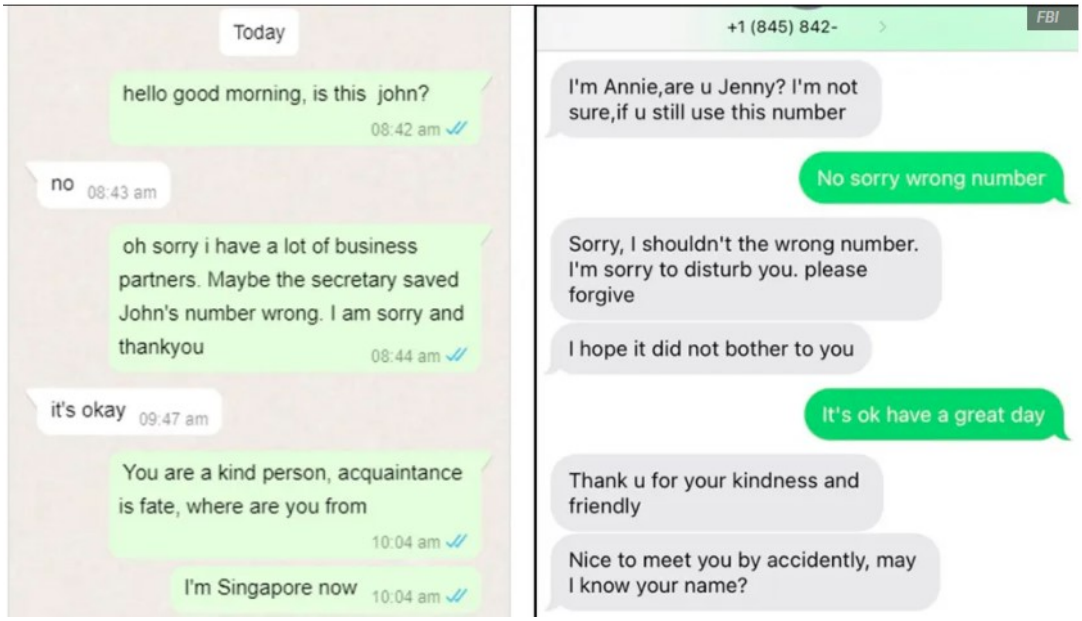
The benefits to a legitimate marketing operation should be obvious – you can simultaneously communicate with more people on a personal level through almost every available medium of communication. One marketer in a small operation can leverage generative AI to speak personally and fluently in nearly any supported language with tens of millions of recipients daily.

Prior to widespread use of generative AI, YouMail would observe 'broken English' in robocall or robotext campaigns that identified as a bank. Poor command of the English language serves as an obvious tell, indicating a campaign is operated by a fraudulent imposter.

One such example YouMail has shared is in generating the script "press 1 to connect to a fraud specialist" to emulate a financial services firm, a Chinese-speaking threat actor with limited skills at English may use a simplistic tool to translate the Chinese word "生成" (shēngchéng) to either "generate" or "connect". YouMail's investigators would observe the audio "press 1 to generate to a fraud specialist" as an indication of fraud as it is highly unlikely a US-based financial services firm would make such a mistake. With threat actors leveraging well-trained, fluent generative AI platforms, such mistakes rarely occur, which then requires additional investigative resources and collaboration to separate legitimate and imposter communications from one another.

As YouMail has expanded its investigative and protective solutions to cover SMS, MMS, RCS and other messaging technologies, it has observed conversations that are clearly evidence of "pig butchering" attacks.

"Pig butchering" often begins by using a messaging platform such as SMS to initiate a conversation that is otherwise indistinguishable from personal conversation by saying something like "Hi" or "Hey Ben, it was good talking last week". If engaged, the conversation apologizes awkwardly for the accidental message but maintains a friendly, charismatic tone and works to establish a casual friendship as a goal. Often, the threat actor is awkward and apologetic, citing English as a second language to cover for any misunderstandings.



Sample pig-butchering conversation provided by FBI and used by NBC Miami
https://www.nbcmiami.com/news/local/new-pig-butchering-crypto-scam-stealing-millions-from-south-floridians-fbi/3009914/

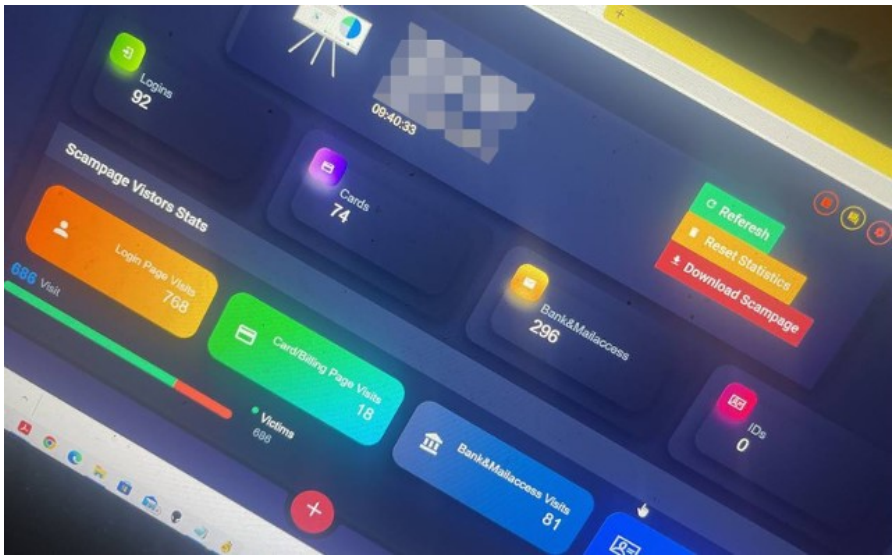
Over time, the threat actor builds a rapport and encourages its target to take certain actions which range from things that may feel trivial like checking out an app or visiting an interesting website. Ultimately, they are more successful the more they appear authentic and patient and don't force their target to immediately connect Apple Pay to their bank account or begin "investing" in cryptocurrency.

A single threat actor using generative AI connected to the communications network can run hundreds to thousands of simultaneous conversations, refining its model while learning from mistakes and exercising patience in rapport-building indistinguishable from a real person. The technology already exists to generate synthetic yet authentic appearing images, video and audio, if those prove necessary hurdles in carrying out further artificial trust-building to support the criminal endeavor.

Messaging continues to trend towards technologies with E2E (end-to-end) encryption (iMessage, RCS, WhatsApp, Telegram) and advanced pig butchering initiated by SMS often tries to move the conversation to an E2E encrypted medium in order to evade detection via unencrypted channels as it reaches deeper, detectible evidence of malfeasance in later steps of its script.

A recent blog[4] from digital risk protection vendor Phishlabs includes several screenshots of how quick and easy an aspiring threat actor can make a few clicks using a PhaaS (Phishing-as-a-Service) platform to deploy automated omni-channel phishing services with out-of-the-box capabilities to impersonate 11 US financial services institutions. The site regularly holds sales.Recent rates to send SMS messages ranged from $130 to send 5,000 SMS messages or $620 to send 25,000 SMS messages.

[4] https://www.phishlabs.com/blog/threat-actor-profile-strox-phishing-as-a-service/



Real-time dashboard from PhaaS provider as live potential victims interact

Anniversary sale prices advertised by PhaaS provider with SMS messaging allowances

VI. Tools, Resources, Success

While the FTC and FBI data indicates an increase in reporting of individual financial harm from communications, despite stability in total robo-communication volumes, the media, trade shows and industry investments reveal a sprint to connect advanced tools such as generative AI and omni-channel marketing platforms to the communication network. Nonetheless, progress has been made in industry to use new tools and techniques to curb high-volume robocall operations that once upon a time plagued consumers.

STIR/SHAKEN

STIR/SHAKEN is one of most cited tools to assist in the combatting of unwanted, unlawful robocalls, with many deadlines for implementation passing in 2022 and 2023.

YouMail tracks the certificates on the voice calls that terminate at its network, and where the voice call matches a known unwanted, unlawful, or illegal campaign, it links the originating or gateway provider that indicated it owns responsibility for attesting to that call.

As of September 2023, YouMail was observing nearly 800 distinct certificates per week in the calls that it answers. YouMail has yet to publicly publish statistics on its observed certificates, but YouMail's observations match the approximately 800 signers in data published[5] by TransNexus. TransNexus also notes the approximate number of 1,200 SHAKEN-authorized providers as of September 2023.

As of October 18, 2023, YouMail observes that there are 17,900 entries in the FCC 499 Filer database[6]. 4,789 entries identify their principal communication type as 'Interconnected VOIP'. As of October 18, 2023, the FCC Robocall Mitigation Database [7](RMD) contained 8,562 entries. 2,891 of the RMD entries state "Complete S/S Implementation" and 1,980 entries state "Partial S/S Implementation, Performing Robocall Mitigation" for a total of 4,871, indicating some STIR/SHAKEN implementation.

It would appear that there are somewhere between 8,000 and 20,000 entities that acknowledge themselves as relevant voice communication providers, so these 800 certificates presently active in September 2023 are potentially only indicating origination information for 4-10% of communication providers.

STIR/SHAKEN & Sample YouMail Investigations

YouMail, as an answering service for customers of mobile network operators (Verizon, T-Mobile, AT&T, et al.), relies on customers setting up their call forwarding feature to divert unanswered calls to YouMail's service. Consequently, YouMail, and services like YouMail's, rely upon voice providers implementing the IETF RFC 8946 Personal Assertion Token (PASSporT) Extension for Diverted Calls in order to carry the originator certificate through to YouMail as the final termination point for a call. When unimplemented at a network, YouMail typically observes a mobile network operator introducing its own certificate (at the lowest level of attestation, a C-attestation) in place of the originating provider's A-attestation, when diverting calls. This negatively affects transparency regarding the origination of unlawful call campaigns carried in the ecosystem on diverted calls going to voicemail services like YouMail.

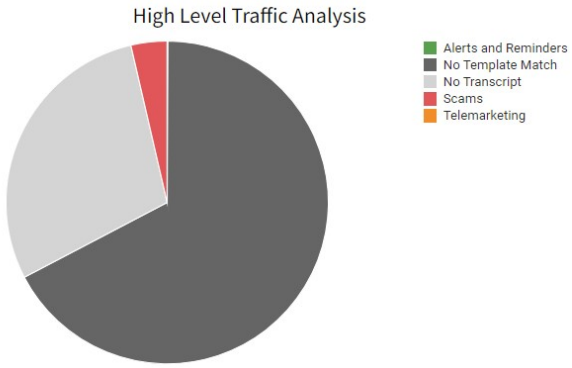
[5] https://transnexus.com/blog/2023/shaken-statistics-september/

[6] https://apps.fcc.gov/cgb/form499/499View.htm

[7] https://fccprod.servicenowservices.com/rmd?id=rmd_welcome

When the originating provider's certificate carries successfully to the call termination point, companies such as YouMail can perform aggregate analysis on the calls received from an originating provider by matching content (such as voicemail) to the originating service providers.

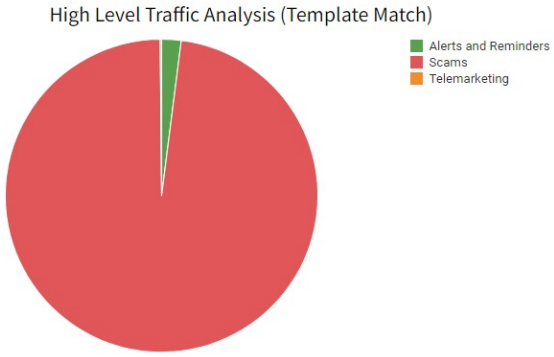
Below is a sample pie chart indicating the content carried by an originating provider's traffic for a month:



This pie chart reveals:

- a light grey area where callers left no message
- a dark grey area where a message was left but did not match the template of a known robocall
- a red area, representing calls for which the audio matched audio of a call suspected to be a scam

It is often helpful to exclude the light and dark grey areas (to remove calls not providing audio evidence and calls where the audio evidence wasn't able to be matched to known good or bad robocalls) in order to produce a drill-down pie chart of all recognized robocalls at that provider.



This pie chart reveals that, of the tracked robocalls at this provider, the majority appear linked to scam campaigns, with only a small green wedge linked to potentially legal/lawful alerts and reminders.

Underlying this pie chart, YouMail can examine the exact campaigns and their relative volumes as they compose this provider's traffic profile. At the time of this testimony, the current campaigns identified here are linked to their best, most likely classification, so this is not intended to be definitive attribution of a campaign to illegal behavior but rather the current suspected nature of these campaigns.

In the case of this sample provider, it reveals A-level attestations were given to audio and calls determined to be carrying illegal, unlawful content. It would indicate accounts that should be terminated if the activity is confirmed within the provider's records and a legal imperative to perform an investigation to find and terminate accounts carrying similar traffic. In the case below, the top campaigns found were "Google Business Listing Scams", "Amazon Alexa Scams", and "Government Grant Scams". What is also of note is that this provider has very little traffic that indicates lawful, desirable robocalls to be received by consumers (such as a prescription reminder, or change-of-venue alert, etc.).

Categ... Name	Group Name	Type Name	Campaign	Attes-tation	Calls Volume Indication
Alerts and Reminders	Inbound Call Alerts	Messaging System Calling	Mortgage Connoisseur	A	
			Fast Pickup	A	
Scams	Business Related Scams	Amazon Alexa Scam	Amazon / Alexa Found Easily	A	
	Government Money	Government Grant Scam	Employee Retention Refund	A	
	Search Listings	Google Listing Scam	Not Verified Or Missing	A	
			Find Your Business Online	A	
			Business Listing Needs Attention	A	
			Verify Your Business	A	
			Flagged For Review	A	
			Verify Your Google Listing	A	
			Done with Voice Command	A	
			Google Business Account	A	
			Google / Amazon Alexa Listing	A	
			Claimed or Verified	A	
	Unclassified Scams	Generic Scammer	Hi My Name Is	A	
	Warranty Scams	Vehicle Warranty Scam	National Dealer Services	A	
Telemarketing	Business Related	Google Listing Spam	Verify Your Listing	A	
	Religious Spam	Religious Spam	Press One	A	
	Unclassified Telemarketing	Generic Robocaller	Hello Hello Hello	A	
			Beep Beep	A	
			Experiencing System Problems	A	
		Random Spam	I'm Sorry, I'm Sorry, I'm Sorry	A	

YouMail's position is that STIR/SHAKEN is an extremely valuable tool that is still in the process of industry adoption, despite recent FCC deadlines. It is a tool presently lacking sufficient resourcing to carry out investigative, compliance, and enforcement efforts and success in curbing robocalls ultimately depends on the resources applied to ensure data is not only properly collected but integrated into the ecosystem to maximize transparency.

It is a non-trivial undertaking to prioritize and investigate thousands of active robocall campaigns each month, understand their legality and effect corrective action where necessary.

KYC (Know-Your-Customer), KYT (Know-Your-Traffic), Know-Your-Upstream (KYUP)

During our investigation-related discussions with voice service providers, they regularly indicate that they were unaware that the indicated account was carrying the communications provided in the supporting evidence attached to the reported incident. Conversations such as these indicate that many providers, intentionally or unintentionally, do not truly know their customers.

Over the past few years, a few parties have weighed in on best practices and requirements for communication providers to "know your customer" or "know your traffic". The FCC recently also included "know your upstream provider" [8] to this growing lexicon on April 27, 2023.

When illegal communications are injected into public communications, it should not matter whether the account holder is considered a "customer", "peer" or a "provider" and it should not matter what the enabling platform considers itself (gateway, intermediate, facilities-based, etc). All platforms enabling communications share responsibility in preventing accounts originating illegal, unlawful communications.

An FCC filing [9] by private company Numeracle, on April 27, 2023, included Numeracle's Model Standards v1.1 for KYC, which includes a list of questions to ask new customers. Numeracle's list is comprehensive, including asking the prospective customer to share marketing materials, reveal prior actions or judgements, provide descriptions of the calls along with consent collection and legal compliance practices. Another example of good KYC policies and controls can be found in settlements between recidivist providers enabling robocalls, such as the March 6, 2023 settlement between State of Texas et al and Rising Eagle Capital Group LLC [10] .

An account faced with strenuous onboarding Q&A that is planning to initiate illegal or grey-area telemarketing communications is unlikely to proceed with establishing the account at a provider using processes such as these, as it indicates the bad actor is likely to be either rejected before they can start sending communications, or if they misrepresent themselves, their ability to communicate would be short-lived before they face a permanent termination.

YouMail is often asked to comment on KYC Practices and observes many communication providers want to keep their current practices private, because they are viewed as both:

- a legal liability, if revealed (and ultimately proven intentionally or unintentionally insufficient)
- a competitive advantage

Interestingly, interpreting the KYC process as a competitive advantage perception cuts two ways. Some providers view their "light touch" policies, procedures, and controls as an advantage because they maximize their revenue in turning away only the most egregious new accounts, while permitting less egregious yet still unlawful revenue-bearing accounts to onboard. On the other side, providers with stricter controls and policies comment they are playing the "long game" and, while they lose out on this potential revenue in the short term, they envision they will eventually see account migrations from peers and competitors, as those peers and competitors are publicly identified as a risky supplier for legitimate high-revenue enterprises.

[8] https://docs.fcc.gov/public/attachments/DOC-392975A1.pdf

[9] https://www.fcc.gov/ecfs/search/search-filings/filing/1042778647719

[10] https://www.texasattorneygeneral.gov/sites/default/files/images/press/Spiller%20Stipulated%20Order.pdf

KYC, Analytics, Call Labeling & Blocking

Numeracle filed further comments[11] with the FCC on August 9, 2023, through which they addressed the current state of analytics, labeling, and blocking. Some of Numeracle's[12]commentary was furthered by an FCC filing made that same day by United Office[13], who included screenshots demonstrating how their customers' calls were displayed on Android and iOS devices across major carriers.

Both Numeracle and United Office cite working with customers who had their calls labeled as 'Spam Likely' or 'Scam Likely'. Seeking to remediate the labeling on behalf of their customers, they worked closely with them to get to know them and determine whether these calls were mislabeled, often to provide evidence to call analytics companies and voice providers in order to correct the mislabeling.

YouMail has observed that telephone numbers of legitimate calling parties (banks, government, security alerts, emergency, and disaster alerts) drift from accurate labeling to 'Spam Likely' or 'Scam Likely' treatment over time at individual mobile operators,without any evidence to show that the numbers have been compromised or spoofed by a threat actor. As the mislabeling occurs, YouMail also observes that its customers with the YouMail app installed on their device no longer answer these calls, indicating that mislabeling an incoming call effectively results in the same outcome as blocking the call as it drifts into an answer rate below 5% when prior answer rates exceeded 50%.

Typically, engagement with services or solutions that would remediate and clear up this mislabeling corrects the issue. As expected, this generates revenue for vendors that provide these solutions and results in increasing the costs of this business communicating with its customers, which could eventually mean this business passes those higher costs to communicate along to its customers.

YouMail has also observed in its investigations that many robocalls received by consumers receive a "green checkmark" treatment as they appear on devices. TransNexus indicated in their September 2023 blog.[14] that among prolific robocall signers, 88.46% of calls they signed with B-level attestation were robocalls and 79.4% of calls they signed with A-level attestation were robocalls. Robocalls with C-level attestation trend downward (from <40% in April 2023 to <20% as of September 2023) .

Robocall operators are the most engaged, active calling parties seeking to stamp their calls with legitimacy in their quest to maximize engagement and answer rates. As a result, they have become the most prolific early adopters of new services that promise them A attestations for their calls. This presents distinct challenges to measure the benefit of labeling and display indicators like checkmarks to

[11] https://www.fcc.gov/ecfs/search/search-filings/filing/108102252803712

[12] https://www.fcc.gov/ecfs/search/search-filings/filing/108092119116596

[13] https://www.fcc.gov/ecfs/search/search-filings/filing/108092119116596

[14] https://transnexus.com/blog/2023/shaken-statistics-september/

the public when legal, legitimate call originators are slower to adopt than the operators of suspect, grey-area or unlawful calls.

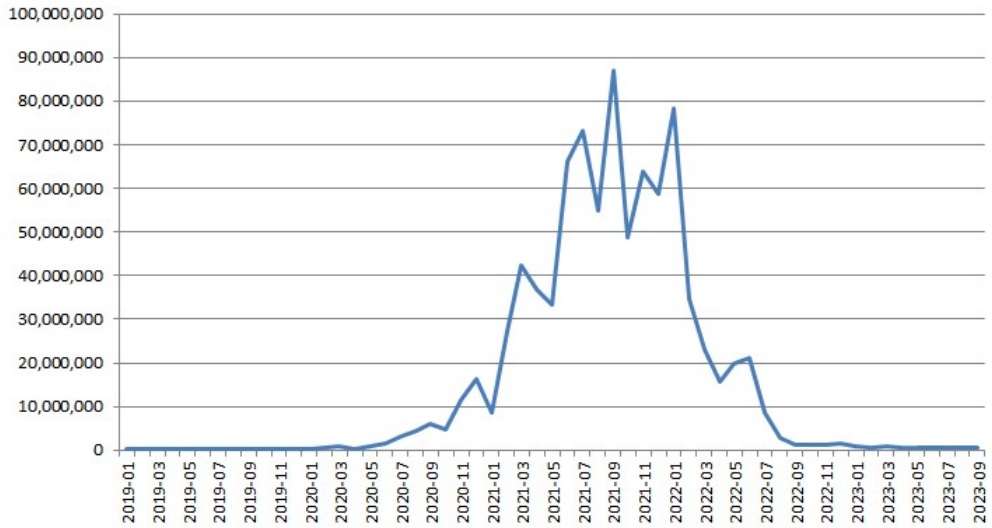
It is unclear how "pay to display" dynamics in the robocall labeling industry will ultimately play out. YouMail observes that calls with a green STIR/SHAKEN checkmark and display name generally have lower answer rates than calls without a green checkmark, which runs counter to the results promised by vendors charging call originators for these solutions. On the other hand, at the present time, this merely indicates the financial commitment of the marketing professionals operating highest volume telemarketing robocalls to spend to achieve their revenue goals and quotas, and their willingness to absorb an extra cost for the calls they place.

TCPA Class Actions

TCPA class action litigation can have a powerful effect on reducing unwanted robocalls. YouMail selected two recent class action settlements and the effect on calls received by Americans per month.

In 2022, DirecTV settled [15] a $17M TCPA class action lawsuit. DirecTV's robocalls per month reached a peak of an estimated 87 million calls received in the US in September 2021. This data does not necessarily reflect which calls were subject to the TCPA actions in the assorted TCPA lawsuits filed against DirecTV, but provide YouMail's estimate of DirecTV robocalls per month over time where the surge in calls accounted for approximately 858 million total calls.

YouMail Estimated DIRECTV Calls Per Month (V1.0)

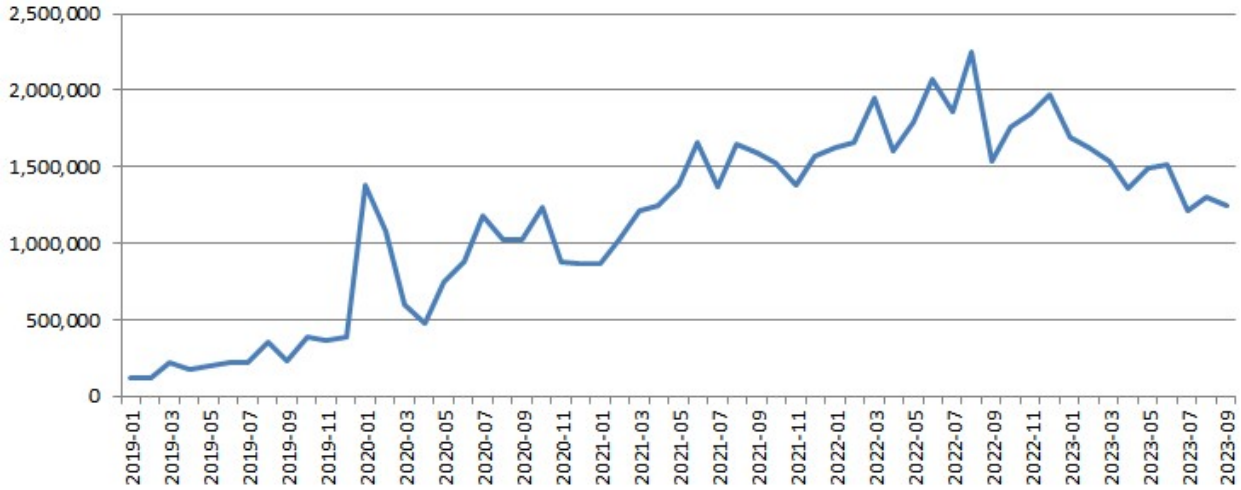


[15] https://topclassactions.com/lawsuit-settlements/closed-settlements/directv-unsolicited-calls-17m-class-action-settlement/

As can be seen, the class action litigation has reduced DirecTV robocalls by over 99%, which from its total volume has had a material impact in the total robocalls received by the public.

Also in 2022, National Grid settled [16] a $38.5M TCPA class action lawsuit. National Grid robocalls reached a peak of 2 million monthly calls by mid-2022, increasing 1500% from their pre-surge monthly volumes of ~150,000 per month.

YouMail Estimated National Grid Calls Per Month (V1.0)



YouMail only analyzed and modeled calls identifying as National Grid or referencing ngrid.com and did not include calls identifying as other entities from the class action suit (KeySpan Gas Corp, Brooklyn Union Gas Co, Niagra Mohawk Power Corp, Boston Gas Co, Colonial Gas Co, Massachusetts Electric Co, Nantucket Electric Co, Narragansett Electric Co). It is entirely possible that the robocall operation distributed call volume into different campaigns that no longer identified directly as National Grid at a point in time.

Based on YouMail estimates and models, the TCPA class action litigation appears to have caused a 45% reduction in monthly robocalls directly identifying at National Grid.

State & Federal Enforcement Actions & Coordination

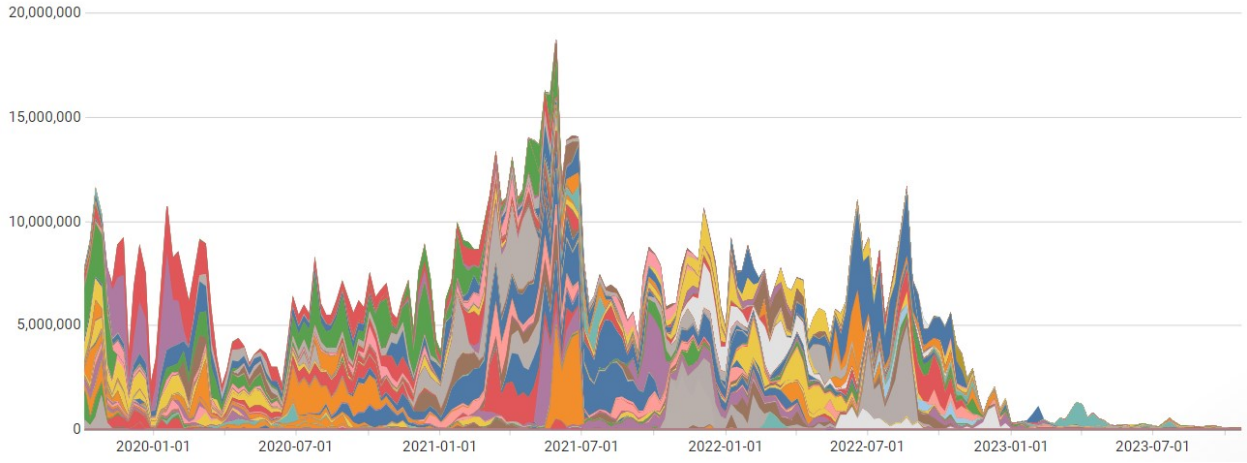
YouMail works closely with partners in state and federal enforcement agencies to model, track, investigate, provide, and analyze evidence of unlawful robocall campaigns. These efforts are largely concentrated on a campaign topic – robocalls that consumers recognize as carrying specific messaging to induce certain actions from them such as to purchase a vehicle warranty contract or to obtain loan

[16] https://topclassactions.com/lawsuit-settlements/closed-settlements/national-grid-pre-recorded-phone-calls-38-5m-class-action-settlement/

assistance services. As consumer complaint data collected at a state or federal level indicate specific areas of problematic robocalls, YouMail's ability to isolate the robocall campaigns from other communications enables real-time tracking, investigation, and enforcement action.

Student Loan Campaigns

In 2022, concerted efforts by state and federal enforcement, in partnership with YouMail have effected a dramatic reduction in robocalls carrying student loan related campaigns. YouMail has modeled and tracked 234 distinct robocall campaigns related to student loans over the past 3 years and recent work to curb these robocall campaigns has resulted in a massive decrease in these calls received by consumers. YouMail attributes the December 8, 2022, FCC order [17] to all US-based carriers as the definitive signal to industry to no longer allow such robocalls in the network. After being made aware of this order, YouMail noted that many providers who had previously tolerated such calls began to adopt non-tolerance stances.



Weekly Estimated Student Loan Robocalls

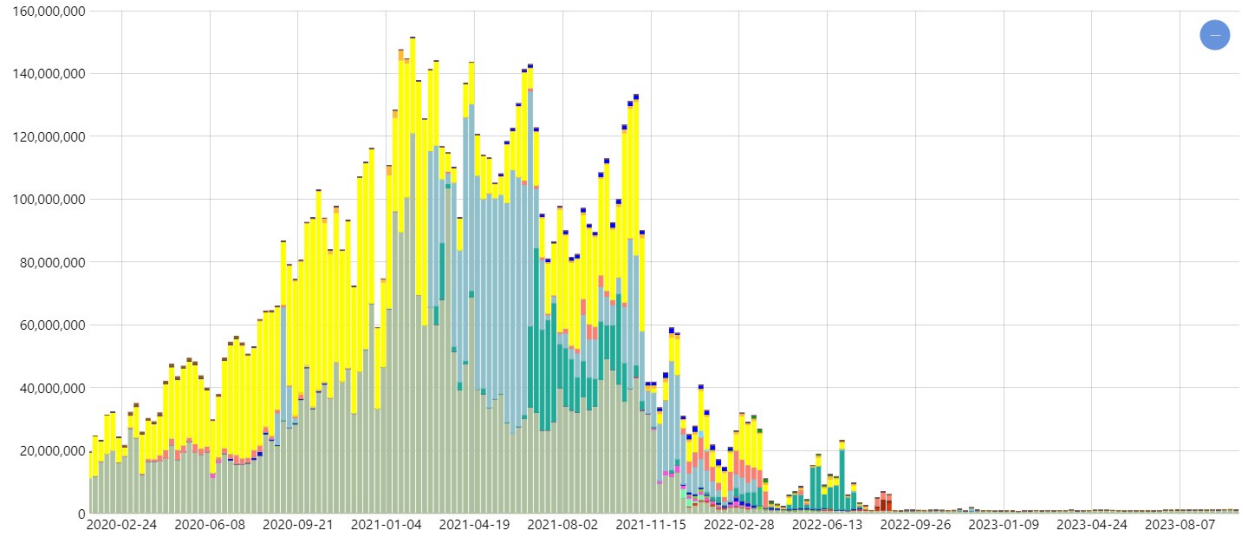
YouMail does believe that many of these robocall operations have shifted from advertising as 'student loan' support to advertising their services as 'debt reduction', 'government grant' or other similar financial assistance offers in order to evade the FCC order restricting student loan robocalls. In this manner, providers cooperating with grey-area telemarketing operations providing underlying services have complied with the "no student loan robocalls" order by shifting their offering to "general loan" services. Further efforts to curb all loan and debt-related robocalls would be necessary to observe an overall reduction in total robocalls received by the public from these operations.

[17] https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls

Auto Warranty Campaigns

YouMail estimates auto warranty robocalls peaked at 150M weekly calls. Joint efforts by state and federal enforcement from late 2021 through 2022 have effectively eliminated the auto warranty robocalls with a 99% reduction to weekly auto warranty robocalls. At present, the small number of remaining auto warranty calls in the ecosystem,which are so small relative to the period of 2020-2022 in the graph they are only a few pixels tall on the graph, appear to be lawful, legal calls.

The final blows to these calls were delivered by the FCC on July 21, 2022, with an order [18] to all US providers to avoid or cease carriage of auto warranty robocall traffic.



Weekly Estimated Auto Warranty Robocalls

Traceback & Transparency

On September 29, 2023, the FCC released a Traceback Transparency report [19]that detailed 844 tracebacks (1,043 tracebacks records, IDs 12808-13882) from the period of April 1, 2023, through June 30, 2023.

The 844 tracebacks were grouped in campaigns from 21 campaign topics tracked by YouMail. These campaign topics were: Amazon Imposter, Authorized Order, Auto Warranty, Customs & Border Patrol Imposter, Camp Lejeune Solicitation, Financial Services Imposter, Package Delivery Imposter, Debt Reduction/Elimination, Financial Hardship, Healthcare Assistance, Home Services, CSP Imposter, Loan Approval, Medicare Offer, Mortgage Assistance, Disability Assistance, Contest/Sweepstakes, SSA Imposter, Student Loan Assistance, Tax/Debt Relief, Utility Imposter.

[18] https://www.fcc.gov/document/robocall-enforcement-order-all-us-based-voice-service-providers
[19] https://docs.fcc.gov/public/attachments/DOC-397295A1.pdf

US Originating Providers (ORG)	61
Non-US Originating Provider (IOR)	14
Point-of-Entry Providers (POE)	51
Non-Responsive Providers (NR)	59
TOTAL Distinct Providers	174

Of the 174 unique providers receiving the 844 tracebacks, there was an average of 4.87 per quarter per provider , or 1.6 per month per provider.

In many cases, multiple tracebacks within the same day reached the same provider. If we recognize this as a "daily provider traceback incident" covering multiple tracebacks within the same day, there were 371 "daily provider traceback incidents" in the 3-month span across the 174 providers. The average provider received 2.1 "daily provider traceback incidents" in the period, or just 0.7 "daily provider traceback incidents" per month.

A provider receiving just a single "daily provider traceback incident" (1 per month) would be higher than the average provider (0.7 per month).

YouMail is often asked in industry discussions to reflect on how many tracebacks in a period are too many? This report is the first such report in which these types of averages can be calculated per provider, day, or campaign, which can enable any analyst engaged by a voice provider to measure relative concern when receiving a traceback.

Based on this now-public data, YouMail encourages providers to take even 1 isolated traceback as a serious matter to apply investigative resources to find all eliminate all present substantially similar traffic, while also implementing preventative controls to disallow new account creations that will bring back the same traffic under a new name. However, it is important to realize that every hour spent by a provider investigating beyond the minimum increases costs and decreases revenue, so the teams at these providers tasked with this responsibility are often at odds to the rest of their organization seeking to minimize costs and maximize revenue.

<u>One Shutdown Equals Dozens of Sales & Revenue Opportunities</u>

Voice service providers have tremendous freedom in how they react to becoming aware of unlawful traffic traversing their network. Some may shut down just a single account as their "responsible action" because that is all the evidence indicated to them was problematic. Providers currently employing policies of quickly shutting down a single account without an extensive investigation not only save expenses on investigating the traffic, but they also retain revenue by turning a blind eye to other accounts carrying similar traffic. In not introducing extra steps and friction into their new account onboarding process, they maximize the conversion rates and success of onboarding new, incoming revenue.

If a provider with effective investigative processes and strong controls succeeds in exterminating these accounts, while industry operates without an advisory to not enable the actor (such as the ones that industry received regarding auto warranty and student loan robocalls), the robocall bad actors have

learned that they should use the services of multiple voice providers in order to have back-up routes to deliver their traffic and often contact dozens of voice providers over the next week to re-establish their operations. Thus, one decisive action by a thorough provider creates a sales opportunity for dozens of their less careful competitors, especially when those dozens do not employ strict requirements to verify the customer or their traffic, or obey similar no-tolerance policies before and after onboarding new accounts.

YouMail Direct Disruptions

Using intelligence and evidence from its own proprietary data sources, YouMail Protective Services conducts direct disruptions of illegal communication campaigns at cooperating communication service providers. These communications disruptions include voice calls, SMS, MMS, RCS and iMessage channels.

For the period of June 2023 to September 2023, YouMail Protective Services disrupted 2,366 non-voice messaging vectors, enabling illegal imposter communications over SMS, MMS, RCS and iMessage channels.

June 2023	700
July 2023	674
August 2023	603
September 2023	389

YouMail is expanding these capabilities, working jointly with enterprises in communications, finance, retail and hospitality, as well as trade associations, with the goal that once the illegal campaigns have been modeled and confirmed by the impersonated enterprise, they can be shut down at cooperating enabling communications platforms within their first minutes to first hour of operation.

VII. Concluding Remarks

My testimony reflects a brief assessment of industry relative to the current state of robocalls, robotexts, omni-channel marketing platforms used by telemarketers and threat actors, potential impacts of generative AI, and the successes and challenges in industry compliance and enforcement.

Significant enforcement progress has been made through federal and state efforts, and I am proud that YouMail and its team have played an important role in some of the most notable successes, particularly when the crosshairs have been trained on specific unlawful robo-communication operations (robocalls, robotexts, and robo-messages on private platforms).

Communications have evolved significantly over the past decade, and businesses and individuals communicate through more channels and mediums than ever before in human history. As generative AI finally brings a robot, indistinguishable from a human to robo-communications, the public has never been at greater risk.

I urge Congress, as well as state and federal agencies, to recognize that the digitalization of society, along with automation of and ease of accessibility to communication platforms, could very well mean that US citizens are now at greater risk of harm sourced digitally than by physical threat. Agencies should strongly consider expanding their budgeted resources to increase investigative and enforcement capabilities, while simultaneously considering new policies to address bad early adoption threat actors, capitalizing on next-generation robo-communication tools.

Thank you for your time today. I am happy to answer any questions.

Respectfully submitted,

Michael Rudolph
Chief Technology Officer
YouMail, Inc.
October 24, 2023