HOSPITAL ROBOCALL PROTECTION GROUP (HRPG)

CONTENTS

I. EXECUTIVE SUMMARY

Hospitals receive fraudulent, disruptive and nuisance robocalls that flood their communications networks. While similar to unlawful robocalls received by consumers generally, the significant difference with hospital-related robocalls is the impact these calls can have on public health and safety to patients and the community. Hospitals can fall victim to a variety of unlawful calling schemes, ranging from telephone denial-of-service attacks to targeted social engineering to phishing and vishing schemes to more general unlawful robocall campaigns that happen to reach hospital numbers. These and other malicious calling activities can disrupt hospitals' critical communications and render hospitals unable to place or receive telephone calls, threaten patients' privacy, facilitate unauthorized access to prescription drugs, and divert hospital resources.

In response to the problem of unlawful robocalls, Congress passed the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, or TRACED Act, in December 2019. The TRACED Act in turn directed the Federal Communications Commission to establish a Hospital Robocall Protection Group (HRPG), a Federal Advisory Committee that the FCC established in June 2020.

The communications industry has taken proactive steps to stop unlawful robocalls, resulting in billions of unlawful and unwanted calls blocked each year. Hospitals too can take preventative steps to protect their infrastructure and personnel. Federal and State enforcement agencies have taken numerous actions to go after those responsible for unlawful robocalls as well. However, efforts by any single entity or group will not prevent robocalls to hospitals. Therefore, collective efforts and coordination between hospitals, government agencies, and voice service providers are critical to the success of unlawful robocall prevention and mitigation efforts. To that end, and consistent with the requirements of the TRACED Act, this report provides the best practices recommendations developed within the HRPG's three working groups on how voice service providers, hospitals, and Federal and State government agencies can take action together to combat unlawful robocalls made to hospitals. The recommendations for each group are divided into two sections: (1) prevention and (2) response and mitigation.

Voice service providers. To better combat unlawful robocalls made to hospitals, voice service providers serving hospitals should engage in the following:

Prevention

- Implement STIR/SHAKEN on the IP portions of their networks
- Have appropriate procedures in place to ensure compliance with applicable laws
- Confirm the identity of and properly vet their customers
- Analyze, identify, and monitor traffic on their network for patterns consistent with unlawful robocalls
- Offer call blocking and call labeling services
- Provide materials and opportunities for education and guidance to hospitals

Response and Mitigation

- Prioritize hospital entities as appropriate in response and remediation efforts
- Establish a method to ensure hospitals can expeditiously notify the provider about unlawful robocalls that interfere with patient care and hospital operations
- Initiate tracebacks as appropriate

Hospitals. To better protect themselves from unlawful robocalls, hospitals should:

Prevention

- Engage in education and raise awareness regarding robocall incidents, including through staff training and preparing robocall incident response plans
- Explore available robocall blocking and labeling capabilities offered by voice service providers
- Manage telephone number resources, including by reporting spoofing of the hospital's numbers and isolating critical phone lines

Response and Mitigation

- Evaluate a given robocall event and capture relevant information about the calling activity
- Contact internal engineers or technicians to implement immediate configuration changes and safeguards within premises-based equipment after an incident
- Coordinate with federal and state agencies as appropriate

Federal and State Governments. Government agencies should continue to expand their efforts to prevent robocalls from reaching hospitals and other end users, and specifically should:

Prevention

- Create and implement balanced policies that facilitate industry's ability to prevent unlawful robocalls from reaching hospitals
- Enforce existing laws, rules, and policies against voice service providers that originate unlawful robocalls as well as those that fail to take sufficient steps to mitigate the transmission of such calls
- Develop clear and concise hospital education materials

Response and Mitigation

- Improve communication methods between hospitals and law enforcement agencies, and establish information sharing methods across all relevant enforcement agencies
- Actively monitor complaints from hospitals and engage in prompt outreach to providers and agencies who can assist in response
- Make prioritized referrals to the Industry Traceback Group and coordinate traceback response among law enforcement partners

II. INTRODUCTION AND BACKGROUND

A. Establishment of HRPG

In December 2019, Congress passed the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, or TRACED Act, to further empower industry and government agencies in the fight against unlawful robocalls.[1] In recognition of some of the unique risks posed by unlawful robocalls to hospitals, the TRACED Act directed the Federal Communications Commission (FCC) to establish a Hospital Robocall Protection Group (HRPG),[2] which the agency announced in March 2020.[3]

The HRPG's objective is to serve as a resource to all stakeholders involved in preventing the receipt of unlawful robocalls by hospitals and patients and mitigating their effect. Included in this report is background information on the different types of unlawful robocalls that hospitals may receive and the numerous ongoing efforts by industry and government to address such calls.[4] The best practice recommendations are arranged to cover voice service providers, hospitals, and Federal and State governments. The best practice recommendations are further separated into two broad categories (1) Prevention and (2) Response & Mitigation.

B. Structure of HRPG

1. 14(b) Membership Structure

As required by Section 14(b) of the TRACED Act, the HRPG consists of an equal number from the following categories:

- Voice service providers that serve hospitals.
- Companies that focus on mitigating unlawful robocalls.
- Consumer advocacy organizations.
- Providers of one-way voice over internet protocol services described in subsection (e)(3)(B)(ii) of the TRACED Act.

---

[1] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. 116-105, 133 Stat. 3274 (2019) (TRACED Act).

[2] TRACED Act § 14(a).

[3] *FCC Announces the Establishment of the Hospital Robocall Protection Group and Seeks Nominations for Membership*, DA 20-333, Public Notice, 35 FCC Rcd 2895 (CGB 2020).

[4] A "robocall" generally refers to "calls made with an autodialer or that contain a message made with a prerecorded or artificial voice." FCC, Stop Unwanted Robocalls and Texts, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited Nov. 18, 2020). This report addresses such autodialed robocalls, but also discusses other types of unlawful and harassing calls made to hospitals by individuals, such as phishing calls targeting an individual hospital employee. For purposes of this report, the term "robocall" refers broadly to any unlawful calls placed to hospitals or patients.

- Hospitals.
- State government officials focused on combating unlawful robocalls. [5]

Section 14(b) also required the HRPG to include:

- One representative of the Federal Communications Commission.
- One representative of the Federal Trade Commission.[6]

2. Section 14(c) Best Practices

In Section 14(c) of the TRACED Act, Congress directed that the HRPG issue best practices regarding:

- How voice service providers can better combat unlawful robocalls made to hospitals.
- How hospitals can better protect themselves from such calls, including by using unlawful robocall mitigation techniques.
- How the Federal Government and State governments can help combat such calls.

The HRPG held its first meeting on July 27, 2020. Three working groups were formed to make recommendations for voice service providers, hospitals and government agencies. [7]

C. The Impact of Robocalls on Hospitals

Hospitals receive fraudulent, disruptive and nuisance robocalls flooding communication networks and annoying calls to patient rooms. While similar to unlawful robocalls received by consumers generally and other organizations, the significant difference with hospital-related robocalls is the impact these calls can have on public health and safety to patients and the community due to the possible disruption of patient care services. For example, a robocall attack disrupted all communication on a Rhode Island-based healthcare company's five lines for 30 consecutive minutes in 2017; one hospital received more than 4,500 robocalls in just two hours in 2018; another hospital had 6,500 calls spoofed to look like internal calls tying up approximately 65 hours of response time of hospital employees over 90 days; and that same hospital also experienced about 300 robocalls spoofing numbers affiliated with the Department of Justice seeking to extract sensitive information from hospital physicians.[8]

---

[5] TRACED Act § 14(b).

[6] *Id.* A full list of HRPG members is available in Appendix A.

[7] TRACED Act § 14(c).

[8] *See* Nick Wingfield, *Swindlers Use Telephones, With Internet's Tactics*, N.Y. Times (Jan. 20, 2014), https://www.nytimes.com/2014/01/20/technology/swindlers-use-telephones-with-internets-tactics.html; FCC, *Caller ID Spoofing*, (last updated Sept. 23, 2020), https://www.fcc.gov/consumers/guides/spoofing-and-caller-id; *Legislating to Stop the Onslaught of Annoying Robocalls: Hearing Before the Subcommittee on Communications and Technology of the H.*

Hospitals and medical professionals also are subject to sophisticated phishing schemes, often for unlawful drug activities. For instance, fraudsters have contacted medical and pharmacy professionals pretending to be a state's Board of Medicine or Board of Pharmacy, or even the FBI, to extract information or financial resources.[9] Robocalls and other malicious calling activity can disrupt hospitals' critical communications and render hospitals unable to place or receive telephone calls, threaten patients' privacy, facilitate unauthorized access to prescription drugs, and divert resources that otherwise would be devoted to quality care and improving patient outcomes. Robocallers also routinely trade on hospitals' names and reputations—and their phone numbers through unlawful spoofing—in order to scam consumers, resulting in even more calls to the hospitals from those confused consumers.

Hospitals can take many preventative steps to protect their infrastructure and personnel, working with service providers, which can be achieved through effective policies, procedures, technology, and education. Despite the preventative steps outlined in this report for hospitals, fraudulent actors will inevitably be able to circumvent these protections in some instances. It is therefore vital that hospitals have a plan to respond to an active robocall event in collaboration with their voice service providers and, in some cases, appropriate government agencies, to mitigate the impact of such calls.

There are several distinct types of unlawful calls that can impact hospitals and patients. The appropriate response to such calls will be different depending on the type of call(s) involved as discussed in the recommendations below.

Types of unlawful robocalls include:

- **Telephone denial-of-service attack (TDoS).** A TDoS attack is an intentional attack to disrupt the telephony/voice service communications of an organization by flooding the network with multiple simultaneous calls. A TDoS may involve caller ID spoofing. A TDoS attack against a hospital could be conducted for extortion or other nefarious purposes such as attempts to obtain personal identifiable information, extort money, harass, or for some other economic gain. The goal of the attacker may simply be disruption, but it is more common that it is an extortion attempt where the attacker demands a ransom to stop the attack. A TDoS attack usually involves spoofing the calling number frequently enough to make the calls difficult to differentiate from legitimate calls. The target could be patient rooms, but more often is a key phone number needed to serve the

---

Comm. on Energy and Commerce, 116th Cong. 12 (2019) (statement of Dave Summitt, Chief Information Security Officer, H. Lee Moffitt Cancer Center & Research Institute).

[9] Off. of the Private Sector, Federal Bureau of Investigation, *Criminals Pose as Law Enforcement and Medical Boards as Part of Mass Marketing Fraud Schemes to Target Medical Providers for Financial Gain*, Liaison Information Report, LIR 201013-007 (Oct. 13, 2020), https://providers.beaumont.org/docs/default-source/pdfs-for-bpp-bulletin/lir_criminals_posing_law_enforcement_medical_boards.pdf?sfvrsn=441f5eec_2 .

public, such as for the Emergency Room or Intensive Care Unit (ICU). The victim of TDoS is normally the hospital, but may be personnel or patients.[10]

- **Targeted social engineering calls.** Social engineering calls, though less frequent than general unlawful or nuisance robocalls, are potentially damaging calls designed to steal information. The goal is to gather sensitive, financial, or information technology (IT) information. The goal may also be to steal some bit of information to be used in a larger data attack. For instance, social engineering calls may seek information about the hospital organization, names and phone numbers of key personnel, email addresses, and information about computer systems, among other data. These calls are very difficult to detect and usually go unreported. The victim of targeted social engineering calls is the hospital.
- **Phishing also known as vishing.**[11] Bad actors may use social engineering techniques to try to steal information and credentials from hospital workers in order to, for example, obtain prescription drugs fraudulently. Such attacks tend to be targeted—including sophisticated attacks targeting individual staff members—and rely on caller ID spoofing to hide the caller's identity in favor of impersonating a more trusted one. The victim of targeted phishing/vishing calls is the hospital.
- **Hospital impersonation.** Consumers regularly receive calls attempting to impersonate some individual or organization, such as the Social Security Administration (SSA), a medical equipment company, an insurance company, or another part of the hospital system. These calls attempt to steal personal information or actual funds, and include hospital-specific impersonation scams where a patient is called and tricked or coerced into giving up personal and financial information. In such a scam, a hospital telephone's number could be spoofed. Hospital impersonation campaigns often intend to defraud current and former patients of the hospital through billing and collection schemes, requests for donations, or the request for personally identifiable information to be used in subsequent identity theft-related frauds. Although these calls do not directly target the hospital, they can lead to recipients contacting the hospital about calls the hospital never made, and expose the hospital to potential negative publicity, regulatory scrutiny and reputational harm. The victim of impersonation scams is the patient and/or hospital personnel.
- **General unlawful robocall campaigns.** General unlawful robocall campaigns rely on automatic dialing to blast mass numbers of prerecorded scam calls to as many potential victims as possible. The calls, which frequently originate from

[10] Several years ago, the "payday loan scam" was common against hospitals. The scam involved a threat against a hospital staff member, accusing the person of owing debt on a loan, with the place of business being flooded with calls until they pay.

[11] Brian Krebs, *FBI, CISA Echo Warnings on "Vishing" Threat* (Aug. 21, 2020), https://krebsonsecurity.com/2020/08/fbi-cisa-echo-warnings-on-vishing-threat/.

outside the United States, often seek to defraud recipients by, for example, claiming to be from a government agency or legitimate business and suggest that the recipient must take some immediate action to avoid a financial penalty or to be eligible for a benefit. In addition to being fraudulent, such calls also very often violate various criminal laws governing calling parties, such as the federal Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act, the Federal Trade Commission's (FTC) Telemarketing Sales Rule (TSR), and similar state laws. While general unlawful robocalls may not specifically target hospitals, they can tie up hospital lines and resources. In addition, patients and staff at hospitals, like any other recipient of the call, can fall victim of robocall scams.

- **Nuisance and disruptive robocalls.** Some robocalls are placed to consumers who wish to receive them (medical appointment reminders, fraud alerts from banks, etc.). Many calls are also made to consumers attempting to sell some product, service, or information. With appropriate consent, as governed by relevant federal and state laws, such calls may not be unlawful, but they are very often unwanted. These calls can irritate patients and reduce hospital personnel productivity and can consume hospital voice system resources. Nuisance robocalls are starting to become more common in hospitals, as they are a lucrative target. The victim of nuisance robocalls is the patient/hospital personnel.[12]

D. Industry Efforts to Stop Unlawful Robocalls

The communications industry has taken proactive steps to stop unlawful robocalls. Voice service providers are increasingly monitoring and analyzing their traffic to look for evidence of suspicious activity that may suggest unlawful calling patterns and taking action to address unlawful traffic activity when discovered. Voice service providers and third-party analytics companies offer customers a variety of powerful options for call blocking and labeling. Most large voice service providers offer default blocking to block apparently fraudulent calls and many providers also offer additional blocking and labeling options to their subscribers.[13]

[12] If enough nuisance or other calls are received, even if the intention is not to disrupt the hospital, a TDoS event can occur. For example, if the same number or a small group of numbers is called continuously, and that number is important for patient or a hospital function, legitimate use of that number or numbers may not be possible. Because inadvertent TDoS is not intentional, the attack is usually not long lasting or persistent. The victim of inadvertent TDoS is the hospital.

[13] FCC, Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking at 12, para. 25 (2020), https://docs.fcc.gov/public/attachments/DOC-365152A1.pdf. Third-party analytics companies and device manufacturers also offer additional services. *Id.*

These services collectively block billions of unlawful and unwanted calls to American consumers each year.[14]

In addition, voice service providers have been actively deploying the STIR/SHAKEN caller ID authentication framework.[15] By the end of 2019, AT&T, Bandwidth, Charter, Comcast, Cox, T-Mobile, and Verizon announced that they had upgraded their networks to support STIR/SHAKEN, and several others had performed necessary network upgrades and were in the process of negotiating and testing the exchange of authenticated traffic with other voice service providers.[16] Since that time, these and other providers are even further along in their deployments.[17]

As of November 11, 2020, the Secure Telephone Identity Policy Administrator has approved 57 service providers to start using the industry process to receive certificates and exchange STIR/SHAKEN enabled traffic.[18]

Voice service providers, through USTelecom's Industry Traceback Group (ITG), also conduct tracebacks of unlawful robocalls.[19] A traceback is a process to trace a suspected unlawful robocall to its source, even if the calling number is spoofed. For tracing back a call that traverses multiple providers' networks, the process begins with the voice service provider that terminated the suspected unlawful robocall, and then the call is systematically traced back chronologically from provider to provider. When the ITG process identifies the originator of suspicious robocalls, or a U.S. Point of Entry routinely responsible for bringing unlawful traffic into the United States, USTelecom's ITG traceback team seeks to work with providers to mitigate the unlawful traffic, such as stopping the traffic and enhancing robocall mitigation measures going forward. When that traffic goes unmitigated, USTelecom may provide

---

[14] *Id.* at 25, para. 57. Voice service providers and analytics companies provide contact information for parties to report to them incorrectly identified calls. *See Id.* at 29, para. 66.

[15] The STIR/SHAKEN framework includes several different standards and protocols. STIR stands for Secure Telephony Identity Revisited and SHAKEN stands for the Signature-based Handling of Asserted Information using toKENs. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, FCC 20-136 at 4-5, para. 7 (Oct. 1, 2020) (*STIR/SHAKEN Second Report and Order*). STIR/SHAKEN digitally validates the handoff of phone calls passing through a complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID. *Id.* at 3, para. 3

[16] *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a)-Knowledge of Customers by Entities with Access to Numbering Resources,* WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3249, para. 18 (2020) (*Call Authentication Trust Anchor*).

[17] *See STIR/Shaken Second Report and Order* at 8, para. 15.

[18] *See* iconnecitve,https://authenticate.iconectiv.com/authorized-service-providers-authenticate (last visited Nov. 11, 2020).

[19] USTelecom, *The USTelecom Industry Traceback Group (ITG)*, https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg (last visited Nov. 11, 2020).

information to downstream carriers, as well as appropriate enforcement agencies, about the source of the unlawful traffic.[20] The ITG currently conducts approximately 250 tracebacks per month, focusing on the highest volume unlawful robocall campaigns (a single traceback can be representative of millions of calls being made by a single party) and high-impact calls (i.e. calls that may not be high volume but are responsible for serious and ongoing fraud, such as an apparent TDoS attack).

Case Study: Stopping a Hospital TDoS Attack in Real Time

In October 2020, the industry successfully worked with a hospital to stop a TDoS attack targeting the hospital, possibly for cyber extortion. On October 15, a major metropolitan hospital's emergency department first started receiving robocalls at a high rate, which overloaded the hospital's emergency telephone lines. After unsuccessful attempts to stop the unwanted calls on its phone system, the hospital contacted the AT&T GFMO (Global Fraud Management Organization), and the calls were stopped the next day. When the hospital started to receive the robocalls, now on an additional number, again less than a week later, it contacted AT&T right away. Aggressive industry action stopped the calls that same day.

The initial calls to the emergency lines had displayed invalid numbers, spoofed numbers or no number. When those calls were answered, the caller asked for a person that was supposed to be an employee, but the name provided was not a current or past employee. The caller then demanded gift cards, before launching the attack. Because the numbers were spoofed, merely blocking the numbers in the hospital's phone system was insufficient to halt the attack – the attacker simply changed to a new spoofed number. The AT&T team, in contrast, was able to rapidly identify the upstream carrier and get the carrier to cease sending the traffic. In addition, the ITG initiated tracebacks for both of the TDoS attacks, identifying the source of the attacks as a company in India. The Indian company has since been blocked by the providers that took its traffic, and a case referral to the FBI is underway.

In addition to these provider-driven efforts, voice service providers across the industry have been actively coordinating with government agencies at the federal and state level. Such coordination is essential for government enforcement where industry is often able to provide information essential to government efforts to crack down on unlawful callers.

E. Government Regulatory and Enforcement Activity to Stop Unlawful Robocalls

Stopping unlawful robocalls is the FCC's top consumer protection priority,[21] and the FCC has taken a multi-pronged approach to do so. In recent years, the FCC has taken aggressive

[20] *See generally* USTelecom, *USTelecom's Industry Traceback Group*, Policies and Procedures (2020), https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf.

[21] FCC, *Stop Unwanted Robocalls and Texts* (last updated Nov. 18, 2020), https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.

enforcement action against unlawful robocallers,[22] authorized voice service providers to block by default unlawful and unwanted calls in several contexts,[23] mandated implementation of the STIR/SHAKEN caller ID authentication framework to help reduce unlawful spoofing,[24] and designated USTelecom's ITG as the single consortium registered to conduct private-led traceback efforts to identify the origins of suspected unlawful robocalls.[25] Several of the FCC's robocall-related proceedings are ongoing.

Other federal agencies also have taken important actions to stop unlawful robocalls. Earlier this year, the Department of Justice filed the first-of-their-kind enforcement actions against Voice over IP (VoIP) providers that were carrying fraudulent robocall traffic into the United States and onto the U.S. telephone network.[26] The FTC also has targeted VoIP providers responsible for unlawful robocall traffic.[27] The FTC, in conjunction with the FCC and with the support of the ITG, also sent letters to multiple VoIP companies this year for their involvement in fraudulent calls related to the coronavirus.[28] Additionally, the Department of Justice

---

[22] *See, e.g., Adrian Abramovich* Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc., Forfeiture Order, 33 FCC Rcd 4663 (2018); *John C. Spiller; Jakob A. Mears, Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group: Rising Phenix Holdings: RPG Leads; and Rising Eagle Capital Group - Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948 (2020).

[23] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017) (*2017 Call Blocking Report and Order*); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4886-88, paras. 33-34 (2019) (*2019 Call Blocking Declaratory Ruling*).

[24] *Call Authentication Trust Anchor*, 35 FCC Rcd 3241 (2020); *STIR/SHAKEN Second Report and Order*, FCC 20-136 (Oct. 1, 2020)

[25] *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 35 FCC Rcd 7886 (2020).

[26] Press Release, Dept. of Justice, The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers (Jan. 28, 2020), https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions.

[27] *See, e.g.,* Press Release, Fed. Trade Comm'n, Globex Telecom and Associates Will Pay $2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider (Sept. 22, 2020), https://www.ftc.gov/news-events/press-releases/2020/09/globex-telecom-associates-will-pay-21-million-settling-ftcs-first; Press Release, Fed. Trade Comm'n, FTC Warns 19 VoIP Service Provider That 'Assisting and Facilitating' Unlawful Telemarketing or Robocalling Is Against the Law (Jan. 30, 2020), https://www.ftc.gov/news-events/press-releases/2020/01/ftc-warns-19-voip-service-providers-assisting-facilitating; Press Release, Fed. Trade Comm'n, FTC Takes Action against Second VoIP Service Provider for Facilitating Illegal Telemarketing Robocalls (Dec. 3, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-takes-action-against-second-voip-service-provider.

[28] Press Release, Fed. Trade Comm'n, FTC Warns Nine VoIP Service Providers and Other Companies against 'Assisting and Facilitating' Unlawful Coronavirus-related Telemarketing Calls (Mar. 27, 2020),

investigates and prosecutes a variety of crimes which may be related either directly or indirectly to robocall schemes, including cyber- crimes.[29]

States also have been active, both by working with industry on robocall mitigation and by bringing enforcement actions against bad actors. Fifteen voice service providers joined all fifty-one State Attorneys General (AGs) in developing and committing to eight anti-robocall principles, including implementing call authentication, analyzing and monitoring network traffic, and investigating suspicious calls and calling platforms, among others.[30] State enforcement actions have targeted both robocallers and voice service providers that unlawfully allow unlawful robocalls to traverse their networks.[31] The Ohio AG joined the FTC in its case against a VoIP provider routing unlawful robocalls,[32] and eight states recently sued a robocaller out of Texas that allegedly generated over a billion robocalls to consumers across the country.[33]

All of the actions taken above by voice service providers and government agencies to

---

https://www.ftc.gov/news-events/press-releases/2020/03/ftc-warns-nine-voip-service-providers-other-companies-against; Press Release, Fed. Trade Comm'n, FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Unlawful Coronavirus-related Robocalls (May 20, 2020), https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning.

[29] Press Release, Dept. of Justice, Five Defendants Arrested and Indicted for India-Based Telemarketing And Email Marketing Scheme Victimizing Seniors Throughout The United States (Dec. 18, 2019), https://www.justice.gov/usao-nv/pr/five-defendants-arrested-and-indicted-india-based-telemarketing-and-email-marketing.

[30] *See State Attorney Generals-Providers Anti-Robocall Principles*, https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf (last visited Nov. 11, 2020) (*Anti-Robocall Principles)*.

[31] *See, e.g.,* Press Release, Michigan Dept. of Att'y Gen., *AG Nessel Announces Significant Settlement with Telecom Carrier Focused on Innovative Robocall Mitigation Measures* (Sept. 11, 2020), https://www.michigan.gov/ag/0,4534,7-359-92297_99936-539389--,00.html; Press Release, Michigan Dept. of Att'y Gen., *AG Nessel Announces Settlement Eliminating Telecom Carrier Responsible for Unlawful Robocalls* (Aug. 7, 2020) https://www.michigan.gov/ag/0,4534,7-359--536108--s,00.html; Press Release, Ohio Att'y Gen., *Ohio Attorney General Dave Yost Announces Settlement in Groundbreaking Lawsuit Against Unlawful Robocall Service* (Sept. 29, 2020), https://www.ohioattorneygeneral.gov/Media/News-Releases/September-2020-(1)/Ohio-Attorney-General-Dave-Yost-Announces-Settleme; *States of Arkansas, Indiana, Michigan, Missouri, North Carolina, Ohio, and Texas v. Rising Eagle Capital Group LLC et al.*, No. 4:20-cv-02021 (Tex. S.D. June 9, 2020) (complaint).

[32] *FTC v. Educare Ctr. Servs., Inc.*, No. EP-19-CV-196-KC, 2019 WL 5415836 (W.D. Tex. Oct. 22, 2019); Press Release, Ohio Att'y Gen., *Ohio Attorney General Dave Yost Announces Settlement in Groundbreaking Lawsuit Against Unlawful Robocall Service* (Sept. 29, 2020), https://www.ohioattorneygeneral.gov/Media/News-Releases/September-2020-(1)/Ohio-Attorney-General-Dave-Yost-Announces-Settleme.

[33] *Texas et al. v. Rising Eagle Capital Group LLC*, No. 4:20-cv-02021 (S.D. Tex. 2020).

prevent unlawful robocalling will benefit hospitals. Thus, in addition to identifying recommendations unique to hospitals, particularly those things hospitals can do themselves, a key focus in these recommendations is to ensure that hospitals are aware of the relevant ongoing activities outside of their control and can take advantage of them where appropriate and in a timely fashion. It is important to recognize that while hospital coordination with government agencies and voice service providers to address robocall incidents is of critical importance, voice service providers and government agencies cannot prevent all robocalls. All stakeholders must work together in a coordinated manner, prioritizing resources consistent with the recommendations below, to effectively prevent and mitigate the impact of unlawful robocalls.

III. RECOMMENDED BEST PRACTICES

Billions of robocalls are placed every month to American consumers, a substantial portion of which are unlawful.[34] As described above, many unlawful robocalls directly target hospitals and hospital patients. Therefore, while it is inevitable that some unlawful calls will get through, it is essential that voice service providers, hospitals, and federal and state government agencies take preventative steps to reduce the number of unlawful robocalls received by hospitals.

Despite preventative efforts by all stakeholders, unlawful robocalls will get through to hospitals and patients. Therefore, it is essential that voice service providers, hospitals, and federal and state government agencies are prepared to rapidly respond to active robocall events and to consider longer-term remediation efforts post-event. Consistent with section 14(c) of the TRACED Act, below are recommended best practices to respond to and remediate unlawful robocalls to hospitals.

A. How Voice Service Providers Can Better Combat Unlawful Robocalls Made to Hospitals

1. Prevention

The following are prevention techniques that voice service providers can engage in to combat unlawful robocalls made to hospitals.

- **Implement STIR/SHAKEN**. All voice service providers providing hospitals with wireline, wireless, or VoIP telephony ("Voice Services") should implement the STIR/SHAKEN authentication framework on the IP portions of their networks.[35]
- **Engage in Compliance**. All voice service providers providing hospitals with Voice Services should have appropriate procedures in place to ensure compliance with applicable laws.

---

[34] *See* Nathan Bomey, Robocall *"Crackdown": FTC Blocks More Than a Billion Unlawful Calls, but the Problem Festers*, USA Today (Jun. 25, 2019 12:38 PM EDT), https://www.usatoday.com/story/money/2019/06/25/ftc-robocall-crackdown/1548714001/.

[35] *See Anti-Robocall Principles, supra* note 30, Principle #2.

- **Confirm Customer Identity.** All voice service providers providing hospitals with Voice Services should follow the North American Numbering Council Call Authentication Trust Anchor Working Group recommendations, titled "Best Practices for the Implementation of Call Authentication Frameworks," with respect to the vetting of subscribers and/or customers.[36]

- **Analyze, Identify, and Monitor Network Traffic.** All voice service providers providing hospitals with Voice Services should follow the North American Numbering Council Call Authentication Trust Anchor Working Group recommendations, titled "Best Practices for the Implementation of Call Authentication Frameworks," with respect to analyzing voice network traffic to identify and monitor patterns consistent with unlawful robocalls.[37]

- **Offer Call Blocking and Call Labeling Services.** All voice service providers providing hospitals with Voice Services should offer call blocking and call labeling services, to the extent such enterprise services are available and able to be implemented by hospitals, consistent with any relevant FCC guidance. Voice service providers should work with individual hospital entities to assist them with implementing call blocking and labeling services consistent with hospital individual needs.

- **Support Education and Guidance for Voice Services.** All voice service providers providing hospitals with Voice Services should provide hospitals access to materials and opportunities for education and guidance related to preventing the receipt of and mitigating unlawful robocalls.

2. Response and Mitigation

The following are response and mitigation techniques that voice service providers can engage in to combat unlawful robocalls made to hospitals.

- **Prioritize Hospital Entities**. Recognizing that other entities (i.e., public safety agencies) as well as the severity of a campaign's consumer impact (e.g., a campaign successfully scamming seniors of their life savings) may also require prioritization, all voice service providers providing hospitals with Voice Services should (1) prioritize hospitals in their response and remediation efforts relating to unlawful robocalls and (2) utilize methods that alleviate burdens, including, but not limited to, administrative and operational burdens, in response and

[36] NANC Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Networks* at 6-10, https://www.fcc.gov/document/best-practices-implementation-call-authentication-framework (last visited Nov. 11, 2020); *see also Anti-Robocall Principles, supra* note 30, Principles #5 and #6.

[37] NANC Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Networks* at 17, https://www.fcc.gov/document/best-practices-implementation-call-authentication-framework (last visited Nov. 11, 2020); *see also Anti-Robocall Principles, supra* note 30, Principles #3 and #4.

remediation efforts, for hospitals to the extent possible.

- **Enable Immediate Inbound Issue Notification**. All voice service providers providing hospitals with Voice Services should establish a method to ensure hospitals can expeditiously notify the voice service provider about the receipt of unlawful robocalls and other communications that interfere with the delivery of patient care and/or other hospital operations.
- **Enable Immediate Outbound Issue Notification**. All voice service providers providing hospitals with Voice Services should likewise establish a method to ensure that hospitals can expeditiously notify the voice service provider about outgoing phone calls being blocked, unauthenticated, or misidentified.
- **Initiate Tracebacks**. All voice service providers providing hospitals with Voice Services should actively cooperate with USTelecom's ITG or successor traceback consortium as mandated by the FCC and initiate traceback requests on behalf of hospital entities as appropriate.[38]

B. How Hospitals Can Better Protect Themselves From Unlawful Robocalls

1. Prevention

a. Education and Awareness

Hospital staff are likely the first to become aware of fraudulent, disruptive or nuisance robocall activity within the hospital and health systems. Training staff to identify and respond to robocall activity will reduce the impact to the patients and personnel of the hospital. The following recommendations are focused on areas for hospitals to establish education and awareness of an event to prevent harm and initiate mitigation tactics.

- **Train staff.** Train staff to identify the different types of robocalls and recognize possible unlawful calls, the nature of these attacks, and how to protect against scams. At minimum, the staff should include security, compliance, and staff members who will answer phones.
- **Gather data.** Define key data for staff to gather including the date/time of the calls, number being dialed, type of calls (recording or live person), volume of calls, CallerID displayed, and the content of the message.
- **Protect data.** Remind staff of their obligation to protect personally identifiable information (PII) and Protected Health Information (PHI).
- **Be prepared to coordinate with voice service providers and law enforcement.**
    - Establish a governance process, policies and procedures on how the hospital will work with voice service providers and law enforcement agencies.

[38] *Anti-Robocall Principles, supra* note 30, Principle #7.

- Establish a plan with your voice service provider for actions to take during and after an event. Discussions might include voice service providers as well as facility equipment vendors (i.e. the telephone system provider). Those involved should be aware that some robocall events are auto-programmed to dial a complete range (block) of numbers.
- Determine internally through legal, compliance, and executive review the willingness of the hospital to report, work with and assist federal and state law enforcement agencies in the investigation and prosecution of robocall schemes, including the acceptance of potential publicity related to the matter upon investigation and prosecution.
- Work with internal security, cybersecurity, and telecom staff to establish procedures on the identification and gathering of technical and non-technical information related to the robocalls which may be used as evidence in a subsequent criminal or civil investigation and enforcement actions.
- Identify and establish relationships with designated points of contact with appropriate representatives of federal and state law enforcement and regulatory agencies[39] and an understanding of how your hospital will cooperate.
- Require staff to report internally to the appropriate function designated to collect the robocall information.
- Have information available for patients and staff should they become a victim of a robocall scheme resulting in fraud or identity theft.[40]
- Consider joining threat intelligence and information sharing organizations which offer contacts, resources, and information sharing between private industry and government, such as the FBI sponsored InfraGard[41] program, the Health-Information Sharing and Analysis Center,[42] and the

[39] FBI, DHS-ICE-HIS, United States Secret Service, FTC, FCC, State Attorney General's Office, State Consumer Affairs Office.

[40] *See, e.g.*, Federal Trade Commission, *IdentityTheft.gov,* http://www.identifytheft.gov (last visited Dec. 11, 2020; Federal Bureau of Investigation, *Internet Crime Complaint Center IC3*, https://ic3.gov; FCC, *Stop Unwanted Robocalls and Texts,* https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited Nov. 11, 2020); Federal Bureau of Investigation, *Scams and Safety, Telemarketing Fraud*, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/telemarketing-fraud (last visited Nov. 11, 2020).

[41] *See InfraGard*, https: www.InfraGard.org (last visited Nov. 11, 2020).

[42] *See H-ISAC: Health Information Sharing and Analysis Center*, www.h-isac.org (last visited Nov. 11, 2020).

American Hospital Association.[43]

b. Mitigation Tactics and Tools

Perimeter defense and network monitoring are critical strategies to protect hospital networks from unlawful robocalls. Not unlike security perimeter defense, tools exist to identify unlawful traffic and stop it before infiltrating the network. Even with sophisticated solutions, bad actors can still circumvent perimeter defenses. Monitoring of telephony networks will identify activity so mitigation tactics can be deployed to prevent further harm.

The following recommendations are actions hospitals and health systems can take to implement tools and technologies to assist with robocall fraud prevention.

- **Explore available robocall blocking capabilities.** The hospital and voice service provider can review possible robocall blocking solutions within the hospital or provider's network to stop inbound calling from specific numbers. This may include requesting a temporary block on a number used in a TDoS attack.
- **Identify fraudulent, disruptive or nuisance robocalls.** Review with your voice service provider the current services that may be available for call labeling and blocking. Identify appropriate contact information with your provider and how to respond to an event, including a description of the data hospitals should collect during an event (date/time of the calls, number being dialed, type of calls (recording or live person), volume of calls, CallerID being displayed, and the content of the message). Review third party offerings that may be available/installed in the hospital environment to assist in detecting and stopping unlawful robocall events.
- **Telephony management.** Not only do hospitals need to be aware of fraudulent, disruptive or nuisance robocall attacks against their network, the identity of a hospital can be compromised.
    - **Spoofing of Hospital number**. Until STIR/SHAKEN is fully deployed and adopted, a hospital's number can be unlawfully spoofed. Through staff training, unlawful spoofing can be identified through random complaints reported from individuals receiving calls not originated by the hospital. When this occurs, staff should capture the dialed number, date and time of calls, and content of the robocall if available. Report the spoofing event to the voice service provider and coordinate with the provider for possible initiation of a traceback request.
    - **Segregation of numbers.** Review and identify configuration of critical and non-critical lines. Discuss with your telephone system engineer or technician possible configuration changes to isolate critical phone lines from administrative and other lines, taking into consideration hunt-groups, busy,

[43] *See* American Hospital Association, *Cybersecurity*, www.aha.org/cybersecurity (last visited Nov. 11, 2020).

or no-answer rollover to other lines, etc. Prevent an overload of non-critical lines from rolling-over to lines answered by key personnel.

2. Response and Mitigation

The following steps are recommended for responding to fraudulent, disruptive or nuisance robocall activity within the hospital network. This covers the bare minimum strategies to be implemented.

- **Evaluate the event**.
  - Determine the type of robocall event.[44] If unclear, consider reporting incident to law enforcement for determination.
  - Determine if the identified event is an isolated event or a part of a campaign of robocalls.
  - Capture the following information:
    - most recent dates and times of the calls;
    - CallerID number displayed;
    - caller name displayed;
    - frequency of calls;
    - volume of calls;
    - examples of call content; and
    - toll-free telephone number or other telephone number provided for call back by the calling party.
  - Confirm the dialed number(s) the calls are routing to within the network.
  - Are one or more numbers receiving calls, possibly an entire range of numbers? If so, what are the numbers?
  - Identify the voice service provider for the numbers being dialed.
    - The voice service provider can assist in researching/stopping the calls.
  - Retain call logs and IP logs where available.
- **Implement internal controls**.
  - Contact the hospital's internal telecom engineers or technicians to implement configuration changes and safeguards within the premise-based equipment
    - Block spoofed numbers where applicable.
    - Route to a single line extension to avoid disruption or limit the number of calls into a line extension to isolate critical phone lines.

[44] *See supra* Section II.C. regarding types of robocall events.

- Separate the affected phone number from other critical trunks, which may require coordination with the PBX provider/maintainer.

- **Coordinate with federal and state agencies as appropriate.**

Hospitals should be familiar with the different types of unlawful robocalls they may receive and which types of calls should be shared with government agencies, directly or via their service provider, to assist in responding to or remediating such calls (whether a real-time event or a cumulative nuisance issue). Federal and state law enforcement agencies may be able to assist hospitals when it has been determined that the robocalls the hospitals are receiving constitute a violation of federal or state law, whether the calls themselves represent a violation of the law or the calls are made in furtherance of another crime (i.e., wire fraud).

Calls designed to elicit sensitive, non-public or protected information such as personally identifiable information or protected health information may constitute multiple violations of federal and state civil and/or criminal laws. Likewise, social engineering calls designed to deceive the recipient into providing sensitive information to be used in the commission of another crime, such a healthcare fraud or various telemarketing frauds, would also warrant law enforcement notification.

For example, a caller may attempt to connect to a patient room and falsely represent themselves as a Federal Medicaid or Medicare representative who needs additional personally identifying information from them to process their insurance claim—only to use that information in a false billing scheme.

Foreign-based cyber criminal gangs have recently been known to make targeted calls to gather information or "intelligence" during the reconnaissance phase of a cyber attack.[45] These calls may target staff of a hospital or health system and attempt to gather technical information under some pretext. For example, the caller may attempt to deceive the recipient into divulging their computer credentials either over the phone or through a follow up email designed to look like a legitimate log in screen from "tech support."

A pattern of unlawful robocalls which interfere or attempt to interfere with patient services and/or attempt to deceive staff and patients warrant law enforcement notification, regardless of whether the calls were successful in extracting the targeted information. It is important for law enforcement to receive these reports to assist them in correlation of reports from multiple victims. This will enable the authorities to identify emerging patterns of criminal activity and may provide valuable pieces of evidence. These reports, when assembled with information from other victims, may lead to the identification, investigation, and, ultimately, prosecution of the perpetrators.

[45] FBI and CISA Joint Advisory, *Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign*, Product ID: A20-233A (Aug. 20, 2020), https://krebsonsecurity.com/wp-content/uploads/2020/08/fbi-cisa-vishing.pdf.

a. Reporting the Event

- **Limit engagement with caller.** Staff members should be instructed to never engage with the caller. Instruct the staff members to disconnect the call once it is detected to be a robocall scam or disruption event.
- **Contact the voice service provider.** Designated staff, such as security, should provide concise information to the voice service provider regarding the event to determine next steps in collaboration with the voice service provider.
- **Traceback.** The service provider may perform a network traceback to identify the carrier(s) routing these calls into the hospital facility and request that upstream carriers cease and desist the continued delivery of such traffic. If the criteria are met, your provider may be able to engage the ITG to conduct a traceback to identify originating source network or end user (see recommendations above on the importance of collecting specific and accurate call information that is necessary for a traceback).
- **File a complaint with law enforcement.** Report the event to applicable regulatory or government agency.
    - Complaints can be made to the FTC at the following locations:
        - DoNotCall.gov (calls that violate Do Not Call and robocall rules)
        - ReportFraud.ftc.gov (complaints involving fraud—including frauds involving phone calls)
        - IdentityTheft.gov (complaints involving identity theft—including identity theft involving phone calls)
    - Complaints can be made to the FCC by visiting consumercomplaints.fcc.gov and clicking the link to "File an Unwanted Call Complaint." Any call that violates the robocall laws, spoofing laws, or Do Not Call rules may be reported to the FCC. The calls do not have to include telemarketing or fraud to be reported to the FCC.
    - For robocalls that appear to be connected to fraudulent schemes, identity theft or cyber attack, file a complaint with the FBI's Internet Crime Complaint Center (www.IC3.gov) and include the words unlawful robocalls, CallerID spoofing, or TDoS in the description of the event. Document the identification and any initial statements made by victim, patients and staff. Have individual victim, patient or staff member report any financial loss to their financial institution and www.ic3.gov immediately. If the financial loss resulted through a bank wire transfer of funds, financial institutions and the FBI through www.ic3.gov may be able to recover the funds if reported within 72 hours of the transfer being initiated. It is essential for effective financial recovery that all details of the financial transfer be reported, such as the originating and terminating financial account numbers, account

names, financial institutions, amount, date, time and location of transfer, transaction and wire transfer numbers, and contact information of sending and receiving parties. Contact your voice service provider, as outlined under previous sections, indicating you have contacted federal and state law enforcement authorities and you may seek prosecution and also request they preserve all technical information.

Report robocall events to your State Attorney General, particularly those that appear to be connected to fraudulent schemes specifically targeting hospital employees or result in a hospital- or department-wide TDoS attack. You can find your State's Attorney General by accessing the National Association of Attorneys General website at this link: https://www.naag.org/naag/attorneys-general/whos-my-ag.php.

b. Post Robocall Event

- **Work with law enforcement and regulatory agencies.**
  - Determine if the law enforcement agency will investigate.
  - Determine if the local Federal U.S. Attorney and/or State Attorney General's Office will seek prosecution.
  - Continue to provide assistance and information requested by law enforcement agencies.
  - Establish and maintain regular contact with your law enforcement contacts for case updates.
  - Conduct and document internal after-action review of incident with all involved entities to identify best practices and challenges.
  - Take corrective actions as necessary.

C. How the Federal and State Governments Can Help Combat Unlawful Robocalls

1. Prevention

State and federal agencies should continue to expand their efforts to prevent robocalls from ever reaching hospitals and other end users (including consumers who receive fraudulent calls from entities unlawfully impersonating hospitals or other healthcare entities) by putting into practice the following recommendations.

- **Create and implement balanced policies that facilitate industry's ability to prevent unlawful robocalls from reaching hospitals**. While many of these efforts are currently underway, they will require ongoing attention, implementation, and enforcement. These policies include:
  - Encouraging the continued development of new call blocking and labeling tools and the expanded use of existing tools;

- Establishing and enhancing, as appropriate, safe harbors that incentivize increased call blocking (including within the network) and labeling of calls that appear to be unlawful based on reasonable analytics;[46]
- Establishing and enforcing industry call authentication requirements to combat unlawful spoofing and ensuring such obligations will sufficiently apply to communications made to or from hospitals, including STIR/SHAKEN for the IP portions of voice service provider networks and effective robocall mitigation programs on the non-IP portions of their networks;
- Encouraging all voice service providers to cooperate with traceback requests in accordance with existing laws;
- Encouraging all voice service providers to adopt State Attorneys General Anti-Robocall Principles as appropriate;[47] and
- Identifying, in cooperation with industry, a process for hospitals to register their own numbers in order to minimize inadvertent blocking of outbound calls from hospitals.

- **Enforce existing laws, rules, and policies against voice service providers that allow unlawful traffic to originate on their network or calling platform. Additionally, enforce existing laws, rules, and policies, as appropriate, against non-originating voice service providers that have not taken sufficient steps to mitigate the transmission of unlawful robocalls**.
  - Historically, enforcement efforts against bad actors focused on robocallers themselves, not voice service providers facilitating those calls. Increased efforts against voice service providers enabling unlawful robocallers are proving successful as part of a comprehensive strategy to reduce the overall number of unlawful calls passing through the U.S. network. These efforts likely fall into both the prevention and remediation categories, but reducing this unlawful traffic will have the effect of fewer robocalls reaching hospital telephone lines.
- **Develop clear and concise hospital education materials**.
  - In addition to regulatory and enforcement efforts to facilitate the prevention of unlawful robocalls, federal and state agencies can help hospitals be prepared in advance of robocalling events by providing education materials on robocall prevention, response, and remediation.

---

[46] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, para. 26 (2020) (discussing "reasonable analytics").

[47] *See Anti-Robocall Principles,* https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf.

Therefore, federal and state agencies should supplement the information in this report as needed and in conjunction with relevant stakeholders by developing materials which provide the following essential information to hospitals:

- An explanation of the different types of robocalls and robocall events, including how staff members can recognize unlawful calls;
- A description of the data hospitals should collect during a robocall event in order to report issues to law enforcement or to seek a traceback, such as the date and exact time of the call, the number receiving the call, the number displayed on the caller ID, whether the caller was a live person or a pre-recorded message, and the content of the message;
- Guidance about which law enforcement agencies hospitals should contact to report unlawful robocalls, including State AG offices, the FTC, the FCC, the FBI, and the Department of Homeland Security, with contact information for those agencies;
- A description of available call blocking and labeling tools and other industry tools that can be utilized by enterprise systems, including STIR/SHAKEN.
- Where and how hospitals can register their own numbers to limit the possibility that those numbers are not inadvertently blocked or mislabeled; and
- Where and how hospitals can get redress from incidents where their legitimate outbound calls are inadvertently blocked or mislabeled.

2. Response and Mitigation

While the immediate effort to stop a robocall event in its tracks is often between a hospital, its provider, and other industry members, law enforcement should take the following steps to ensure that its response to these events is effective and timely.

- Establish improved communication methods between hospitals and law enforcement agencies so that hospitals know where and how to report ongoing or recent robocall events.
- Actively monitor complaints received from hospitals and engage in prompt outreach to relevant voice service providers and other law enforcement agencies that may be able to assist in the response.
- Make prioritized referrals to the ITG for hospital robocall events as appropriate and coordinate the traceback response among relevant law enforcement partners.
- Despite all efforts to prevent and respond to robocall events that disrupt hospital operations, unlawful and fraudulent calls will inevitably get through. State and federal law enforcement agencies, often with the help of the ITG and

individual voice service providers, are continually seeking to track down the bad actors and bring them to justice. To that end, we make the following recommendations.

- Increase and continue collaboration between industry and law enforcement, as well as the ITG, to share information about targeted hospital robocall events.
- Establish appropriate methods for sharing information about hospital robocall events across all relevant enforcement agencies. Agencies may need to enter into memoranda of understanding or common interest agreements in order to share information on existing investigations and may need to identify an internal point of contact for hospital robocall investigations.
- Utilize all tools at agencies' disposal to investigate unlawful robocalls to hospitals, including regular searches of complaint databases for hospital complaints, communication with the ITG about hospital-related tracebacks, and, where necessary and appropriate, the issuance of investigative subpoenas to targets and affiliated parties.
- Ensure sufficient coordination among enforcement agencies to aggressively pursue civil or criminal enforcement actions against robocallers that send unlawful calls impacting hospitals and against voice service providers that assist and facilitate such activities.
- Communicate and coordinate with foreign governments where possible to address unlawful robocall traffic originating internationally and pursue criminal enforcement actions against foreign individuals, call centers, and any other entities responsible for making unlawful robocalls into the United States.
- Collect data on hospital robocall events and actions taken in response, then analyze the data and adapt enforcement approaches to increase efficacy of future response and remediation efforts.

IV. CONCLUSION

Combating unlawful robocalls is an enormous effort. Although this report is not an exhaustive list of actions and recommendations, it has been written with the input of knowledgeable and experienced subject matter experts with the charge of providing guidance and best practices. The reader should understand that the severity of these calls is wide ranging, from nuisance to privacy evasion to life-threatening. Eliminating them may be an impossibility, however significantly reducing them to acceptable risk levels can be attained and will require the cooperation of federal and state governments, law enforcement, the telecom industry, voice service providers and voice service provider customers.

APPENDIX A – HRPG Membership

Chair:

- Dave Summitt, Chief Information Security Officer, Moffitt Cancer Center

Vice Chair:

- Patrick Halley, Senior Vice President, Policy & Advocacy, US Telecom – The Broadband Association

Voice Service Providers that Serve Hospitals:

- John Cunningham, Director of Fraud Management, CenturyLink
- Joseph DeLotto, VP of Voice and Unified Communications Products, Charter Communications (*Chair Working Group 1: Addressing recommendations on how providers can better combat unlawful robocalls made to hospitals*)
- Linda Vandeloop, Assistant Vice President, Federal Regulatory, AT&T

Companies that Focus on Mitigating Unlawful Robocalls:

- Mark Collier, Chief Technology Officer, SecureLogix
- Aaron Foss, Founder and CEO, Nomorobo
- Patrick Halley, Senior Vice President, Policy & Advocacy, US Telecom – The Broadband Association

Consumer Advocacy Organizations:

- John Breyault, Vice President, Public Policy, Telecommunications and Fraud, National Consumers League
- Dawit Kahsai, Senior Legislative Representative, AARP (formerly the "American Association of Retired Persons")
- Irene Leech, Vice-President, Consumer Federation of America

Providers of one-way voice over internet protocol services:

- Gunnar Halley, Assistant General Counsel CELA-Privacy & Regulatory Affairs, Microsoft Corporation
- Rebekah Johnson, Founder & CEO, Numeracle
- Chris Shipley, Attorney & Policy Advisor, INCOMPAS

Hospitals:

- Richard Lovich, Managing Partner, Stephenson, Acquisto & Colman, and National Counsel to the American Association of Healthcare Administrative Management (AAHAM)
- John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association (*Chair Working Group 2: Addressing recommendations on how hospitals can protect themselves from unlawful robocalls*)
- Dave Summitt, Chief Information Security Officer, Moffitt Cancer Center & Research Institute

State Government Officials Focused on Combating Unlawful Robocalls:

- Creecy Johnson, Special Deputy Attorney General, North Carolina Attorney General's Office (*Chair Working Group 3: Addressing recommendations on how the Federal Government and State governments can help combat unlawful robocalls*)
- David McCoy, Assistant Attorney General, Office of the Arkansas Attorney General
- Wisam Naoum, Assistant Attorney General, Michigan Department of Attorney General

FCC Representative:

- Commissioner Brendan Carr

FTC Representative:

- Commissioner Noah Joshua Phillips

Donna Cyrus, Designated Federal Officer

Aliza Katz, Deputy Designated Federal Officer

A. APPENDIX B – Additional Resources

a. Resources Available from State Attorneys General's Offices

Many state AGs have made combating unlawful robocalls a top priority for their offices' consumer protection enforcement actions. These offices often have one or more attorneys and investigators that regularly investigate and litigate persons and companies that commit robocall violations. Plus, these offices may be a more immediately accessible resource than other government agencies. Contact information for every State Attorney General may be found at:

https://www.naag.org/naag/attorneys-general/whos-my-ag.php

b. Resources Available from the FCC and FTC

FTC

Suggestions for Blocking & Reporting Robocalls

https://www.consumer.ftc.gov/features/how-stop-unwanted-calls

https://www.consumer.ftc.gov/articles/how-block-unwanted-calls

Complaint Reporting Website

https://www.ftccomplaintassistant.gov

FCC

Suggestions for Blocking & Reporting Robocalls

https://www.fcc.gov/call-blocking

https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

Complaint Reporting Website

https://consumercomplaints.fcc.gov

c. Resources Available from the Industry Traceback Group

Industry Traceback Group Policies and Procedures

https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf

Guidance to law enforcement agencies for submitting traceback requests

https://www.ustelecom.org/wp-content/uploads/2020/09/Guidelines-for-Law-Enforcement-Submissions-of-Traceback-Requests.pdf